



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA



DEPARTAMENTO DE ORGANIZACIÓN DE EMPRESAS

**PROGRAMA: INTEGRACIÓN DE LAS TECNOLOGÍAS DE LA
INFORMACIÓN EN LAS ORGANIZACIONES**

TESIS DOCTORAL

Título: Factores críticos en la adopción de las medidas de seguridad utilizadas por los alumnos de los Centros formativos universitarios de tecnologías TIC al usar herramientas 2.0

Alumno: JOSÉ RAMÓN DÍAZ SÁENZ

**Directores: HERMENEGILDO GIL GÓMEZ
JUAN VICENTE OLTRA**

Curso 2014 – 2015

Valencia, Junio de 2015

Agradecimientos

Esta tesis no habría sido posible sin la colaboración, ayuda y consejo de muchas personas. No debo dejar de agradecer las diferentes aportaciones que cada una han realizado para que finalmente fuese una realidad.

En un momento como éste en el que se culmina el esfuerzo de varios años, quiero dejar constancia de una actuación muy especial, la de mis directores de Tesis, Hermenegildo y Juan Vicente, por sus directrices, múltiples revisiones, colaboración en las encuestas e infinita paciencia que han tenido conmigo.

A mis amigos, compañeros y directores de una nueva tesis en ciernes, Luisa Tolosa y Carlos Hernández, por sus consejos semánticos para la redacción, el apoyo para el acceso a encuestados y su consideración al reconocer prioridades investigadoras.

También quiero recordar a todos aquellos familiares, amigos, conocidos.....que durante todos estos años me preguntaban por las razones para dedicar tanto tiempo a esta investigación, porque ellos fueron un acicate para completarla, sobre todo en los momentos más difíciles, que haberlos los hubo.

Como no, a mi esposa Concha, porque sin sus ánimos, favor y tolerancia no habría dispuesto del tiempo requerido para desarrollarla.

Y, finalmente a mis hijos Francisco y Fernando quienes, sin siquiera intuirlo, han sido los auténticos impulsores de esta investigación al comprobar, en unos seres tan cercanos y queridos, los riesgos que están asumiendo nuestros jóvenes y que pueden comprometer su futuro como ciudadanos libres.

Resumen

Deseamos conocer los factores que influyen en la seguridad de los estudiantes universitarios actuales, de tecnologías TIC, cuando utilizan recursos para navegar en la web 2.0.

La idea, y sensibilidad, que tienen estos jóvenes respecto la seguridad informática en general es elemento clave para entender la forma en la que la ponen en práctica.

Estudiando las motivaciones que justifican el auge de las redes sociales en ese segmento de población, supuestamente la más preparada respecto la utilización de sistemas digitales de comunicación, encontraremos los factores que condicionan su rendimiento así como el nivel de riesgo que asumen consciente o inconscientemente.

Los resultados obtenidos nos ayudarán a modificar, si fuese necesario, la docencia impartida en esas titulaciones o nos indicarán lo idóneo de las mismas, informándonos sobre la posible existencia de una brecha entre lo que deben saber y como lo aplican en su vida diaria.

Resum

Desitgem conèixer els factors que influeixen en la seguretat dels estudiants universitaris actuals, de tecnologies TIC, quan utilitzen recursos per navegar a la web 2.0.

La idea, i sensibilitat, que tenen aquests joves respecte la seguretat informàtica en general és element clau per entendre la forma en què la posen en pràctica.

Estudiant les motivacions que justifiquen l'auge de les xarxes socials en aquest segment de població, suposadament la més preparada respecte la utilització de sistemes digitals de comunicació, trobarem els factors que condicionen el seu rendiment així com el nivell de risc que assumeixen conscient o inconscientment.

Els resultats obtinguts ens ajudaran a modificar, si fos necessari, la docència impartida en aquestes titulacions o ens indicaran la idoneïtat de les mateixes, informant-nos sobre la possible existència d'una bretxa entre el que han de saber i com l'apliquen a la seva vida diària.

Summary

We want to know the factors that influence the safety of current college students, ICT technologies, when used resources to surf the web 2.0.

The idea and sensitivity that these young people about computer security in general is key to understanding how the implemented element.

Studying the reasons that justify the rise of social networks in that segment of the population, supposedly more prepared regarding the use of digital communication systems, we find the factors that affect performance and the level of risk assumed consciously or unconsciously.

The results will help us to modify, if necessary, the training provided in those degrees or teaching us ideal state of the same, telling us about the possible existence of a gap between what they should know and how they apply in their daily lives.

Sumario

1.- INTRODUCCIÓN	14
1.1 Justificación del trabajo	15
1.1.1 Razones personales	16
1.1.2 Razones docentes	18
1.1.3 Razones científicas	21
1.2 Objetivos de la investigación.....	23
1.3 Estructura: contenido por capítulos	26
2.- MARCO TEÓRICO	30
2.1 Antecedentes	31
2.1.1 Bases conceptuales de la investigación	32
2.1.2 Seguridad global en internet.....	38
2.1.3 Protección de la privacidad en internet	51
2.1.4 Seguridad en la Web 2.0: identidad digital.....	55
2.2 Estado actual.....	69
2.2.1 Big Data.....	69
2.2.2 Brecha digital.....	71
2.2.3 Legislación (Europea / Americana / Española).....	75
2.3 Literatura revisada de otros investigadores.....	88

3.- MODELO PROPUESTO	96
3.1 Estrategia para el desarrollo de la investigación	97
3.2 Táctica para el desarrollo de la investigación	100
3.3 Modelo inicial de estudio.....	103
3.4 Hipótesis.....	112
4.- METODOLOGÍA	118
4.1 Metodología para el estudio de campo de la tesis doctoral	119
4.2 Herramientas estadísticas utilizadas	122
4.3 Calendario de actuaciones	129
4.4 Codificación de la encuesta de la tesis	140
4.5 Selección de la muestra objeto del estudio	145
4.5.1 Cálculo del error muestral.....	146
5.- RESULTADOS	148
5.1 Estadísticos básicos: análisis de fiabilidad	149

5.2 Estadísticos estructurales previos	153
5.3 Evolución del análisis	163
5.3.1 Estadísticos básicos	165
5.3.2 Estadísticos estructurales	171
5.4 Modelos estructurales completos	180
5.4.1 Modelo estructural alternativo	195
5.4.2 Modelo estructural “multiobservado”	203
6.- CONCLUSIONES.....	210
6.1 Limitaciones.....	211
6.2 Discusión de los resultados.....	213
6.3 Resumen de aportaciones.....	220
6.4 Acciones futuras, recomendadas	223
7.- BIBLIOGRAFÍA.....	228
7.1 Cursos realizados en el Centro de Formación Permanente de la UPV (CFP).....	258
ANEXOS.....	260

Sumario de Anexos

ANEXO 1 – Grafos estructurales modelo.....	261
ANEXO 2 – Aspectos básicos sobre Teoría Estadística en Ciencias Sociales	266
2A - El Método Científico en las Ciencias Sociales	266
2A.1 - Métodos cuantitativos en las Ciencias Sociales	269
2A.2 - Diseño de la investigación	271
2B – Encuestas.....	273
2B.1 - El cuestionario.....	275
2B.2 - Presentación del cuestionario	277
2B.3 - Prueba del cuestionario	278
2B.4 - Constructos y variables.....	281
2B.5 – Causalidad	286
2C - Introducción a las Escalas de Medición	289
2C.1 - Escala de Likert	291
2C.2 - Construcción de las escalas Likert	294
2C.3 - Análisis de los ítems	296
2C.4 - Maneras de aplicar la escala Likert	297
2C.5 - Fiabilidad y Validez de las Escalas de Actitud	299
2C.6 – Codificación	301
2C.7 - Análisis de datos.....	304
2C.8 – Muestra.....	306
2D - Fundamentos Estadísticos para nuestro estudio.....	309
2D.1 - Medidas de tendencia central, dispersión y concentración.....	310
2D.2 - Análisis descriptivo inferencial: comparaciones en muestras	312
2D.3 - Análisis simple de la varianza.....	317
2D.4 - Coeficiente de correlación de Pearson	319
2D.5 - Análisis de regresión simple	320
2D.6 - Análisis multivariado	322

2D.7 - Regresión múltiple	323
2D.8 - Análisis de trayectorias.....	324
2D.9 - Coeficientes de senderos (path coefficients)	327
2D.10 - Criterio de los mínimos cuadrados.....	329
2D.11 - Análisis factorial	330
2E - Características de los modelos de ecuaciones estructurales.....	332
2E.1 - Estrategias de modelización.....	333
2E.2 - Fases de un modelo de ecuaciones estructurales	334
2E.3 -Resumen y conclusiones de utilización de Ecs. Estructurales	336
2E.4 - Prueba de chi cuadrado	340
2E.5 - Coeficiente de ajuste comparativo (CFI)	340
2E.6 - Error Medio Cuadrático de Aproximación (RMSEA).....	341
2E.7 - Coeficiente de ajuste normalizado (NFI).....	342
ANEXO A – Codificación x pregunta	343
ANEXO A1 - Primer cuestionario piloto, con comentarios resaltados	344
ANEXO A1.1 - Resultados análisis primer cuestionario piloto.....	350
ANEXO A2 - Segundo cuestionario piloto.....	354
ANEXO A2.1 - Resultados análisis segundo cuestionario piloto	360
ANEXO A3 - Cuestionario definitivo	372
ANEXO A3.1 - Resultados cuestionario definitivo (curso 2011-12).....	378
ANEXO A3.2 - Resultados cuestionario definitivo (curso 2012-13).....	409
ANEXO B - Preguntas sobre conocimientos (test)	421
ANEXO B 1 - Respuestas a conocimientos (test)	422
ANEXO B2 – Calificaciones.....	429
ANEXO C - Cálculo de regresiones, curso 2011-12.....	431
ANEXO C.1 - Cálculo de factores, curso 2011-12.....	445

ANEXO C.2 - Modelos estructurales, curso 2011-12	459
ANEXO D - Cálculo de regresiones, curso 2012-13.....	467
ANEXO D.1 - Cálculo de factores, curso 2012-13	487
ANEXO E - Cálculo para todos los alumnos de los dos cursos	498

Sumario de Figuras

Figura 1. Fases de la investigación	33
Figura 2. Problemas por ataques de virus, infecciones por spyware, o spam, en 2007 (UE-27).....	39
Figura 3. Comparativa de medidas de seguridad en empresas, según tamaño (España)	39
Figura 4. Comparativa de incidencias de seguridad en el último año en empresas.	40
Figura 5a. Penetración del Comercio electrónico en Europa (2010).....	41
Figura 5b. Penetración del Comercio electrónico en Europa (2012).....	41
Figura 6. Evolución trimestral del Comercio electrónico en España.....	41
Figura 7. Internautas con problemas de seguridad en España (último mes)	44
Figura 8a. Percepción sobre la protección de privacidad en los sitios web	47
Figura 8b. Percepción de que las autoridades no protegen la privacidad suficientemente.....	47
Figura 9. Anatomía de una amenaza moderna	54
Figura 10. Impactos en la Red que conforman la identidad digital	56
Figura 11. Coexistencia real y virtual	57
Figura 12. Recursos para la Identidad digital	57
Figura 13. Datos de los diferentes perfiles de Identidad Digital	58
Figura 14. Características de la Identidad digital	59
Figura 15. Tipo de información que se distribuye en Redes sociales y sitios de compartición, en la UE.....	60
Figura 16. Recomendaciones preventivas y reactivas sobre la identidad digital	62
Figura 17. Ciclo de vida de la identidad digital.....	62
Figura: 18. Tareas realizadas en internet para proteger la identidad digital (UE).....	63
Figura 19. Datos e información considerados personales (UE)	63
Figura 20. Impresiones sobre la revelación de datos considerados personales (UE)	64
Figura 21. Usuarios de internet a nivel mundial.....	72
Figura 22. Penetración de internet en España y Europa.....	73
Figura 23. Acceso a internet en España por tramo de edad y sexo	74

Figura 24. Acceso desde el móvil en España	74
Figura 25. Distribución del tipo de delitos informáticos.....	85
Figura 26. Tipologías penales.....	86
Figura 27. Cibercriminalidad y principales delitos cometidos con Nuevas Tecnologías.....	87
Figura 28. Objetivos del estudio	97
Figura 29. Parámetros de observación del estudio	102
Figura 30. Latentes comunes	113
Figura 31. Influencias en la actitud.....	113
Figura 32. Relaciones actitudinales	114
Figura 33. Influencias de la confianza	115
Figura 34. Influencias del riesgo	115
Figura 35. Fundamentación teórica del modelo de ecuaciones estructurales.....	126
Figura 36. Fundamentación empírica del modelo de ecuaciones estructurales.....	128
Figura 37. Ejecución de la investigación	212
Figura 38. Círculo de Deming	268
Figura 39. Curvas actitud-probabilidad de respuesta 1 -.....	292
Figura 40. Curvas actitud-probabilidad de respuesta 2 -.....	292
Figura 41. Distribución normal, para el 95% de confianza.....	313
Figura 42. Casos en uno de los extremos del área de la curva	315
Figura 43. Diagrama de senderos	325
Figura 44. Ecuaciones de regresión 1	328
Figura 45. Ajuste de regresión.....	329
Figura 46. Fases de obtención de un modelo de ecuaciones estructurales.....	334

Sumario de Grafos

Grafo 1.	Modelo estructural teórico	106
Grafo 1bis.	Modelo estructural causal teórico.....	111
Grafo 2.	Modelo más simple propuesto del curso 2011-2012.....	153
Grafo 3.	Modelo simple con variables de control del curso 2011-2012	158
Grafo 4.	Modelo sugerido, con variables de control, del curso 2011-2012	159
Grafo 4bis.	Modelo sugerido, con variables de control, del curso 2012-2013.....	171
Grafo 5.	Modelo de cuatro constructos con los alumnos del curso 2012-13	175
Grafo 6.	Modelo de cuatro constructos con todos los alumnos de los dos cursos.....	180
Grafo 6bis.	Modelo optimizado de cuatro constructos con los alumnos de ambos cursos.....	184
Grafo 6tris.	Modelo básico de cuatro constructos optimizado con los alumnos de ambos cursos.....	191
Grafo 6-tetrakis.	Modelo básico de cuatro constructos optimizado con los alumnos de ambos cursos – valores estandarizados	193
Grafo 7.	Modelo correlacional con los 396 alumnos de los dos cursos	196
Grafo 7bis.	Modelo correlacional con cinco variables de control para los dos cursos.....	204
Grafo 8.	Diversos tipos de Relación entre variables.....	286
Grafo 9.	Diversas influencias internas entre variables	287

Sumario de Tablas

Tabla 1. Objetivos de la investigación	25
Tabla 2. ¿Cambió su password durante el último año para acceder a esos servicios?	42
Tabla 3. Indicadores para medir las variables latentes	104
Tabla 4. Motivaciones descritas por autores consultados	105
Tabla 5. Relación de Hipótesis con variables.....	143
Tabla 6. Población objeto de la muestra	147
Tabla 7. Parámetros encuesta curso 2011-2012	152
Tabla 8. Regression Weights: (Group number 1 - Default model).....	154
Tabla 9. Standardized Regression Weights	155
Tabla 10. Efectos entre las variables latentes	156
Tabla 11. Parámetros modelos estructurales curso 2011-2012	157
Tabla 12. Resultados proceso grafo 4	160
Tabla 13. Frecuencias de alumnos que realizan funciones sobre uso de contraseñas	166
Tabla 14. Frecuencias de alumnos que realizan funciones sobre uso de backups.....	167
Tabla 15. Correlación entre funciones de defensa que realizan los alumnos y Estadísticos básicos	167
Tabla 16. Frecuencias de alumnos que realizan funciones sobre normas básicas de Seguridad	168
Tabla 17. Frecuencias de alumnos que expresan contenidos a través de Redes Sociales.....	168
Tabla 18. Parámetros encuesta curso 2012-2013	169
Tabla 19. Parámetros encuesta ambos cursos.....	170
Tabla 20. Resultados proceso grafo 4bis.....	172
Tabla 21. Resultados proceso global con alumnos 2012-2013	176
Tabla 22. Resultados proceso global con alumnos ambos cursos	181
Tabla 23. Resultados optimizados del proceso global con alumnos ambos cursos..	185
Tabla 24. Resultados optimizados del modelo correlacional con alumnos ambos cursos	197

Tabla 25. Resultados del modelo con 5 variables de control para ambos cursos.....	205
Tabla 26. Comparación parámetros de ajuste modelo final y alternativo	217
Tabla 27. Resultados de Hipótesis	218
Tabla 28. Formulación de preguntas correspondientes a valores	298
Tabla 29. Valores de K más usados	308
Tabla 30. Casos en ambos lados del área de la curva a partir de la media aritmética	314
Tabla 31. Casos en uno de los extremos del área de la curva	315

1.- INTRODUCCIÓN

1.1 Justificación del trabajo

En los siguientes apartados desarrollaremos las distintas razones que generaron la suficiente inquietud como para impulsar esta investigación.

Fundamentalmente describiremos la convergencia de características propias del autor (ingeniero, educador, padre de familia, consumidor, usuario, curioso, ciudadano) a través de los siguientes factores:

- Personales, debidos a la formación, experiencia y observación
- Responsabilidades próximas al apoyo a la formación de las próximas generaciones, impulsadas por la colaboración con organizaciones educativas así como también por la percepción de los hábitos de los jóvenes más próximos
- Interés por sacar provecho y abordar el aprendizaje para el conocimiento de las herramientas más novedosas que nos sirvan de soporte para el desarrollo del presente estudio.

A lo largo de la presente tesis referenciaremos noticias que nos llegan a través de los diversos medios de Comunicación (generalistas, universitarios, profesionales y/o especializados) sobre los problemas que surgen con frecuencia debidos a un uso inadecuado de las TIC y que, por si solos, exacerban nuestro interés e incrementan la inquietud que se va a indagar.

Asimismo, la importancia de esta investigación se confirma por la coincidencia en el tiempo de estudios realizados por investigadores de otros continentes sobre experiencias similares que certifican la conveniencia de abordarla.

1.1.1 Razones personales

El motivo del interés sobre estos temas radica en los siguientes puntos:

- a) La formación académica: Ingeniero Superior de Telecomunicación y Diplomado en Planificación Financiera por la Universidad Politécnica de Madrid, Máster CALSI (Contenidos y Aspectos Legales de la Sociedad de la Información) y Diplomado en Estudios Avanzados (Programa ITIO) por la Universitat Politècnica de València

- b) La carrera profesional, vinculada desde el principio al sector de las Tecnologías de la Información como becario en IBM desde 1973, trabajando posteriormente como Analista de aplicaciones técnicas en empresas de ingeniería (Heredia y Moreno, S. A. y Foster Wheeler Iberia, S. A., en Madrid) e incorporándome nuevamente a IBM, promoviendo proyectos informáticos, hasta mi prejubilación en Valencia, en 1997. A continuación, como administrador de una empresa de servicios de telecomunicación (Fringes, S. A.) y finalmente, simultaneando labores como Profesor de Tecnología en la Licenciatura de Comunicación Audiovisual de la UPV en el campus de Gandía con Asesoramiento tecnológico a diversas empresas locales.

- c) Personal, como usuario de los programas más generalizados para navegar y trabajar en la red (correo, mensajería, redes sociales, Office...)

- d) Inquietud personal / profesional / ética / moral / legal..., como consecuencia de la observación directa de algunas de las posibilidades que permiten las herramientas informáticas actuales de uso generalizado, incluso llegando a consultar con profesionales del Derecho al comprobar la distancia entre lo que permite la tecnología y lo que se puede y no se debe hacer. Sabemos que el legislador siempre irá por detrás de la tecnología (experimentos genéticos, clonaciones, nuevos tipos de delito...), pero la obsesión por las posibilidades que ofrece ésta no debe dejar que los árboles nos impidan ver el bosque; es decir, hay que tener perspectiva y ver, en su conjunto, lo que las nuevas herramientas permiten y como evitar los perjuicios que puedan generar.

e) Responsabilidad social, intentando preservar el interés común de la sociedad en su conjunto, y de los individuos que la componemos en particular, por los riesgos inherentes al uso indiscriminado y masivo de herramientas que facilitan la comunicación pero que, sin los conocimientos básicos necesarios, pueden generar graves perjuicios a una parte de la población que integra esa misma sociedad, la más vulnerable, y que puede comprometer su futuro y el del resto.

1.1.2 Razones docentes

Durante varios años (1990-1997) representé a IBM como Patrono en ADEIT¹, y también en la Fundación ETNOR². Como Secretario General de la RSEAP³ también representé a esta sociedad cultural en la Fundación Valenciana de Estudios Bursátiles. A título más personal fui miembro del Consejo Asesor de ESTEMA⁴.

La convergencia subyacente de estas actividades, junto con mi dedicación como Profesor Asociado en la UPV, tienen un factor común: la Educación.

Durante esos años he participado en innumerables reuniones en las que he estado escuchando estrategias docentes, planes formativos, proyectos y problemas sobre diferentes aspectos educativos, y he tratado de aportar ideas sobre cómo paliar las dificultades aparecidas, cómo conseguir la mayor calidad y dar respuesta a las necesidades sociales de nuestro entorno, en los diferentes ámbitos.

Sin embargo, en un encuentro con motivo de la presentación del informe “Gestión de Riesgos y medios de comunicación social, un cambio de paradigma” realizado por el *International Development Research Centre*⁵ (Moyer, 2009), se denunció que muchas organizaciones e instituciones preferían ignorar los problemas sobre los riesgos de vulnerabilidad y violación de la privacidad y los derechos de autor cuando se navega por redes sociales, incluyendo a estudiantes, profesores y administradores. Se recomendaba establecer directrices para paliar la falta absoluta de control sobre la información que se publica.

En esas mismas fechas, según el director de seguridad de internet de la empresa de seguridad de vigilancia NetWitness, de Herndon (Virginia), “*las instituciones que optan por hacer la vista gorda ante el sector de los medios sociales se están haciendo un flaco favor que podría, en algún momento en el futuro, convertirse en su mayor problema*” (McCrea, 2009: 2).

¹ Fundació Universitat Empresa. Universitat de Valencia

² Ética de los Negocios y de las Organizaciones

³ Real Sociedad Económica de Amigos del País, de Valencia

⁴ Escuela de Negocios. Universidad Europea

⁵ Corporación de la corona canadiense establecida por una ley del Parlamento en 1970 para ayudar a los países en desarrollo a encontrar soluciones a sus problemas.

Los centros de enseñanza deben elaborar directrices para el uso de las redes, controlar cómo se utilizan y saber qué hacer cuando se sobrepasan los límites.

De hecho, en relación con las estrategias de aprendizaje, Beltrán (1993) ya señalaba que los resultados de dicho aprendizaje están muy vinculados con el uso de estrategias cognitivas que son las que convierten el material enseñado en material aprendido. A su vez, García y Pintrich (1994) ya indicaban que el uso de este tipo de estrategias, no su conocimiento, está relacionado e influenciado por la motivación del propio estudiante.

Nos referimos al aprendizaje de la competencia que integra conocimiento, habilidad y predisposición para afrontar adecuadamente las situaciones complejas que se presenten, de forma profesional. Interviene la componente actitudinal y volitiva sin la cual el desempeño competente no se alcanzaría. (Lasnier, 2000; CIDEC, 2004).

Desde la perspectiva docente, la motivación es un factor de impulso y orientación para los estudiantes que les implica en el aprendizaje de las actividades académicas y determina su nivel de adquisición. Una de las nociones más intuitivas de la motivación implica que solo ocurre en las personas interesadas, o preocupadas, por alguna actividad concreta.

Esta motivación está integrada por cuatro factores (Githua y Mwangi, 2003):

- interés o curiosidad por el aprendizaje,
- utilidad o valor del contenido del aprendizaje,
- confianza en su probabilidad de éxito, y
- satisfacción respecto al equilibrio de recompensa y esfuerzo.

Diversos estudios han investigado sobre las motivaciones de los alumnos para el logro de sus metas. La teoría de la Motivación-Logro, iniciada por Dweck (1986) y seguida por Pintrich (2000) y Dupeyrat y Mariné (2005) determinan que el comportamiento del estudiante está basado en la consecución de unos objetivos concretos, superar las pruebas. La orientación de los trabajos que se han desarrollado ha ido hacia el aprendizaje y hacia el resultado. Estudios sobre la Teoría de la Autoeficacia llegan a la conclusión de que se realizan las acciones necesarias para llegar a la meta deseada, el

resultado (Usher y Pajares, 2006). Los alumnos que se sienten suficientemente seguros de sí mismos si se preocupan por su aprendizaje y no solamente por sus resultados académicos (Elliot y Church, 1997). Cuestionarios específicos fueron desarrollados para conocer la relación entre motivación y actitud de nuestros estudiantes (Beltrán *et al*, 2006) adecuados a otras muchas investigaciones (Gargallo *et al*, 2007 y 2012)

En algunas de esas investigaciones se describe la ausencia de efecto significativo entre las estrategias de aprendizaje y el rendimiento académico. Cuando su motivación se dirige a obtener buenos resultados académicos no importando la utilidad del aprendizaje realizado, no se consigue la competencia necesaria (González *et al*, 2002).

Es decir, he estado vinculado a organizaciones que determinan estrategias educativas e incluso, como profesor, he estado en contacto directo con los alumnos.

Pero a la vez, con los informes anteriores referenciados me encuentro con llamadas de atención sobre:

- Responsabilidad, control y directrices, de los que pueden y deben hacerlo
- Condiciones para impulsar motivación y obtención de la competencia, por parte de los estudiantes

Queremos comprobar la parte de los estudiantes; es decir, sus factores críticos de éxito en el caso concreto de la adopción de medidas de seguridad cuando utilizan las tecnologías TIC los estudiantes más preparados para su uso, navegando por internet e interactuando en Redes Sociales, tal y como se titula la presente tesis.

Y, como consecuencia de los resultados que se obtengan en la investigación, aportar la suficiente información para no obviar la parte de responsabilidad que pueda derivarse para quien proceda.

1.1.3 Razones científicas

Nos hemos planteado preguntas sobre la actuación en seguridad informática que debieran estar influenciados por los conocimientos de los jóvenes estudiantes de estas materias tecnológicas, basadas en las teorías constructivistas sobre la motivación y que se enfocan principalmente en las componentes socio-culturales del aprendizaje.

Según la psicología educativa constructivista (Risnes, 1999), se explica la forma en la que los alumnos entienden el aprendizaje y cómo se consideran a sí mismos con respecto a sus posibilidades de aprender y cómo puede influir en sus resultados, habiendo tres frentes que conforman el conocimiento en general de los alumnos:

1. Su ambiente sociocultural
2. Su ambiente curricular e institucional de sus antecedentes escolares y formación
3. Las motivaciones, intereses y sentimientos que les produce la navegación y uso de estas herramientas

Estudiado por Alonso (2005) a través de un cuestionario que mide las metas, valores-intereses y expectativas de los alumnos en diferentes contextos de aprendizaje.

Sobre el ambiente curricular es posible plantearse las siguientes cuestiones: sus antecedentes escolares, es decir qué tipo de formación cursaron y cuáles fueron sus resultados; el rendimiento académico, y el número de cursos en la UPV. Estas cuestiones se representan por variables curriculares cuyas respuestas son cuantitativas y por lo tanto es posible responderlas con el contraste de hipótesis, tales como que no hay diferencia en las calificaciones promedio entre los alumnos de una u otra Escuela seleccionada.

Las ideas que los estudiantes tienen respecto de la seguridad informática es elemento clave para entender la forma en que la ponen en práctica y que hay que considerar para entender la forma de adoptar medidas de seguridad cuando utilizan ordenadores.

Esta tesis comporta un estudio para derivar un conjunto de indicadores que relacionen los conocimientos reales que tienen y la actitud de los alumnos ante el propio aprendizaje de temas relacionados con este fin, formulándonos preguntas teniendo en cuenta que, según Lahey (1999: 685), “*las creencias son las que nos predisponen para actuar y sentir de determinada manera*” y pueden ser positivas o negativas. Lo que viene a significar que la actitud está relacionada con los gustos y las preferencias.

Indagaremos en el comportamiento y las razones que tienen los alumnos de las Escuelas TIC de la UPV para actuar como lo hacen en el terreno de esta investigación, y para ello recurriremos a las herramientas más actuales disponibles, enriqueciendo nuestra formación y buscando el soporte que sea conveniente.

1.2 Objetivos de la investigación

Esta tesis versa sobre aspectos de “Seguridad en internet”, con especial atención a las “Redes Sociales”; es decir, a la más comúnmente denominada Web 2.0.

El desarrollo e implementación de todo avance tecnológico (los rayos X, el automóvil, la aeronáutica, la desintegración del átomo, etc.) conllevan un “lado oscuro” que es necesario asumir, medir y controlar para minimizar sus posibles riesgos. La formación de usuarios y la adopción de medidas preventivas, deberían ser prerequisites para su explotación, máxime cuando se universaliza, como es el caso de internet.

El objetivo fundamental de nuestra investigación consiste en conocer el grado de sensibilidad y puesta en práctica de los conocimientos adquiridos en sus estudios (aptitud) por parte de los alumnos de las escuelas de Telecomunicación e Informática de nuestra Universidad, a la hora de salvaguardar su información y privacidad cuando navegan por internet, con la inquietud suficiente (actitud) como para protegerse adecuadamente, y cuáles son los factores que les hacen comportarse de la forma en que lo hacen. Ellos serán los futuros profesionales que formarán, desarrollarán y aplicarán estas tecnologías en empresas o instituciones, con prácticas seguras.

Nos centraremos fundamentalmente en el estudio de aquellas acciones que designaremos como “fronterizas”, al ser no provocadas directamente por los ciberdelincuentes, sino más bien las que les facilitan la labor y permiten actuaciones no deseadas, carentes de ética y en algunos casos ilegales. Propiciadas por las posibilidades actuales de la Tecnología, puestas a disposición de los usuarios generalistas e incluso facilitadas por los propios fabricantes de software (Díaz, 2008).

Indagaremos sobre los Factores Críticos (conocimientos técnicos, hábitos, metas, motivaciones psicológicas) que, tanto en el ámbito de su actividad de aprendizaje como en el de su vida social, determinan la adopción de medidas de seguridad por parte de los alumnos de tecnologías TIC en los Centros formativos de nuestra Universidad, al usar herramientas Web 2.0. Para conseguirlo (Lahey, 1999), nos plantearemos preguntas como:

- ¿Cuáles son los factores de la actitud y la motivación que tienen mayor influencia sobre los conocimientos sobre seguridad informática necesarios?
- ¿Es posible lograr un cambio en la actitud de los estudiantes?

Lamentablemente, siempre ha habido y seguirá habiendo gente sin escrúpulos que basa su beneficio en el aprovechamiento de los demás, no dudando en utilizar métodos delictivos. Internet también acaba siendo un foco de gran atracción para este tipo de personajes que, con una formación tecnológica avanzada, acceden a un potencial muy elevado de posibles víctimas. Más aún, incluso sin ser objetivo concreto de los ciberdelincuentes, dar información sobre nuestros anhelos, relaciones o inclinaciones puede volverse contra nosotros al facilitar la construcción de perfiles que acaben permitiendo manipular nuestra conducta, privada, profesional, o como consumidores.

Se estudiarán las recomendaciones más adecuadas al escenario real que faciliten la protección de los usuarios de la Web 2.0 y ayuden a perseguir actuaciones ilícitas, teniendo también en cuenta la diferencia legislativa existente entre los diferentes países.

Ese es, básicamente, el fin de esta investigación, poner de manifiesto algunas prácticas, no necesariamente muy sofisticadas pero que, acostumbrados a encontrarlas en el día a día, acaban pareciendo normales para los usuarios, sin tener en cuenta que están vulnerando los derechos que las leyes nos otorgan, evidenciando la distancia entre el legislador y el tecnólogo, máxime en una época en la que con la gran difusión de las redes sociales y la Web 2.0, es más fácil conseguir y compartir datos personales. Además de la aparición de un nuevo factor de riesgo como es el nuevo tipo de acceso desde dispositivos móviles.

Es decir, básicamente nuestros objetivos serán los siguientes, resumidos en el siguiente cuadro:

Tabla 1. Objetivos de la investigación

<p>Objetivo general</p>	<p>Conocer si los alumnos de Escuelas TIC (Telecomunicación e Informática) adoptan suficientes medidas de seguridad cuando navegan por Internet en general, y Redes Sociales en particular, cuidando su información y su privacidad (diseño del perfil, publicación de datos personales, manifestarse abiertamente).</p>
<p>Objetivos específicos</p>	<p>Verificar si los alumnos son cuidadosos con la protección de sus ordenadores, accesos y datos (uso de contraseñas y copias de seguridad, almacenamiento de la información, actualización de conocimientos y recursos de seguridad, actividad realizada).</p> <p>Saber si hay diferencias entre los alumnos más cuidadosos en la protección de sus datos y su privacidad respecto el nivel de sus conocimientos</p> <p>¿Cuáles son sus motivaciones para hacerlo de una u otra forma?</p> <p>Saber si hay diferencias en los factores motivacionales a la hora de adoptar medidas de seguridad entre alumnos con mayores o menores conocimientos.</p> <p>¿Es suficiente el nivel de precaución adoptado, basado en su aprendizaje, o es conveniente mejorar ambos?, ¿Qué factores habría que estimular para conseguirlo?</p> <p>¿Los resultados de la formación recibida cubren esta finalidad o habría que replantearla?</p>

Fuente: Elaboración Propia (EP)

1.3 Estructura: contenido por capítulos

Pese a la necesaria compartimentación en capítulos de la presente tesis, el lector encontrará un hilo conductor que le permitirá conocer desde los orígenes que generaron la inquietud de acometer esta investigación, permanentemente alimentada por el auge de noticias que a lo largo de estos años no han hecho más que enervarnos al comprobar el crecimiento de los riesgos de seguridad al navegar por redes sociales, hasta las recomendaciones finales basadas en los resultados obtenidos. Pasando, por supuesto, por todos los eslabones exigidos en toda investigación científica.

Esa “aparente” estanqueidad puede parecer que indique cierta independencia entre unos contenidos y otros. Nada más lejano de la realidad. Vamos a hacer un recorrido que recoja la situación global de seguridad en internet en general, y al navegar por redes sociales en particular, dando la información suficiente sobre los aspectos fundamentales que competen a la investigación (protección, privacidad, identidad digital). Describiremos los principales obstáculos que encontramos para garantizar un uso seguro de las herramientas TIC, la brecha digital e incluso algunos desarrollos tecnológicos sobre manejo masivo de datos que pueden tener un uso indebido, teniendo en cuenta las distintas legislaciones existentes, que deben servir para proteger a los ciudadanos, aunque también mencionaremos algunas de las razones para sus diferencias.

Seguiremos continuamente las recomendaciones de investigadores que nos antecedieron en estudios similares, referenciando sus descubrimientos, para que en todo momento mantengamos la certeza de mantenernos con el rumbo correcto que nos lleve a interpretar y consensuar nuestros resultados. Máxime teniendo en cuenta que deberemos apoyarnos en conceptos no físicos, como son las motivaciones y las actitudes, ante determinados comportamientos.

Aseguraremos cada paso que demos, afianzando cada peldaño de nuestra investigación, confirmando y reconfirmando los diferentes análisis, para garantizar que los resultados son coherentes y no son fruto de un análisis coyuntural.

En el primer capítulo, la Introducción, se describen los motivos que nos impulsaron a acometer el estudio, tanto de inquietud personal como de responsabilidad docente y curiosidad científica.

También se indican los objetivos de la presente tesis centrándonos en los aspectos que se van a desarrollar sobre la situación general que se puede percibir del tema de nuestro estudio a través de cualquier canal de comunicación, sean medios de masas, informes empresariales, institucionales o experiencias personales o cercanas, demostrando la relevancia de la investigación sobre medidas de seguridad en internet, y sobre redes sociales.

El segundo capítulo, Marco Teórico, nos ayuda a posicionarnos sobre el núcleo de la investigación aportando información sobre datos de seguridad informática actuales y su implicación en el desarrollo de la red, tanto a nivel particular como empresarial o institucional, con referencias a formas de vulnerar la intimidad.

Se relacionan los conceptos más actuales, con los informes aparecidos más recientes, que generan incertidumbre incluso a nivel judicial en la defensa de derechos fundamentales de los ciudadanos.

Se reseñan los hitos que, desde una perspectiva global, hay que controlar para que aún sirviendo al desarrollo de la Sociedad de la Información, no se coarte la libertad individual.

Indicamos una serie de estudios previos, sobre factores comunes a todo tipo de aprendizaje, que nos permiten definir los factores idóneos, herramientas y modelos con los que vamos a trabajar en nuestro caso. Hemos incluido también referencias de investigaciones más específicas que nos sirven de soporte para la nuestra que, aunque sea muy concreta al ceñirse a una población determinada de nuestra Universidad, marcha en paralelo con estudios realizados en otras partes del mundo, con otras poblaciones, respecto otras materias, pero que convergen sobre inquietudes similares. En este punto, hemos introducido los conceptos que, más cercanos a las Ciencias Sociales y la Pedagogía, nos son menos afines a los profesionales de las ramas de Ingeniería.

El capítulo tercero, sobre el Modelo Propuesto utilizado en el estudio, está dedicado a la descripción de las relaciones utilizadas entre los diferentes perfiles de alumnos que nos servirán como base para su desarrollo y ajuste, en donde definimos las hipótesis sobre las que versará nuestra tesis.

El cuarto capítulo, Metodología, describe las actividades realizadas y sus plazos, la forma de obtención de la información, su proceso y tolerancias.

Hacemos un recorrido que justifica las razones de la adaptación de los Cuestionarios utilizados y sus características, así como las Escalas de medición utilizadas y las Encuestas llevadas a cabo.

Detallamos las etapas previas, las pruebas, su fiabilidad y validez estadística, la forma de seleccionar la muestra, sus márgenes, la codificación de los datos y los criterios de filtraje de los mismos.

Describimos algunos de los conceptos metodológicos y estadísticos, así como los recursos con los que vamos a procesar nuestros datos, de forma que nos sirva de posicionamiento y concreción sobre herramientas e indicadores menos habituales, como son los de las Ecuaciones Estructurales, con un mayor detalle en uno de los anexos (2E).

El quinto capítulo muestra los resultados obtenidos, su tolerancia y aceptación, así como los modelos alternativos que se proponen y su justificación.

Partimos de un estudio de frecuencias, tablas, correlaciones, varianzas entre los alumnos del curso 2011-2012 para acabar haciendo un análisis factorial exploratorio que asociase las variables observables formando los constructos esperados. En los casos en los que detectamos falta de respuesta a alguna de las variables que formaban parte de alguna latente recurrimos a los métodos de regresión para completarla. Nos aseguramos de sus coherencias y fiabilidad mediante los respectivos indicadores. Con los resultados de este primer grupo pudimos diseñar los modelos estructurales previos que empezaron a darnos información sobre la situación general con la que actúan los estudiantes. Analizamos diversas agrupaciones de nuestra muestra con el modelo ajustado. Para ello utilizamos diversas variables de control agrupadas según comportamiento ante diversas formas de actuar y obtuvimos unos valores de ajuste que confirmaban la calidad del proceso.

Actuamos de idéntica manera con los alumnos del curso siguiente, comprobando sus estadísticos básicos, factorizando, completando ausencias vía regresión y analizando estructuralmente con la totalidad de constructos que habíamos observado en la teoría. Confirmando los resultados ya obtenidos con la primera muestra.

Finalmente, procesamos los modelos definitivos con la totalidad de alumnos encuestados en los dos cursos y propusimos un modelo alternativo que independizaba el resultado de la causalidad entre variables latentes.

En el capítulo sexto, de Conclusiones, se describe el análisis diagnóstico sobre lo que nos han mostrado los resultados, especificando los intervalos de validez y limitaciones, respondiendo a las hipótesis iniciales planteadas y sugiriendo medidas que permitan mejorar la situación puesta de manifiesto para garantizar la disminución de riesgo e incrementar la mejora del aprendizaje y del conocimiento que la sociedad espera.

El séptimo y último capítulo está dedicado a la Bibliografía, incluyendo la relación de cursos realizados en el CFP de la UPV, para adquirir y/o completar los conocimientos sobre las herramientas utilizadas para el desarrollo de esta tesis.

Se incluyen diversos tipos de anexos que aportan información adicional, de soporte y/o aclaratoria al contenido de los textos descritos en cada capítulo.

2.- MARCO TEÓRICO

2.1 Antecedentes

En los siguientes sub-apartados vamos a indicar los principios en los que debe apoyarse toda investigación científica, como guía de las etapas por las que fuimos pasando para acometerla, así como facilitaremos datos sobre la evolución de indicadores de seguridad en internet como prerequisite indispensable para tener la suficiente confianza en la Red, minimizar los riesgos al navegar por la misma y potenciar el desarrollo de la Sociedad de la Información.

Describiremos las posibilidades de la Web 2.0, en donde se desarrolla gran parte de la actividad que queremos asegurar que se realiza con la suficiente prudencia, indicando los nuevos problemas que puede conllevar un uso descuidado de la misma.

Nos centraremos en la definición y defensa de los factores personales que nos ocupan en nuestra investigación y que básicamente giran en torno a nuestra intimidad, como primer bastión indispensable para proteger imagen, bienes y libertades.

2.1.1 Bases conceptuales de la investigación

Según Albert (2007) para iniciar una investigación, siempre se necesita una idea. Las ideas constituyen el acercamiento a la realidad que habrá que investigar.

A su vez, Danhke (1989), citado por Albert, menciona distintos criterios para generar ideas de investigación productivas, indicando que las buenas ideas deben intrigar, alentar y excitar al investigador de manera personal. No es necesario que sean nuevas, pero si novedosas y deben servir para elaborar teorías y aportar solución a los problemas, así como pueden limitarse a servir para generar nuevos interrogantes.

Y todo problema de investigación debe ir pasando por las siguientes fases que lo van depurando (Albert, 2007: 43-44):

- a) Detección del problema*
- b) Elaboración del problema*
- c) Formulación del problema*
- d) Evaluación del problema.*

El planteamiento del problema consiste en afinar y estructurar más formalmente la idea de investigación (Albert, 2007). Puede llegar a ser la parte más difícil e importante de la investigación científica, pues requiere una gran iniciativa por parte del investigador, así como unos conocimientos previos sobre la materia que va a abordar y disponer de unos medios que le permitan su estudio.

No siempre podemos definir un problema de manera simple, clara y completa. Puede ocurrir que tengamos una noción general difusa e inclusive confusa sobre el problema. Puede llevarnos años de exploración y reflexión para poder definir el problema de forma inequívoca; sin embargo, enunciar el objeto de la investigación de una forma adecuada, es una de las partes fundamentales del proceso.

Este mismo autor nos dice que la selección de un problema particular depende en parte de los intereses del investigador, de sus habilidades, ingenio, creatividad y las exigencias del medio relacionadas con la situación de la investigación. El problema es esencialmente una pregunta sobre el mundo en que vivimos para la que no tenemos respuesta o las existentes no nos parecen satisfactorias; por eso nuestra investigación debe plantearse en forma de interrogante lo más concreta posible para que después sea factible avanzar una solución tentativa.

Pero uno de los riesgos que entraña toda investigación reside en la propia capacidad de delimitación del tema de estudio. Según (Tamayo y Tamayo, 2003: 117): “*Delimitar el tema es ver la viabilidad para su desarrollo. Uno de los fallos más comunes en las investigaciones consiste en la ausencia de la delimitación del tema de estudio, el 80% de las investigaciones fracasan por carecer de delimitación del tema, es decir, por ambición del tema.*”

Podemos resumir esos criterios básicos representándolos mediante las siguientes fases:



Fig .1: Fases de la investigación

Fuente: EP

Kerlinger (1999), citado por Albert, propone tres criterios para formular correctamente un problema:

1. Debe expresar la posible relación entre diversas variables, con preguntas como ¿Cuál es su relación, hay otras variables que intervengan en esa relación?
2. El enunciado del problema debe hacerse en forma de pregunta de forma clara y sin ambigüedad.
3. Problema y enunciado deben poder ser comprobados mediante alguna prueba empírica. Es decir, que las variables que enuncian una relación deben ser medidas de alguna forma.

Teniendo en cuenta estos antecedentes, vamos a describir las etapas previas por las que ha pasado esta investigación.

Durante el curso 2007-2008 desarrollé mi tesina para la obtención del DEA con el título de “*Seguridad en internet*”, describiendo las principales actividades delictivas que se estaban llevando a cabo a través de la red, así como las directrices emanadas desde la Unión Europea y las medidas establecidas a nivel país para atajarlas. También incluí ciertas posibilidades que permitían las TIC, contrarias a garantizar la Propiedad Intelectual y la privacidad, y que bordeando las leyes no eran en absoluto éticas y parecía que “escapaban” a muchas percepciones (Díaz, 2008).

Decidí dar un paso más queriendo empezar desde el principio; es decir, no dando nada por supuesto y tratando de averiguar la realidad de los conocimientos e inquietudes de nuestros jóvenes usuarios, disponiendo de una pequeña muestra como la que constituían mis propios alumnos. Basándome en mi propia tesina del Máster CALSI⁶ titulada “*Análisis de seguridad de la Web 2.0, en alumnos de la UPV*”, ya pude observar que los conocimientos, sensibilidad y actuación de los alumnos de primer curso de la Licenciatura de Comunicación Audiovisual en el Campus de Gandía de la UPV eran muy preocupantes. Parecía que podía deberse a que acababan de acceder a la Universidad, que su formación en el uso del PC era mayoritariamente autodidacta y que, procedentes de Humanidades, estaban menos sensibilizados con las potencialidades y

⁶ Máster Universitario Oficial de la Universitat Politècnica de València en Contenidos y Aspectos Legales en la Sociedad de la Información.

los riesgos del uso de unas tecnologías en las que no estaban muy seguros, como pude comprobar dándoles clase de Tecnología Digital durante varios cursos (Díaz, 2009).

Por esa razón quise profundizar todavía más en la situación real estudiando una población que ya no era novata (segundo, cuarto y quinto cursos) ni tampoco estaba alejada de los estudios más relacionados con el tema que nos ocupa, como son los alumnos de las Ingenierías Superiores de Telecomunicación e Informática.

La elección de ese perfil de alumno se debe al hecho de que, con unas asignaturas técnicas en sus respectivos planes de estudio más próximas al uso de estas tecnologías, deberán ser los mejor formados en las diferentes alternativas de su uso y de las medidas más apropiadas para la salvaguarda de sus datos e imagen.

Queremos conocer si nuestros estudiantes, supuestamente más preparados y sensibles en el uso de estas tecnologías, son lo suficientemente conscientes de la necesidad de tomar medidas autoprotectoras. Son los que algún día serán responsables de la adopción de medidas de seguridad en su actividad profesional, y queremos saber si ya adoptan esas medidas, asegurándose a sí mismos en su vida diaria.

También tenemos en cuenta que cuando el investigador inicia un nuevo estudio, no solo se basa en sus investigaciones anteriores, sino que debe conocer los trabajos de otros investigadores, lo cual obliga a estar al día en la literatura pertinente y en las informaciones publicadas, ya sea para comprobar los resultados presentados en ella o para proponerse otros problemas relacionados con su línea de trabajo. (Briones, 2002)

En definitiva, tuvimos una idea que nos intrigó pues no nos gustaba lo que percibíamos, tal como aconsejaba Albert (2007). Despertó nuestro interés y nos alentó a investigarla, como indicaba Danhke (1989). En un principio era algo difusa y no la concretamos suficientemente pero, tras años de exploración, llegamos a definirla gracias a los conocimientos previos que teníamos sobre la materia y los que habíamos ido desarrollando, así como a la posibilidad de acceso tanto a recursos materiales (disponibilidad de aplicaciones, teoría previa, cursos complementarios) como a recursos humanos (la población objetivo), pasando por las fases enunciadas por Albert (2007), pero intentando no ser víctimas de los riesgos anunciados por Tamayo y Tamayo (2003) respecto la delimitación de la investigación.

Así pues, en nuestro estudio decidimos aplicar los pasos del método de investigación científica de Asimov que puede considerarse el método por excelencia (Asimov, 2010) que consiste en:

- detectar la existencia de un problema, identificándolo, y que en general puede corresponder a la propia inquietud del investigador como consecuencia de la observación y los conocimientos previos que, sobre la materia, se tengan.
- Obtener información sobre el tema objeto de estudio, separando y desechando los aspectos no esenciales. Para poder abordar el estudio del problema desde el punto de vista científico, hay que tener la suficiente información sobre ese tema. Parte de esa información será consecuencia del conocimiento que ya tengamos (nuestra propia experiencia) y que deberemos completar con el estudio de la bibliografía existente al respecto.
- Reunir datos que incidan sobre el problema, mediante la observación simple.
- Elaborar una descripción general provisional que los describa de la forma más simple posible: un enunciado breve. Esto es, plantear las hipótesis. Con toda la información recogida y analizada estaremos en condiciones de plantear posibles conjeturas como respuesta a nuestros interrogantes. Estas conjeturas, o hipótesis, nos irán orientando en la dirección de las metas que trataremos de obtener.
- Con las hipótesis se pueden predecir los resultados de experimentos no realizados aún y ver con ellos si la hipótesis es válida.
- Verificar las hipótesis. Si los experimentos funcionan, se pueden convertir dichas hipótesis en nuevas teorías. Para lograr dicha verificación deberemos seguir unas pautas tales como:
 1. Observar la realidad, midiendo sus aspectos más relevantes y registrando la información obtenida.
 2. Reflexionar sobre los resultados obtenidos, analizarlos, estudiar desviaciones, causas, y correcciones

3. Comprobar, experimentando si lo que nos indican nuestras reflexiones coincide con la realidad
4. Actuando, de acuerdo al conocimiento adquirido lo que, en definitiva, conforma el método experimental.

2.1.2 Seguridad global en internet

El hecho de ser una red abierta permitiendo que cualquier ordenador independiente, o constitutivo de una subred, pueda conectarse sin más coste que el de la conexión ha facilitado la rápida extensión de internet y la popularización de la Sociedad de la Información. Pero esta apertura, que ha fomentado la incorporación de muchísimos usuarios, ha servido para atraer también a personas con intenciones poco éticas que han visto una oportunidad para llevar a cabo sus fechorías.

La generalización del uso de las nuevas tecnologías pasa por garantizar a los usuarios la confianza en las mismas y su seguridad (COMSI, 2005).

El fenómeno de la seguridad ha ido evolucionando incluyendo factores políticos, económicos, ecológicos, tecnológicos, sociales y/o culturales. Las posibilidades de la tecnología interfiriendo comunicaciones electrónicas, fundamento de la Sociedad de la Información, pueden entrar en colisión con conceptos tales como la intimidad, o la inviolabilidad de las comunicaciones, o con el acceso a secretos industriales que incluso puedan afectar a la seguridad de las naciones.

Un ordenador conectado a internet puede tener el mismo software que otro ordenador aislado pero es más vulnerable al poder ser accedido desde la red. El riesgo aumenta ya que la propagación de la explotación de una vulnerabilidad es muy rápida en internet.

Muchos de los problemas que plantean los usuarios respecto internet se han relacionado con asuntos como las infecciones por virus, los programas espía y la falta de confidencialidad, siendo el virus informático el más temido por los resultados que puede provocar. En Europa (FUNTEL, 2007: 99) cerca del 30% de las empresas manifestó haber detectado algún problema de seguridad con respecto a virus, lo que demostraba el escaso nivel de prevención, ya que se podía disponer de una gran variedad de programas antivirus para proteger los sistemas. Con datos del estudio del siguiente año, se puede observar en la Figura 2 la evolución de la incidencia de estos ataques en los países europeos (FUNTEL, 2008: 258).

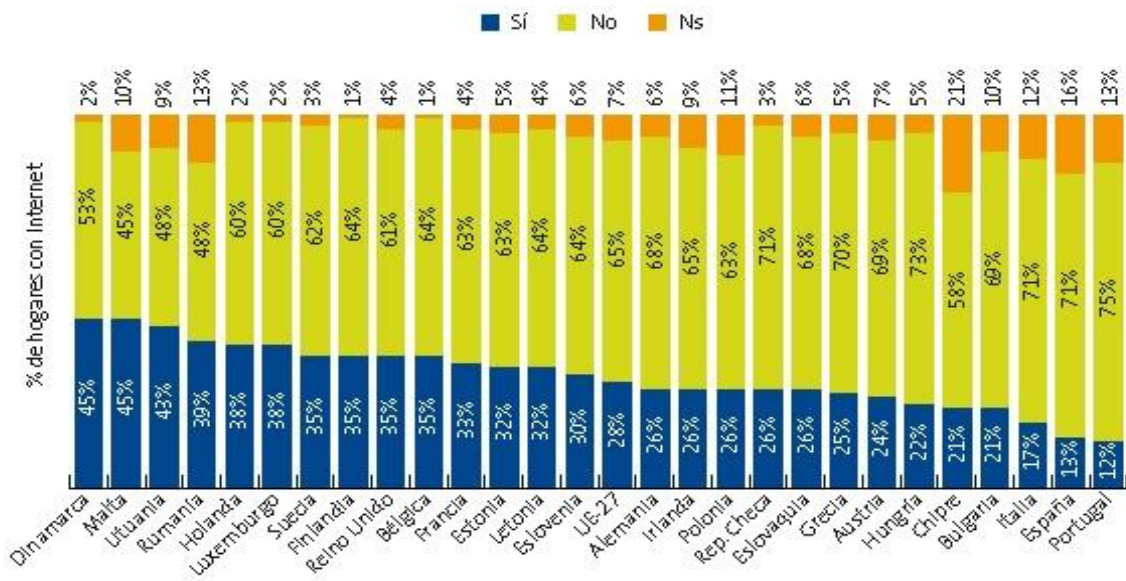


Fig. 2: Problemas por ataques de virus, infecciones por spyware, o spam, en 2007 (UE-27).

Fuente: EUB (2007)

En nuestro país, las medidas de seguridad que aportan antivirus y firewalls son comunes a todas las empresas, si bien otro tipo de medidas más cualificadas se encuentran en las de mayor tamaño, como puede verse en el siguiente gráfico.

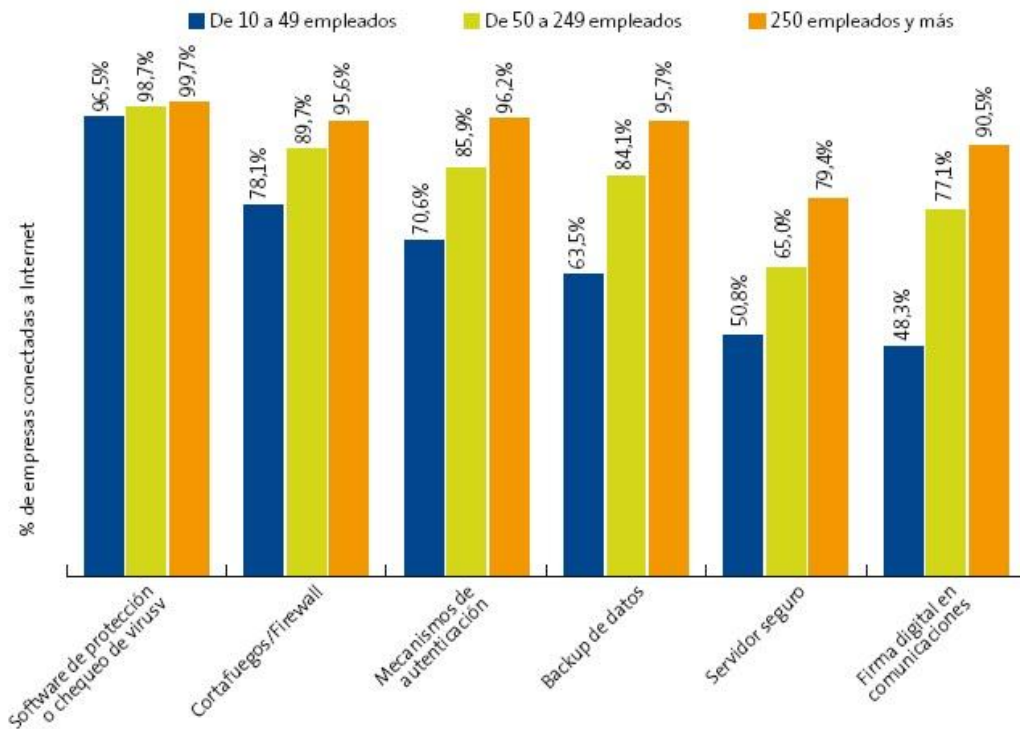


Fig. 3: Comparativa de medidas de seguridad en empresas, según tamaño (España)

Fuente: FUNTEL (2009: 257)

Sin embargo las empresas más grandes son las que sufren los mayores ataques por virus e intento de fraude económico (FUNTEL, 2009)

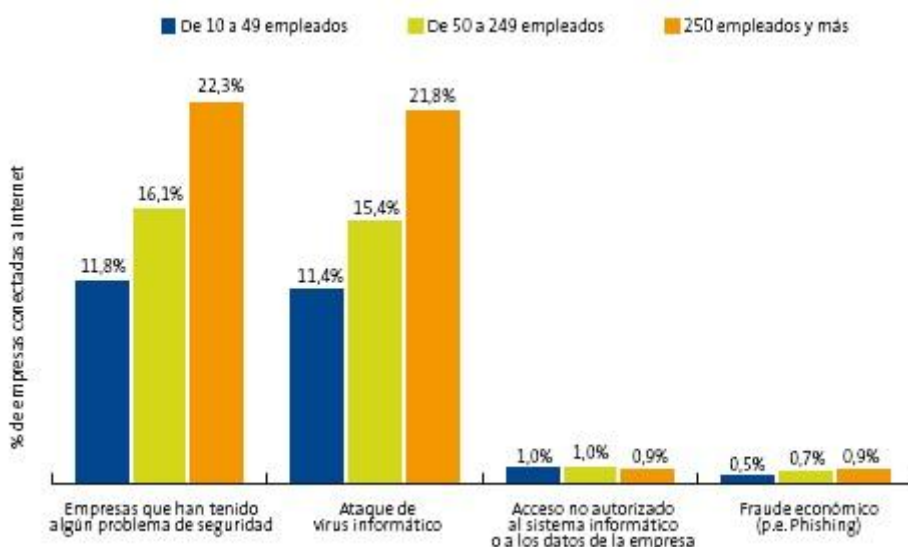


Fig. 4: Comparativa de incidencias de seguridad en el último año en empresas

Fuente: FUNTEL (2009: 256)

Otro de los factores esenciales para el desarrollo de la Sociedad de la Información es la confianza de los usuarios en internet, basada en el respeto a la privacidad de los datos personales y las garantías sobre la seguridad de los mismos.

La falta de confianza constituye un obstáculo importante para el crecimiento de la gestión de información y el comercio electrónico en la red. El dato positivo que favorece el crecimiento del B2C pasa por ese incremento de la confianza en los medios de pago vía internet al descender los desconfiados desde el 35,2% en el 2005, al 16,3% en el 2008 en nuestro país y continuar incrementando la cifra de negocio por la red en el 15,9% en 2009, sobre el 2008, o en el 23,1% en 2011 sobre 2010 pero aún lejos de la media europea (FUNTEL, 2011 y 2012).

La confianza incrementa la presencia de las empresas en internet, con independencia de su tamaño, y una adecuada usabilidad de la web y su personalización colaborarán en su éxito (Oltra, 2003).



Fig. 5a: Penetración del Comercio electrónico en Europa

Fuente: Eurostat. Datos de 2010. (FUNTEL, 2012)

Con importantes avances en los siguientes ejercicios, como puede comprobarse al comparar con la siguiente figura, incluida en el informe de Telefónica (FUNTEL, 2013)

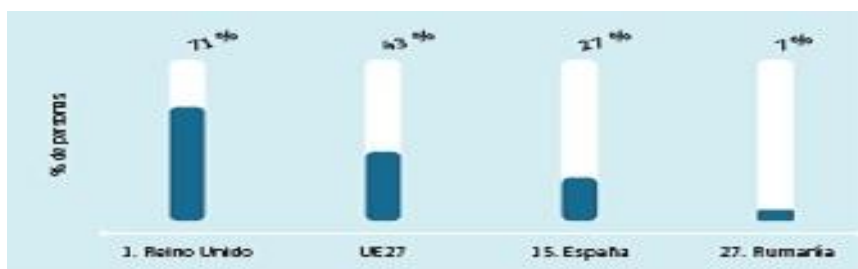


Fig. 5b: Penetración del Comercio electrónico en Europa

Fuente: Eurostat. Datos de 2012

así como su evolución durante los cuatro últimos años en nuestro país (FUNTEL, 2014).
































Fig.6: Evolución trimestral del Comercio electrónico en España

Fuente: CMT (2013)

Sin embargo, cuando la Comisión Europea realiza una encuesta preguntando si la preocupación por los problemas de seguridad ha hecho cambiar las contraseñas en el último año en los diferentes servicios descritos en la tabla 2, nos encontramos que, en nuestro país, los porcentajes siempre están por debajo de la media europea.

Tabla 2. ¿Cambió su password durante el último año para acceder a esos servicios?

		Web-based e-mail	Online social networks	Online banking websites	Shopping website (e.g. travel agents)	None (SPONT.)	Don't know	Total 'Has changed'
	EU27	31%	26%	20%	12%	50%	2%	48%
	BE	36%	30%	12%	9%	45%	2%	53%
	BG	16%	26%	5%	4%	67%	1%	32%
	CZ	32%	14%	24%	6%	51%	1%	48%
	DK	33%	27%	24%	17%	52%	0%	48%
	DE	27%	19%	18%	13%	55%	4%	41%
	EE	31%	25%	51%	8%	29%	5%	67%
	IE	28%	26%	14%	12%	53%	2%	45%
	EL	26%	33%	6%	5%	56%	1%	43%
	ES	20%	21%	11%	7%	61%	2%	37%
	FR	31%	24%	25%	10%	51%	1%	47%
	IT	28%	28%	14%	10%	47%	3%	51%
	CY	25%	26%	10%	8%	60%	1%	39%
	LV	29%	26%	50%	6%	27%	2%	71%
	LT	30%	23%	43%	9%	40%	2%	58%
	LU	45%	33%	29%	19%	39%	1%	60%
	HU	10%	26%	8%	4%	65%	1%	33%
	MT	32%	31%	15%	11%	53%	1%	46%
	AT	25%	23%	21%	12%	55%	1%	44%
	NL	35%	26%	37%	11%	40%	1%	59%
	PL	28%	22%	18%	7%	53%	3%	44%
	PT	29%	29%	8%	6%	57%	1%	42%
	RO	22%	23%	4%	5%	59%	6%	34%
	SI	36%	28%	15%	7%	56%	1%	43%
	SK	30%	24%	11%	4%	52%	1%	47%
	FI	48%	33%	43%	24%	31%	1%	67%
	SE	39%	29%	23%	21%	40%	1%	59%
	UK	44%	36%	32%	27%	35%	2%	63%
	HR	23%	27%	5%	4%	62%	1%	37%

Highest percentage per country	<i>Lowest percentage per country</i>
Highest percentage per item	Lowest percentage per item

Fuente: EUB (2013)

En este apartado estamos repasando la evolución de la situación general de seguridad en internet y de los ataques que con mayor frecuencia nos podemos encontrar en la red. Debido al interés de nuestra tesis, introduciremos también las implicaciones y atentados a la privacidad de las personas que se derivan de su explotación.

La RAE⁷ define privacidad de una forma un tanto ambigua como el “*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*”. En nuestro contexto, hace referencia al uso que las empresas hacen de los datos personales que les suministran sus clientes o los usuarios de los servicios que prestan. Datos que pueden recopilarse online o a través de otros sistema (formulario escrito, teléfono, etc.).

Preocupan las noticias diarias de ataques a sistemas informáticos de todo el mundo por parte de los *hackers*, preguntándonos sobre lo que podría ocurrir con nuestros datos personales si se vulnera la seguridad de los sistemas de las organizaciones a las que se los hemos dado o por si se pueden interceptar los mensajes que mandamos por la red.

El Senado español, en la Declaración de Derechos de Internet del 9/XII/99, declaró que el domicilio electrónico es inviolable y que ninguna entrada o registro podrá realizarse sin consentimiento del titular o resolución judicial (BOCG, 2003).

Pero los piratas informáticos cada vez utilizan herramientas más avanzadas y complejas para crear códigos malignos. El número de virus (gusanos y troyanos) que descubrían información confidencial era mayoritario (casi un 75% de los principales virus) y también aumentaba el número de spam y programas malignos que instalan “adware” para la exhibición de publicidad en el navegador del ordenador del usuario y programas “spyware” que además ocupan capacidad de procesamiento donde se instalan. Entre las diferentes formas de Spam, destacamos el Correo electrónico, el Spam por ventanas emergentes (Pop ups), Phising, Pharming⁸, Hoax, Scam⁹, y el Spam en el móvil. (FUNTEL, 2005: 284).

⁷ Real Academia Española de la Lengua

⁸ Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio a otra máquina distinta

⁹ Scam son estafas por correo electrónico o sitios web que ofrecen un producto o servicio falso

Hace unos años los ataques eran generalizados y trataban de interferir en el rendimiento de los ordenadores para obtener el reconocimiento de su entorno. Posteriormente, se centraron más en conseguir datos críticos de los usuarios (propiedad intelectual, identificaciones, dinero, etc.) para lucrarse y dañar la imagen de marca de una empresa o sus clientes (FUNTEL, 2008).

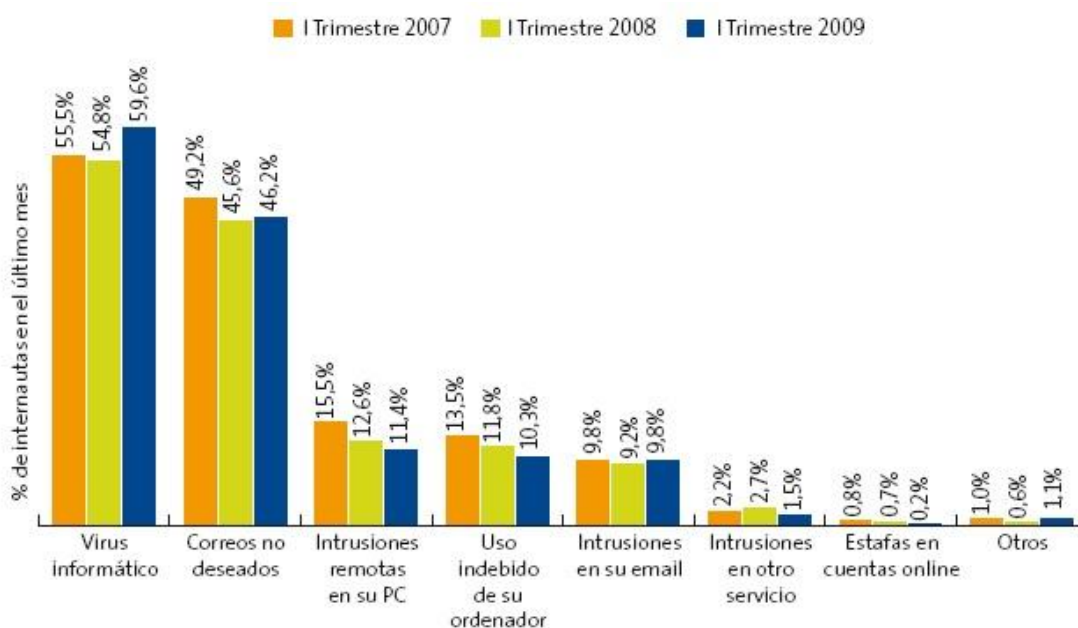


Fig. 7: Internautas con problemas de seguridad en España (último mes)

Fuente: FUNTEL (2009: 253)

Podemos leer en Bit (2008), que la división de seguridad de la Compañía de protección de datos EMC informaba en diciembre de 2007 que España era el tercer país del mundo que más intentos de fraude por internet había sufrido, concentrando el 7 % del total a nivel mundial, solo superada por EE.UU. y UK. Ese año los casos de phishing crecieron un 66% en todo el mundo. La mayoría de los intentos procedían de EE.UU. (44 %), Japón (16 %) y China (12 %).

Es decir; unido a las ventajas de las TIC, todos los sectores de la sociedad se enfrentan a mayores amenazas que ponen en riesgo su estabilidad y crecimiento.

En consecuencia, la denominada “**ciberseguridad**” ha pasado a ser un asunto prioritario en las agendas políticas, tanto nacional como internacional.

Las comunicaciones comerciales realizadas por carta o teléfono son más fáciles de interceptar que las comunicaciones a través de internet, pues realizar actividades delictivas por este medio requiere unos conocimientos técnicos sofisticados que no están al alcance de cualquiera pero también hay que tener en cuenta que las posibilidades de protección de las comunicaciones electrónicas son mayores que las que permiten los medios tradicionales. El problema estriba en que no hay una “cultura” de la seguridad en internet de la misma forma que sí la hay en la vida cotidiana. Fuera del mundo virtual seguimos una serie de normas básicas para prevenir cualquier ataque o fraude, como cerrar la puerta de casa o del coche al salir y no dar publicidad a nuestros datos personales. Sin embargo en internet hay carencias en este tipo de hábitos.

Una estafa siempre será una estafa, se realice por el método que se haga. Variará la forma de llevarla a cabo y si en tiempos pasados el famoso “timo de la estampita” se repitió una y mil veces sorprendiendo a incautos cegados por la avaricia, hoy en día se utiliza el phishing para desvalijar a unos nuevos incautos, sorprendidos en su buena fe.

Al popularizarse las nuevas redes sociales, nuestras listas de contactos se hacen públicas (Facebook), nuestra imagen circula por la red (Flickr), o nuestros vínculos familiares (Genoom). Se puede atentar contra nuestra privacidad cruzando mucha de esa información, llegándose incluso a la posibilidad de la suplantación.

El uso diario de recursos universales como las redes de acceso abiertas incrementan las posibilidades de acceso a nuestros perfiles y los ataques contra entre el 20 y el 30 % de las redes inalámbricas no protegidas por ninguna contraseña, a las que se puede usurpar parte de su ancho de banda utilizando programas rastreadores de señal (FUNTEL, 2007).

Hay que tener también en cuenta que internet crece sin que las legislaciones estén preparadas para este rápido crecimiento. Si bien es cierto que las leyes y las necesidades de regulación siempre van por detrás de la realidad, en el caso de la red este hecho está más agudizado. No solo por la rapidez de la evolución tecnológica sino también porque se hace necesaria una regulación que sobrepasase las fronteras de los países.

De hecho la gran paradoja de internet es que mientras que las leyes están vinculadas a un territorio geográfico, el acceso a la información no.

Muchas de las explicaciones a las cifras relacionadas con los problemas de seguridad hay que buscarlas en la formación de los usuarios y los hábitos adoptados en cuanto a la toma de precauciones de seguridad TIC. Sáez Vacas (2004: 349) confirma la declaración de un famoso hacker (Kevin Mitnick) en ese sentido: *“Las medidas técnicas sobre seguridad no pueden evitar a menudo las brechas y negligencias de la propia organización humana que se sirve de la Red Universal Digital”*.

Se puede conseguir información sobre construcción de explosivos en diversas páginas web indicando “bombas caseras” en Google o en Youtube, con foros para aclarar dudas, como (<http://www.foro3k.com/rincon-boludisima/155892-tutorial-bombas-potentes-caseras-ojo.html>), ofrecimientos de madres de alquiler, venta de productos sin ningún tipo de control (farmacéuticos, por ejemplo), contratación de sicarios (<http://centroceremialotomi.metroblog.com/>), presión para extender anorexia y bulimia, suplantación de personalidad, reclutamiento para asociaciones poco recomendables, información sobre claves de acceso a programas de Pay per view, instrucciones para invalidar la protección anticopia en soportes digitales, distribución de imágenes tomadas sin consentimiento, ni conocimiento de los involucrados, p.e., en playas (http://www.ziza.es/2007/04/10/Chicas_en_la_playa_42_fotos.html), o centros nudistas (<http://ovejaneira.peru.com/temas-libres-12-mejores-playas-nudistas-mundo-fotos-267791>), o simplemente “pilladas” descuidadas y sin su consentimiento (http://www.ziza.es/2008/07/30/Robados_en_la_playa_79_fotos.html), utilización de correos humanitarios para conseguir direcciones activas, golpes mortales (<http://adictamente.blogspot.com.es/2013/04/22-golpes-mortales-para-la-defensa.html>), cómo forzar cerraduras con la excusa de ayudar a propietarios con problemas de acceso a su vivienda (<http://es.wikihow.com/forzar-una-cerradura>), etc., son algunos de los contenidos que pueden obtenerse a partir de la red y cuya persecución es difícil, máxime si se ubican en servidores de países con legislaciones laxas en la materia.¹⁰

Siendo evidente la sensibilidad de los datos personales, lo es más aún la privacidad de las conversaciones que a través de la red mantienen los internautas. Se trata de la misma privacidad que protege a las conversaciones telefónicas entre abonados, donde se abordan contenidos de relaciones sociales, amistosos, de amor/odio, sexuales,

¹⁰ El contenido de las direcciones referenciadas en este párrafo, ha sido comprobado el 19/III/15

discusiones religiosas y/o políticas, familiares, de salud, consejos ... en las que solo un juez, y por razones suficientemente justificadas, puede autorizar su escucha y grabación.

Sin embargo, si no hemos configurado adecuadamente el perfil de acceso a determinada información a través de las redes sociales, pueden quedar expuestos todos nuestros comentarios. De hecho, en España, el nivel de preocupación sobre la falta de seguridad de la información personal en línea, tanto de los propios sitios web como de las medidas generadas por la Administración, son de las más altas de la Unión Europea tal como podemos comprobar en las figuras siguientes

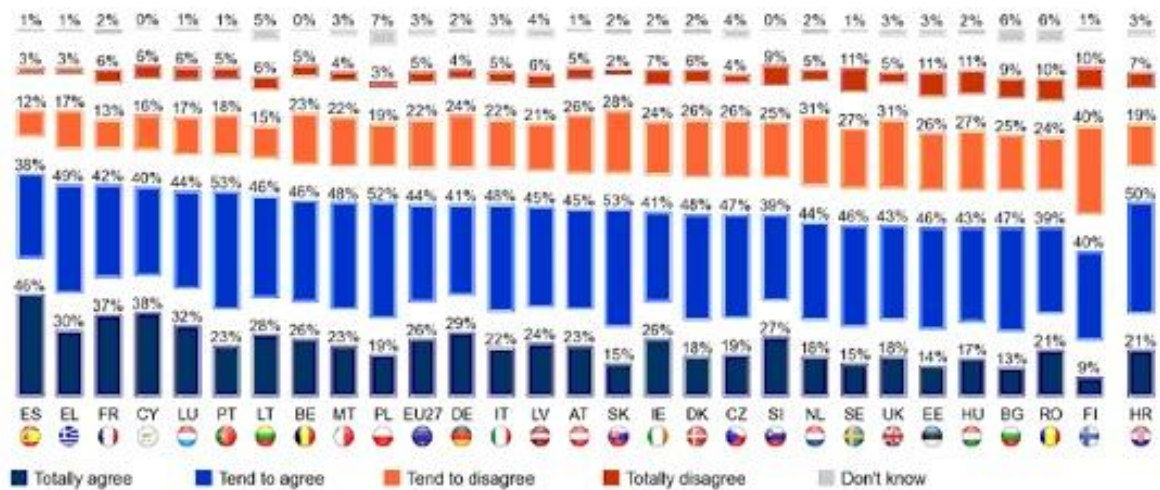


Fig. 8a: Percepción sobre la falta de protección de privacidad en los sitios web

Fuente: EUB (2013)

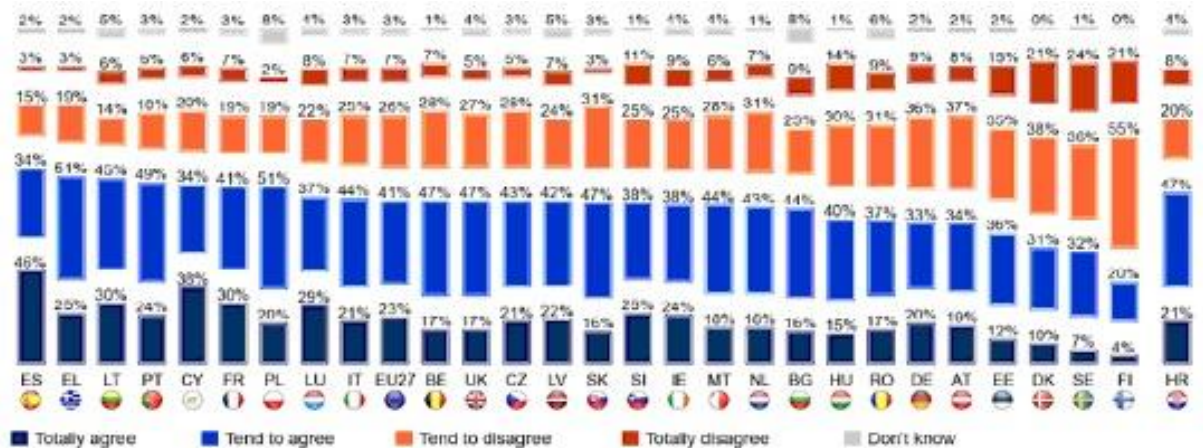


Fig. 8b: Percepción de que las autoridades no protegen la privacidad suficientemente

Fuente: EUB (2013)

Así como en un principio había unas normas de autorregulación sobre los contenidos en la red, sin necesitarse unas normas escritas al respecto, con el paso del tiempo y el incremento de las potencialidades económicas se desvirtúa aquella filosofía inicial y con el aumento exponencial de contenidos, aumenta el número de posibles nuevas problemáticas (López, 2005).

En la informática clásica de las décadas 70 y 80, utilizando el concepto de la autorregulación, el departamento de informática de cualquier empresa sabía que tenía que permitir el acceso a las diferentes bases de datos a los interesados y legítimos usuarios de cada una de ellas: el dpto. de Personal a los datos de los empleados, Marketing a los clientes, Tesorería a bancos, Finanzas a contabilidad....

Muy posteriormente, España legisló en este campo y anunció la LORTAD (Ley Orgánica 5/1992, de 29 de octubre del Tratamiento Automatizado de los Datos de Carácter Personal), estableciendo los niveles de protección de las distintas bases de datos y legislando también sobre qué autoridades podían exigir la entrega de datos.

Con posterioridad, la LORTAD fue sustituida por la LOPD (Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal) al adaptarse al ámbito europeo (ESPAÑA, 1999), que entiende como personal a cualquier información gráfica, numérica, alfabética, fotográfica, sonora o de cualquier tipo referidos a personas identificadas o identificables, otorgando derechos de acceso a los datos, a su rectificación, oposición o cancelación y que cumple con la normativa relativa a la transferencia internacional de datos, permitiéndola siempre que se haga a países de la Unión Europea o a terceros países con el nivel de protección equiparable al que se establece en el marco europeo.

Pero no es fácil impedir cruzar toda la información que sobre los individuos circule por las redes sociales, así como mantener las defensas de la red sobre el software malicioso que se propaga a través de los nuevos dispositivos de acceso móvil, menos protegidos.

No obstante, durante el periodo de 2010 en el que nuestro país ostentó la Presidencia de la UE se aprobó la Agenda Digital Europea (ADE, 2010), pilar de la estrategia EU2020 que persigue el crecimiento económico de la eurozona apoyándose en las TIC para el desarrollo del empleo, la sostenibilidad y la inclusión social.

Uno de sus objetivos es fomentar el uso avanzado de internet, salvaguardando el carácter abierto de la red e incrementando una Economía Digital Europea y el uso generalizado de las TIC en Educación, así como promover una concienciación pública sobre los riesgos de la seguridad on-line para conseguir una cultura de protección de datos y privacidad que capacite a los usuarios para su integración plena en el mundo digital, incrementado su confianza y habilidades para un acceso transaccional y navegación más seguras (FUNTEL, 2011).

En el objetivo de nuestro estudio no tratamos de estudiar la capacidad de nuestros alumnos respecto el hecho de poder eludir cualquier amenaza tecnológica, pero si al menos no facilitarla. Siempre hay situaciones que requieren unos conocimientos y una especialización tan alta que solo están al alcance de unos pocos. Sirvan como ejemplo de plena actualidad los siguientes casos:

- Julian Assange quien, desde WikiLeaks, difundió documentación “sensible” del Departamento de Defensa de EEUU sobre guerras en Oriente Medio, obtenida a través de accesos no permitidos (directamente o mediante connivencia con los supuestos guardianes de la misma). (RTVE, 2010)
- Edward Snowden que, a su vez, también publicó documentos de alto secreto sobre actividades de la NSA (Agencia Nacional de Seguridad) americana, denunciando el desarrollo tecnológico del “estado de vigilancia” en el que no se respeta la privacidad y la libertad en internet. (RTVE, 2013).
- Carbanak, el grupo de hackers que ha realizado el mayor robo de la historia a varios bancos, superando los mil millones de dólares. (Gutiérrez, 2015)

Estas dos referencias más la forma en la que se están realizando enfrentamientos entre naciones pueden escucharse en la página del Instituto de Ingeniería de España¹¹ en la conferencia dada por el famoso hacker Chema Alonso, en septiembre de 2013, que desvela la forma en la que el presidente Obama resolvió el enfrentamiento por el enriquecimiento de uranio, entre el gobierno iraní y la anterior administración Bush.

Otros ataques a la privacidad de los usuarios que han sido difundidos recientemente son:

¹¹ http://www.iies.es/Chema-Alonso_a3169.html [Consulta: 19-03- 2015]

- La página web “celebgate” en la que se difunden fotos y vídeos íntimos de personajes famosos, hackeados desde sus teléfonos móviles. De hecho, entre las mayores vulnerabilidades de 2014 publicadas por la revista digital ChannelBiz, del grupo NetMediaEurope, se encuentran las que afectan a este tipo de dispositivos.¹²
- La página web “insecam”¹³ que publica fotos tomadas de nuestro entorno desde la cámara de nuestro PC sin nuestro consentimiento ni, por supuesto, conocimiento

¹² <http://www.channelbiz.es/2014/12/09/fotogaleria-15-brechas-de-seguridad-registradas-en-2014/>

¹³ <http://geeksroom.com/2014/11/insecam-sitio-que-muestra-streaming-de-mas-de-73-000-camaras-web-sin-seguridad/89818/>

2.1.3 Protección de la privacidad en internet

Desde antes del fuerte desarrollo de las redes sociales ya se temía la posible pérdida de privacidad que podía suponer el imparable avance tecnológico de las comunicaciones y el proceso masivo de datos, aunque incluso se trataba de justificar.

El profesor Sáez Vacas (1991) nos alertaba sobre los riesgos de vulnerabilidad que implicaba la Sociedad de la Información y sus consecuencias sociales. Con posterioridad, el profesor Cayetano López¹⁴ vaticinaba sobre los riesgos de manipulación, trivialización intelectual, embrutecimiento, limitación de libertades, propiedad intelectual, autoría, etc. que podía significar la irrupción de las nuevas tecnologías y la necesidad de prevenirlos para poder contrarrestarlos.

Adicionalmente, Donald Tapscott¹⁵ advertía de que corríamos el peligro de la desaparición de la frontera horaria entre trabajo y ocio, generando un nuevo tipo de adicción y limitando nuestra libertad individual.

De hecho, en nombre de la libertad de expresión y de información, para la sociedad global, la intimidad se anunciaba como un valor a la baja (Cebrián, 1998).

Miguel Ángel Davara (2000: 1), en un artículo publicado sobre el humanismo tecnológico decía: *“todo el mundo navega por internet aunque, irónicamente, puede decirse que, como mucho, flotan en la Red, porque para navegar hace falta rumbo y los incontrolados accesos a Internet son, si me apura, un flotar a la deriva”*.

El problema surge por la inseguridad que proporciona la duda y el desconocimiento debidos a una falta de formación y asimilación de métodos y medios. Siguiendo con el símil, antes se “buceaba” en la información. Ahora hay tanta y tan fácilmente accesible, que nos limitamos a “surfear” sobre la misma.

¹⁴ Ex-Rector de la Universidad Autónoma de Madrid, en el prólogo de La Red (Cebrián, 1998)

¹⁵ Miembro del Foro Económico Mundial, presidente de la Alianza para las Tecnologías Convergentes, en el prefacio de La Red (Cebrián, 1998)

Tras los atentados de septiembre del 2001, EEUU decretó la *USA Patriot Act*¹⁶ que acentuó la primacía de la seguridad nacional sobre la privacidad de los ciudadanos. Siendo ese país la cuna de desarrollos y empresas tecnológicas, no nos debe extrañar que los recursos puestos a nuestra disposición mantengan esa estrategia. Derechos básicos como la intimidad ya estaban cuestionados en aras de sus estrategias de defensa.

Desde la división de productos de seguridad de International Data Corporation (González, 2007), se alertaba del riesgo de acceso a la web 2.0 al combinar las esferas privada y corporativa, en un espacio en el que no se separan ambos ámbitos de actividad y que complica la adopción de las necesarias medidas de protección para todo tipo de productos conectables a la red empresarial. En consecuencia, cada vez en más ocasiones, la vulneración de la información se efectúa desde el interior de la propia red.

Los empleados acceden a redes sociales que instalan archivos maliciosos e infectan sus propios terminales móviles, con menores medidas de protección, y los transmiten a las redes corporativas de sus respectivas empresas (Monsoriu, 2008).

La multinacional británica de seguros *Legal & General* hizo un estudio con un ex-ladrón en el que se comprobó que, siguiendo el rastro de sus potenciales víctimas a través de su actividad reflejada en las redes sociales, se reunía suficiente información para determinar el mejor momento para el saqueo de su vivienda. (Belt, 2009).

Por otra parte, entre las frecuentes recomendaciones emanadas por la Agencia Española de Protección de Datos, podemos reseñar los avisos sobre identificación como usuarios, contraseñas, no abrir mensajes de desconocidos, no aceptar descargas no identificadas, actualizar antivirus, etc., (AEPD, 2009). Campañas similares se venían realizando en otros países de la UE (BBC, 2005).

Los datos aportados por el Observatorio de la Seguridad de la Información, integrado en el *Instituto Nacional de Tecnologías de la Comunicación*, muestran una mejoría en la adopción de medidas preventivas en el conjunto de los hogares españoles a la hora de navegar por internet, si bien considera que hay que seguir manteniendo niveles

¹⁶Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

educativos que favorezcan la implantación de medidas que garanticen una navegación más segura (INTECO, 2010a).

Respecto la seguridad tradicional, dejar rastros de nuestra actividad, como vacaciones, viajes, fotos, datos geoetiquetados, etc., facilita ser víctimas de los delincuentes de toda la vida, como ladrones, extorsionadores, acosadores, etc. (INTECO, 2010b).

Investigadores del *International Computer Science Institute*, de la Universidad de Berkeley, hicieron demostraciones sobre la facilidad del seguimiento de confiados usuarios desde la información fotográfica de objetos en venta, descubriendo sus movimientos, itinerarios recorridos, dirección actual (Naone, 2011).

Con demasiada frecuencia nos llega información a través de los medios de comunicación tradicionales de los graves problemas que están surgiendo en la sociedad como consecuencia del exceso de confianza, el desconocimiento en el uso de los recursos tecnológicos disponibles y las consecuencias de alimentar las redes sociales con información personal. (Urueña, 2011). Si a la información de ocio añadimos nuestras relaciones sentimentales, laborales, profesionales, creencias, etc., corremos el riesgo de que ese conjunto de datos digitalizados se difundan fuera de nuestro control.

Comentarios inadecuados sobre el propio trabajo, virus, ciberacoso, phishing, smishing¹⁷, vishing¹⁸ o suplantación tienen una incidencia muy grave en algunos casos.

La revista del IEEE¹⁹, de reconocido prestigio sectorial internacional, destaca en una de sus más recientes portadas un artículo sobre la evolución de los recursos utilizados en internet por organizaciones que tratan de conocer nuestra actividad al navegar por la red, coartando nuestra privacidad e incrementando nuestros riesgos, para satisfacer unos fines exclusivamente lucrativos que se ven facilitados por la escasa concienciación de los usuarios (Nikiforakis, 2014).

¹⁷El smishing es un ataque de phishing mediante un mensaje SMS a través de telefonía móvil celular en el que se indica que se está cobrando un servicio no solicitado, ofreciendo una dirección en la que solucionarlo, dando claves de la cuenta bancaria.

¹⁸ El ataque de vishing se realiza desde plataformas de telefonía, copiando los sistemas de atención telefónica de los bancos para requerir las claves de acceso a cuentas bancarias.

¹⁹ Institute of Electrical and Electronics Engineers

La proliferación de teléfonos inteligentes, con mayores funcionalidades y potencia acaba siendo sinónimo de falta de seguridad, pues suponen una entrada por la puerta trasera a las redes de los sistemas a los que se conectan, incrementando los riesgos.

Las empresas imponen medidas disciplinarias a sus empleados por uso indebido de los recursos cuando acceden a los servidores profesionales a través de terminales privados de uso común o expresan abiertamente opiniones políticas, tendencias sexuales o creencias religiosas en unos soportes en los que se mezclan vida privada y profesional.

La forma de infiltrarse de una amenaza puede verse en la siguiente figura, donde queda patente que el objetivo final del cibercrimen es asaltar los centros de datos. En el caso representado, se produce una acción maliciosa en un dispositivo externo a la red corporativa que causa una infección y afecta a la red del entorno. Esa red actúa como plataforma de lanzamiento a la red de la empresa y la amenaza se abre paso hasta el centro de datos.

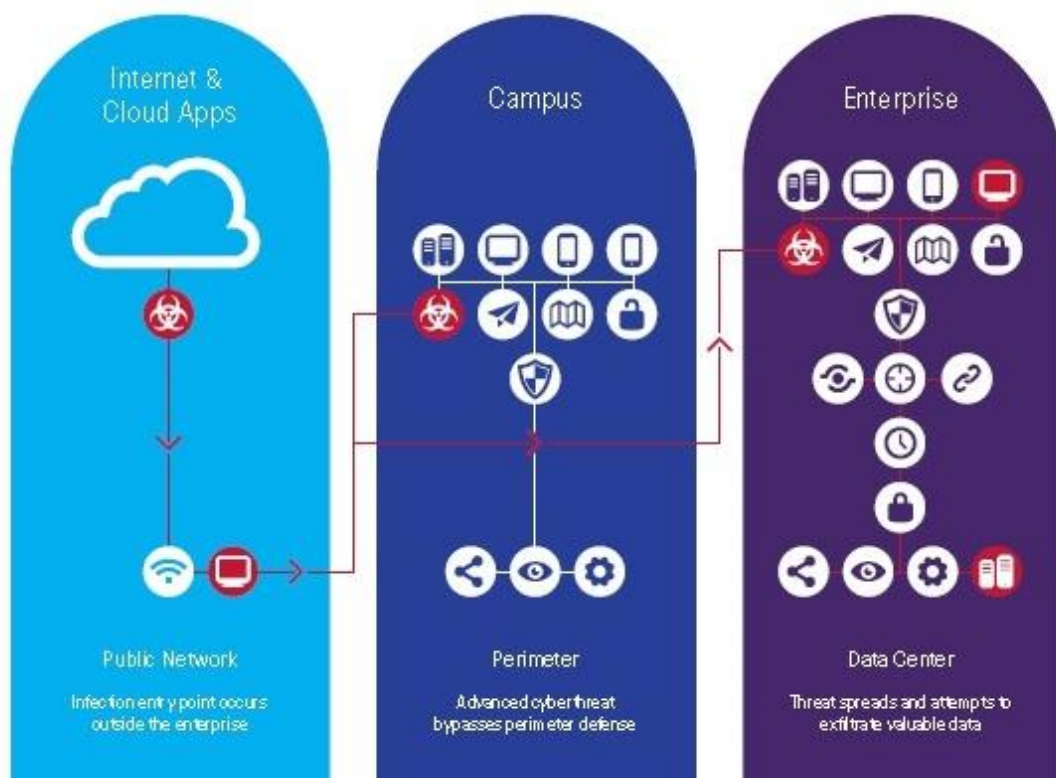


Fig. 9 Anatomía de una amenaza moderna

Fuente: Cisco (2014)

2.1.4 Seguridad en la Web 2.0: identidad digital

En su sentido más fundamental, Web 2.0 hace referencia a cualquier herramienta o aplicación distribuida por internet que permite la interacción de usuarios a través del uso compartido de contenidos. En vez de los contenidos estáticos de una página Web (1.0), ahora internet ofrece la participación y colaboración activa de los usuarios (Web 2.0).

Se puede decir que las aplicaciones de la Web 2.0 y en especial las Redes Sociales, sitios web que permiten interconectar a usuarios conocidos y desconocidos con características e intereses comunes desde cualquier rincón del mundo, están convirtiéndose en lugares de referencia para numerosos internautas.

La clave está en que con las aplicaciones de esta "2ª versión" de la Web, el usuario pasa de ser un mero receptor de información a convertirse en protagonista del Universo Internet, interactuando con contenidos, creándolos, colaborando con otros usuarios.

Entre estos tipos de aplicaciones se encuentran algunas tan conocidas como los blogs, que permiten a usuarios sin grandes conocimientos informáticos escribir sus propios "cuadernos de bitácora" o "diarios", o lo que es lo mismo, una página web personal a través de la que pueden expresarse desde su hogar para el mundo. Como derivados de éstos tenemos fotoblogs, videoblogs, webs de podcasting (blogs de audio), además de buscadores especializados, wikis (como la famosa wikipedia), aplicaciones de tagging, comunidades de videos, redes sociales personales que nos conectan con amigos y personas de nuestro interés, redes profesionales para aumentar los contactos de negocios y facilitar su gestión, además de un largo etcétera de nuevas aplicaciones.

Nuestro perfil en Redes Sociales y nuestros comentarios abiertos, los blogs personales y cualquier información de todo tipo (resultados de oposiciones, trabajos universitarios, notas, currículum, multas, noticias, altas-bajas de servicios, clubs, requerimientos, sanciones aparecidas en el BOE...) complican el equilibrio entre nuestra vida personal, familiar, social, de relación y nuestra vida profesional. Se entremezclan (figura 10) y pueden llegar a perjudicarnos en cierto modo.

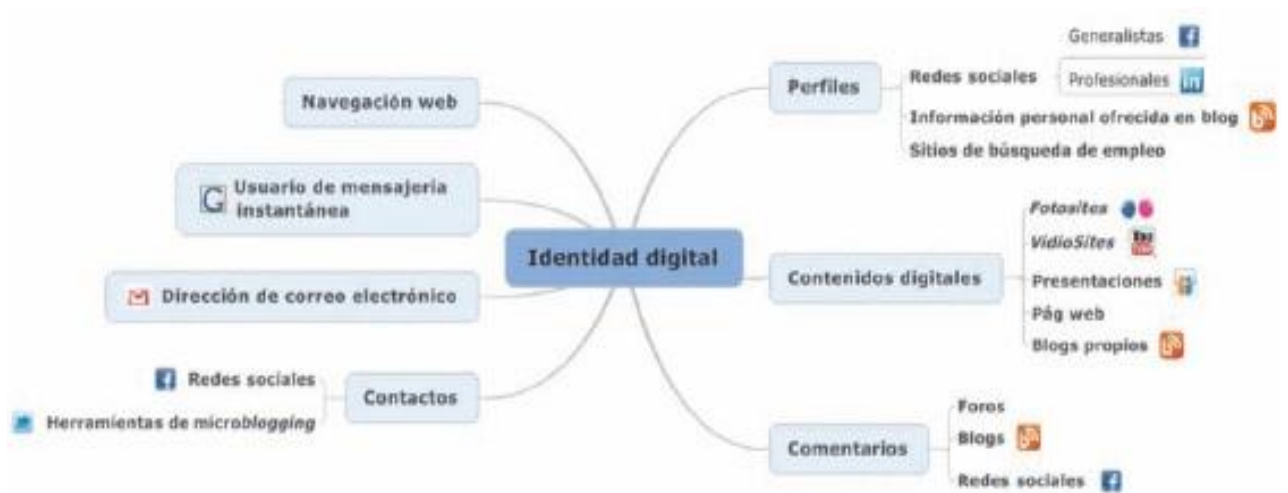


Fig. 10: Impactos en la Red que conforman la identidad digital

Fuente: Fundación CTNE (2013)

Un perfil algo radical desde el punto de vista político, manifestado en nuestro blog, puede condicionar nuestra selección para un proyecto con la Administración.

Una dedicación excesiva a determinada actividad (deportista de competición), documentada en la red, puede complicar nuestra contratación por responsables de RRHH que saben que va a ser necesaria una dedicación más allá del horario laboral habitual.

En una entrevista pueden soslayarse estos extremos pero, a través del tiempo, hemos dejado huellas suficientemente claras y profundas como para no poder eludir cualquiera de esas características de nuestra personalidad. El incremento de las capacidades de almacenamiento en memorias digitales permite disponer de datos suficientes para hacer un seguimiento de nuestra actividad puesto que al interactuar con la red dejamos rastro de fotos, textos, videos, participación en foros, compras, ventas, mensajes, correos, llamadas, reservas, etc. Datos que alimentan las grandes bases de datos que señalaremos en apartados posteriores (Sáez, 2004).

Nuestra vida analógica condiciona la imagen que damos en internet pero, también a la inversa, una vida activa en la red puede repercutir en nuestro mundo real. Lo ideal es ser homogéneos; es decir, mostrarnos de la misma forma. Ambas existencias forman parte de una misma realidad, de forma que nuestras actuaciones tanto en el mundo real, físico,

como en el virtual, la red, convergen hacia una identidad híbrida que cuasi se superponen.

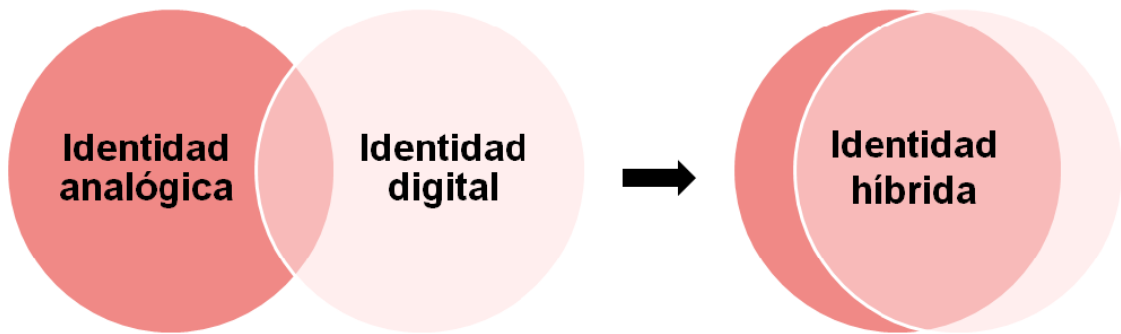


Fig. 11: Coexistencia real y virtual

Fuente: INTECO (2012)

Al interactuar en la Web 2.0, participando activamente, introduciendo comentarios y expresándonos libremente vamos tejiendo una serie de datos que conforman nuestra personalidad. Somos consumidores y productores de información para el ocio, el trabajo, los estudios, las relaciones sociales y familiares y frecuentemente para todo a la vez (Gionés-Valls, 2010).



Fig. 12: Recursos para la Identidad digital

Fuente: Gionés-Valls (2010)

Si hacemos una búsqueda de nosotros mismos a través de los motores de los potentes buscadores existentes en la Red nos encontraremos datos como nuestra edad, imágenes, actividad u ocupación, aficiones, filiaciones, estatus social y/o económico, reservas, compras, datos de contacto, amigos, contactos profesionales, residencia, direcciones de correo, comentarios que hemos colgado nosotros o que han hecho otros nombrándonos, incluso nuestra localización geográfica en todo momento a través del móvil, etc., provenientes de distintas fuentes de información como nuestro perfil en redes sociales, blogs o noticias generales.

Es decir, existe una descripción de nosotros mismos en el plano digital que, a su vez, da lugar a una reputación online u opinión que los demás usuarios tienen sobre nosotros. Estamos definiendo una “construcción social” creada de forma colectiva, basada en percepciones, y que puede tener efectos favorables o no para el protagonista (INTECO, 2012).

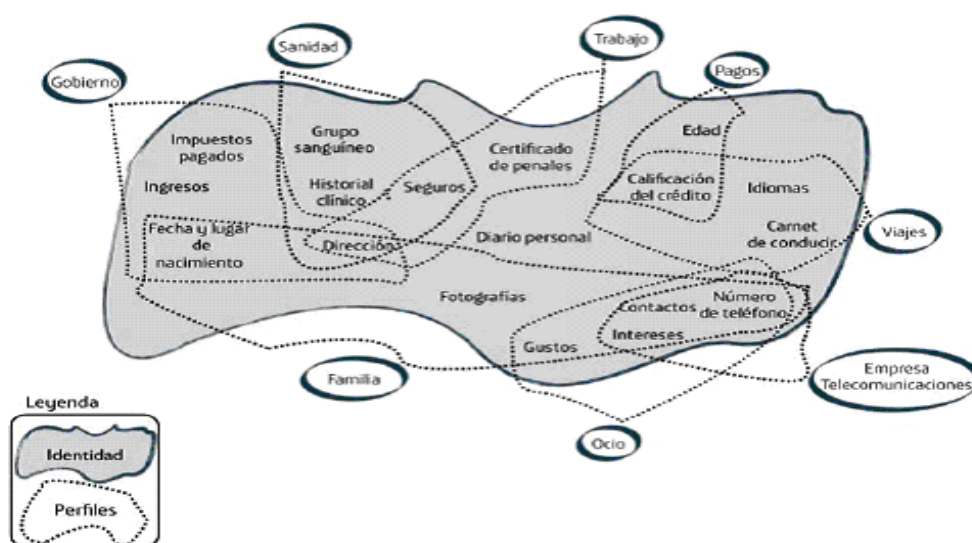


Fig. 13: Datos de los diferentes perfiles de Identidad Digital

Fuente: Fundación CTNE (2013)

La reputación es un componente clave de la identidad que refleja quiénes somos y cómo interactuamos con los demás (Solove, 2007).

Toda la información de que se dispone sobre nosotros puede ser analizada desde distintos contextos. Sitios como 123people.com ofrecen todo tipo de datos que recogen sobre la información existente en la red de una determinada persona.

La identidad digital es un concepto social y dinámico que se genera con las interacciones de los usuarios, por lo que es subjetiva y pueden construirse distintas «identidades» referidas al mismo usuario, como podemos observar en la siguiente figura

Social	Soporta los procesos de interacción social de las personas
Subjetiva	El proceso de identificación incorpora la subjetividad de las otras personas
Con valor	Permite la realización de transacciones que no serían posibles sin ella
Referencial	Se trata de una referencia a la persona
Crítica	Su uso por terceros puede implicar riesgos para la persona
Compuesta	Formada por varios elementos, tanto procedentes de la propia persona como por otros
Dinámica	Está siempre cambiando e incorporando nuevos elementos
Contextual	Según el contexto en el que se desenvuelva la persona, el perfil de la identidad digital tendrá una información u otra
Permanentemente accesible y ordenada cronológicamente	La información registrada sobre la persona se puede conservar y, por lo tanto, se puede acceder a ella de manera permanente. De hecho, en muchas ocasiones la información no puede ser borrada porque ha sido compartida con otros Por otro lado la información queda almacenada siguiendo un orden cronológico claro
Inexacta	El proceso de identificación siempre está sujeto a errores, algo que conviene tener muy en cuenta

Fig. 14: Características de la Identidad digital

Fuente: Fundación CTNE (2013)

Por otra parte, aportamos información para la identificación de pautas de comportamiento o consumo que permiten un marketing personalizado dirigido a nuestros gustos y/o capacidad económica, como puede verse en la siguiente figura



Fig. 15: Tipo de información que se distribuye en Redes sociales y sitios de compartición, en la UE

Fuente: EUB (2011)

Tras un cúmulo de datos que nos identifican individualmente o sirven para encasillarnos en algún grupo concreto, puede surgir la necesidad de modificar algunos de esos datos. En la guía de Inteco se define el llamado “derecho al olvido” como la facultad del usuario para conseguir que se elimine cierta información sobre su identidad digital.

Hay ocasiones en las que se publica información oficial sobre nosotros y se puede recurrir a los buscadores o a la propia AEPD para que se cancelen datos personales relevantes. Esta última, junto con los tribunales de la UE, persigue que la regulación europea proteja el derecho fundamental de la protección de datos e incluya el derecho al olvido. Nuevamente se da el caso de la existencia de detractores que priorizan el derecho a la información, argumentando que todo lo que hay en la red forma parte de su propia historia y, en consecuencia, no debe ser borrado, poniendo como ejemplo de información de seguridad la importancia para una comunidad de conocer si en su ámbito conviven delincuentes tipo pederastas o violadores (INTECO, 2012).

En mayo de 2014 el Tribunal de Justicia de la Unión Europea dio la razón a un ciudadano español que, con el apoyo de la AEPD, se querelló contra Google al exigir que se eliminasen determinadas referencias publicadas en distintas páginas web que afectaban a la reputación de su identidad digital.

Para lograrlo, el Alto Tribunal tuvo que resolver previamente la aplicación de la competencia de la LOPD española frente al operador norteamericano, así como considerar que el funcionamiento como proveedor de contenidos del motor de búsqueda se relacionaba con dicha ley. (TJUE, 2014).

Con independencia de los efectos concretos de esta sentencia, se inicia una jurisprudencia que obliga a las empresas americanas que dan un servicio fuera de sus fronteras a tener que acatar no solo sus propias leyes, sino también las de los lugares en los que se explota ese servicio.

Para ayudarnos a proteger nuestra identidad digital, INTECO ha elaborado una guía con recomendaciones para los ciudadanos y poderes públicos para construir una identidad digital correcta y disminuir los riesgos existentes al gestionar la personalidad online de cada uno. Esta gestión consiste en tener la habilidad de conseguir una visibilidad y reputación a la vez que mantenemos nuestra privacidad en la red, aspectos que se han convertido en fundamentales en la Sociedad de la Información. Esa habilidad, denominada alfabetización informacional se define como el saber cuándo necesitamos determinada información, por qué la necesitamos, dónde encontrarla, cómo evaluarla, atizarla y comunicarla de forma ética (CILIP, 2004).

A su vez, más ampliamente, Área, Gros y Marzal (2008) definen la alfabetización digital como la adquisición y el dominio de las habilidades para el uso de las herramientas y tecnologías digitales.

Más ambiciosamente, Pozuelo (2014) señala cuáles deberían ser consideradas las habilidades digitales actuales así como configura como objetivo las sesenta competencias digitales que todo estudiante universitario debería tener al finalizar sus estudios, entre las que están el saber diferenciar y usar diversas redes sociales, ajustando el perfil de privacidad y conocer la utilización que se puede hacer de las diversas informaciones existentes en la red y su grado de confianza.

Alguno de los riesgos referenciados por INTECO, que aparecen cuando la proliferación de nuestros datos es suficiente, consiste en la suplantación de nuestra identidad digital, de forma que terceras personas actúan en nuestro nombre a través de la red. Puede hacerse desde un perfil falso caricaturizando la imagen o transmitiendo informaciones dispares o accediendo a nuestro perfil y suplantándonos en alguna red social.

Las recomendaciones básicas pueden verse en la figura



Fig. 16: Recomendaciones preventivas y reactivas sobre la identidad digital

Fuente: INTECO (2012)

A su vez hay que tener en cuenta que, casi como el ciclo de vida de todos los organismos, la identidad digital pasa por varias fases: la creación (provisión) de los datos, su propagación, uso, mantenimiento (actualización) y su borrado (eliminación).



Fig. 17: Ciclo de vida de la identidad digital

Fuente: Fundación CTNE (2013)

Entre las medidas adoptadas por los usuarios para proteger su privacidad a través de internet tenemos las siguientes:



Fig. 18: Tareas realizadas en internet para proteger la identidad digital (UE)

Fuente: EUB (2011)

Estas nuevas formas de comunicación y relación, con círculos de “amistades” cada vez más amplios, van dejando un rastro fácil de seguir, que perjudica los conceptos tradicionales de intimidad y privacidad. Una gestión eficaz de nuestra identidad digital pasa por ser conscientes de la importancia de preservar la privacidad en internet, siendo los usuarios los nodos principales y la información se transmite a través de las redes que conforman (Aced *et al*, 2009).

Hay concepciones culturales diferentes sobre la privacidad que con la globalización pueden soslayarse, pues a través de desarrollos informáticos podemos alojar información no permitida en ciertos lugares, en otros dominios, con diferente grado de permisividad (Díaz, 2008).



Fig. 19: Datos e información considerados personales (UE)

Fuente: EUB (2011)

En USA las políticas de privacidad de las empresas se basan en las recomendaciones de la Comisión Federal de Comercio (FTC) y la única posibilidad de los ciudadanos para proteger sus datos era dejar de tener relaciones comerciales con quien consideraban que no los gestionaban adecuadamente.

La sensibilidad con la protección de la privacidad se va desarrollando con el mayor nivel cultural y uso intenso de internet (Fundación CTNE, 2013).

Sin embargo hay cierta concienciación respecto la necesidad de disponer de ciertos datos personales a la hora de disponer de determinados servicios.



Fig. 20: Impresiones sobre la revelación de datos considerados personales (UE)

Fuente: EUB (2011)

La Web 2.0 también es una oportunidad para los hackers y otros delincuentes que buscan infectar sistemas corporativos con el fin de robar información. "Siempre que aparece una nueva tecnología, esta provoca una serie de problemas relacionados con la seguridad", aclara Williams analista del Gartner Group (D'Agostino, 2007: 1). Y lógicamente estos problemas son distintos a los tradicionalmente experimentados por las compañías.

El por qué lo encontramos en que los servicios Web normalmente son aplicaciones JavaScript complejas que se ejecutan a través de un navegador y que acceden a los datos guardados localmente en el equipo del usuario. Al no tratarse de datos y aplicaciones ubicados en un servidor central, éstos se ejecutan con mucha más rapidez. El lado negativo es que estos datos no están adecuadamente protegidos. Es más, con las prisas

de implementar estas herramientas, el aspecto de la seguridad pasa normalmente a un segundo plano, dejando así, vulnerables las aplicaciones frente a los ataques.

Según dice Tom Longstaff, director de Tecnología en el *Centro de Coordinación CERT* de Carnegie Mellon University y responsable de estudiar las vulnerabilidades en internet "*imagínese que dispongo de una aplicación Web 2.0 que es un cliente de email, descargado como un programa Java en mi ordenador, los mensajes se almacenan localmente. Y como los puestos cliente no están integrados en el servidor de la compañía, carecen de protección. Basta que llegue un código que ataque al cliente de correo, para que acceda a los mensajes en memoria y, desde ahí, infecte al sistema*" (D'Agostino, 2007: 1). Otro escenario descrito por el mismo responsable se refiere a que si un empleado de un banco utiliza un servicio Web para acceder a datos sensibles e interactúa con otras páginas Web, un ataque de phishing podría robar datos sin que el usuario se enterase.

La monitorización de estas vulnerabilidades es prácticamente imposible, ya que la mayoría de compañías no dispone de la visibilidad de los equipos individuales. "*Cuando los programas se ejecutan desde el servidor y disponen de control de entorno, un administrador puede monitorizar toda la actividad de la red*", añade Longstaff. Sin embargo, en el caso de la Web 2.0, los ataques se dirigen preferentemente hacia los equipos locales.

"*Lo que ocurre*", según Williams, "*es que las compañías están creando servicios fuera del perímetro corporativo que permiten esta interacción en internet. Como resultado, pierden la visibilidad de la seguridad de los equipos locales*". En el ámbito empresarial, las amenazas son insignificantes, por ahora. "*Aún así, los hackers siempre desarrollan nuevas técnicas*", apunta Longstaff. "*La creciente facilidad de creación de contenidos, también facilita el desarrollo de herramientas maliciosas*", añade Williams. Irónicamente, las compañías que, durante los últimos diez años, se lanzaron a robustecer la seguridad de sus sistemas, ahora tienen que abrir los cortafuegos para permitir el acceso de aplicaciones Web 2.0.

Los expertos coinciden en que la mejor manera de asegurar la Web 2.0 es partiendo de aplicaciones seguras. "*Lo primero que un CIO debe hacer es inculcar la importancia de la seguridad al propio equipo de desarrollo*", apunta Williams. "*Debe haber un punto*

en el ciclo de desarrollo donde se compruebe la seguridad de la aplicación". Esto significa la incorporación de capacidades de rastreo para monitorizar los comportamientos sospechosos.

Cualquiera que sea la evolución de la Web 2.0, está claro que la seguridad seguirá siendo uno de los temas que más den que hablar. Para Williams, *"las nuevas aplicaciones marcarán la diferencia entre las compañías, pero no podemos permitir que la seguridad sea un inhibidor de la innovación; queremos que la seguridad sea la razón de innovación"*.

"Los ciberdelincuentes van allá donde hay oportunidades y aprovechan todas y cada una de las vulnerabilidades", dice Brian Grayek, vicepresidente de gestión de productos de la unidad de negocio de seguridad en internet de CA (una de las mayores compañías de software independiente del mundo, que ofrece soluciones software para unificar y simplificar la gestión de las TI). *"Aunque la protección de seguridad está mejorando en la detección de código malicioso, los ladrones online son más sigilosos en la forma en que atacan nuestros ordenadores"* (CA, 2008: 1).

Las predicciones de CA acerca de la seguridad online ya para 2008 preveían que las redes sociales estarían en el punto de mira: los sitios web de redes sociales cada vez son más populares, y como resultado de ello, más vulnerables. En 2009 la penetración de las redes sociales en España era del 28,7% y, en solo un año, pasó al 50% en 2010 (FUNTEL, 2011).

El gran número de víctimas potenciales y su relativa poca preocupación por la seguridad informática hace que estos sitios web sean una oportunidad de ganancias para los ladrones cibernéticos. Y los sitios y servicios web 2.0 serían blancos de ataques dirigidos, aunque es relativamente sencillo implementar servicios de web 2.0, puede ser todo un reto configurarlos para que sean completamente seguros. Por lo tanto, muchos sitios de internet que utilicen estos servicios son blancos fáciles con pocas indicaciones externas que hagan sospechar que la seguridad del sitio se ha visto comprometida.

Hoy más que nunca no es suficiente con disponer de un buen sistema antivirus para mantener seguro nuestro equipo. Ya hemos dado el siguiente paso incorporando recursos anti espía y cortafuegos para filtrar los ataques desde el exterior y evitar fugas

de información desde el interior. Pero no basta con tener la mejor herramienta ya que el factor humano es crucial.

Navegando por internet nos encontramos ante sitios de riesgo que debemos evitar, normalmente relacionados con la pornografía, descargas ilegales de software, música, juegos, películas, por sólo citar algunos ejemplos. Además, el nivel de riesgo aumenta con el mal uso de otras aplicaciones como los messengers, chats, etc., y muy especialmente con las redes P2P.

Hay que tener en cuenta que detrás de cada nombre de usuario, o avatar (ese muñequito con aspecto humano que nos representa dentro de un chat en tres dimensiones o en un mundo virtual), puede haber alguien como nosotros, un simple internauta, o alguien completamente distinto a quien dice ser, con intenciones poco claras.

Por este motivo debemos proteger con sumo cuidado nuestra información personal, desde nuestro "inocente" correo electrónico, hasta por supuesto nuestro nombre, apellidos, edad o teléfono y, especialmente, nuestras fotos e imágenes personales o familiares; es decir, el conjunto que conforma nuestra identidad digital.

En caso contrario nos exponemos a un bombardeo de correos electrónicos indeseados, a recibir llamadas desagradables, a que se suplante nuestra personalidad en diversos sitios web dañando nuestra imagen y nuestras relaciones, lo que además resulta especialmente grave cuando afecta a menores.

No hablamos sólo de peligros que generan gran alarma social, como el de los pederastas que se hacen pasar por jóvenes en los sitios web sociales para contactar con niños y conseguir fotos, quedar personalmente, engañarlos o chantajearlos, sino que también proliferan otros riesgos como el ciberbullying o acoso escolar.

No se trata de actuar con miedo en internet ni dejar de utilizarlo, sino que debemos ser capaces de actuar consciente y coherentemente, aprendiendo a trabajar de forma segura en este medio y sobre todo saber comportarnos frente a los desconocidos.

Hay numerosas iniciativas a nivel nacional e internacional trabajando para promover un uso seguro de internet, mejorar el nivel de seguridad informática de los hogares y las

empresas, así como ayudar a educar y guiar a los más pequeños, como son www.inteco.es (actualmente www.incibe.es), Pantallas Amigas (iniciativa por un uso seguro y saludable de internet y las Nuevas Tecnologías por parte de los menores) - www.pantallasamigas.net, Protégeles (dedicada a la sensibilización y con líneas de denuncia sobre pornografía infantil, ciberbullying,...) - www.protegeles.com, o Insafe (la red europea de nodos de concienciación en seguridad online) - www.saferinternet.org²⁰.

Así es que, si bien hay muchos peligros en la sociedad en red, también hay multitud de recursos y apoyos para aprender a sacarle todo el partido con total confianza.

Un estudio muy reciente realizado por profesores británicos y californianos pone de manifiesto la forma en la que actuaciones ingenuas en la red social Facebook acaban comprometiendo nuestra identidad. A través de los múltiples “Me gusta” con los que podemos calificar noticias, comentarios o actos de nuestros propios amigos, se puede generar un perfil con nuestra forma de pensar cuya comercialización puede perjudicarnos. (Kosinski, 2014). Con técnicas Big Data, como veremos a continuación, se pueden construir catálogos con los perfiles de los usuarios de la citada red de todo el mundo.

²⁰ Páginas consultadas en fecha 19 de Marzo de 2015.

2.2 Estado actual

En este punto vamos a destacar tres aspectos que inciden muy directamente con los objetivos de nuestra investigación:

- el tratamiento masivo de datos, como un desarrollo adicional consecuencia del nivel tecnológico alcanzado
- la brecha digital, efecto indeseado del diferente nivel de conocimiento sobre los desarrollos tecnológicos por parte de los diferentes grupos de población, y
- la legislación en el sector TIC.

O lo que es lo mismo:

- las razones que se aducen para justificar los desarrollos que se están llevando a cabo y que, colateralmente, pueden condicionar nuestra privacidad,
- el nivel de preparación al utilizar la tecnología y sus riesgos, y
- las estrategias y herramientas defensivas de los Estados para proteger a los ciudadanos.

Veamos cada uno de ellos.

2.2.1 Big Data

Se define como Big data, o analítica de datos, al conjunto de datos que excede la capacidad del software habitual para su captura, gestión y proceso en un tiempo razonable. El reto consiste en su transformación en información, pues de nada nos sirve almacenar datos acumulándolos sin ponerlos en valor (Cánovas, 2014).

El crecimiento constante de datos que se alojan en la red constituye una oportunidad para su explotación a la vez que se convierte en un reto tecnológico y legal (Laney, 2001).

La generación de información crece cada vez más aceleradamente. Durante 2012 se han creado cerca de 2,5 QB (quintillones²¹ de bytes) diarios (FUNTEL, 2013)

El desarrollo tecnológico (Big data, cloud computing, CRM²² o IoT²³) conllevan la cesión de parte de la privacidad para mejorar la calidad de vida.

Por ejemplo, con Google Flu se pueden hacer estimaciones sobre epidemias de gripe basándose en las búsquedas de los usuarios.

Servicios como los de Amazon permiten recomendaciones de lectura en función del histórico de compras e incluso de lo que los amigos identificados a través de redes sociales han adquirido.

Algo parecido vienen haciendo desde hace tiempo los bancos, ofreciéndonos catálogos cuasi-personalizados basados en nuestra capacidad económica y aficiones, generando unos perfiles de consumo individualizados.

Las técnicas de CRM vienen siendo explotadas por la informática tradicional desde hace décadas.

Y el IoT implica la transferencia de gran cantidad de datos de forma automática, como la monitorización de nuestras constantes vitales a través de los wearables²⁴, o recomendaciones de vías alternativas de tráfico y cesión de infinidad de datos que pueden facilitar nuestra vida a la vez que coartan nuestra intimidad.

Las grandes cantidades de datos que recogen las redes sociales pueden proporcionar información de gran alcance. Muchos investigadores estudian Facebook para analizar las relaciones sociales entre las personas utilizando las conexiones hechas por esa red como sustitutivo de las relaciones del mundo real (Boyd, 2011).

La explotación de la información recogida a través de esos canales sobre nuestros sentimientos, proyectos, planes, metas o deseos facilita el testeado de aplicaciones que permiten diseñar perfiles a los que manipular individual o socialmente.

²¹ 2.5×10^{18}

²² Customer request management

²³ Internet of things

²⁴ Dispositivos con conectividad de uso personal que el usuario lleva encima en forma de complementos

2.2.2 Brecha digital

Si bien las TIC han contribuido a que el mundo sea cada vez más global y las coordenadas de espacio y tiempo se vean superadas dando lugar a una nueva sociedad mundial más interconectada y homogénea, nos encontramos que estas argumentaciones parten de que toda la población, o al menos la mayoría, tenga la llamada competencia digital, es decir, herramientas teórico-prácticas para usar las TIC.

Esta competencia depende de varios factores, como son la alfabetización digital, los niveles de cobertura, el poder adquisitivo o el conocimiento de idiomas. Lamentablemente, estas condiciones no las reúnen todos los ciudadanos, por lo que resulta que la supuesta homogeneización provocada por las TIC en la era de la globalización genera una nueva exclusión. Esta nueva forma de brecha digital, término acuñado por Schiller (1996), va en sentido opuesto a facilitar la inclusión digital.

Este nuevo paradigma se corresponde con la fractura entre los capacitados para utilizar las nuevas tecnologías, que las han integrado en su vida diaria, y los no capacitados. Esta brecha digital aumenta más las diferencias geográficas, culturales y económicas.

Ya en la era Clinton (1992-2000), el vicepresidente Gore (1993) potenció las entonces denominadas “autopistas de la Información” dando lugar a la aparición de la diferencia entre *los conectados* y *los no conectados*, augurando presagios poco halagüeños para estos últimos que difícilmente podrían seguir el ritmo de conocimiento y desarrollo de los primeros.

Si analizamos la brecha digital global, veremos que el grupo de *no conectados* apenas llegaba en 2006 a un 41,4% en los países desarrollados y, en cambio, en las zonas del Tercer Mundo ascendía hasta un 89,8%, según los datos de la *International Telecommunications Union* (ITU, 2006). Aunque, con la llegada de la web 2.0 en los últimos años, han accedido nuevos usuarios a las TIC, donde las redes sociales y la proliferación de Apps de telefonía móvil han tenido un rol fundamental.

No obstante, sigue habiendo una gran población perteneciente al grupo de no conectados, y mientras que en los países desarrollados se circunscribe a sectores de edades avanzadas, en otras zonas del mundo afecta de un modo más generalizado pues

hay factores como la pobreza, falta de cobertura de comunicación, bajos niveles educativos e incluso escasez de recursos energéticos.

Los datos de la ITU (2011) correspondientes al uso de internet durante en el periodo 2006-2011 indican que hay una brecha global importante, y continúa siendo mayor la población a nivel mundial que no está conectada de la que sí lo está, si bien es cierto que las diferencias van disminuyendo. En 2006 el 82% de la población mundial no estaba conectada, mientras que en 2011 el porcentaje se situaba en el 65%. Sin embargo, este aumento de *los conectados* se concentra en los BRIC (Brasil, Rusia, India y China).

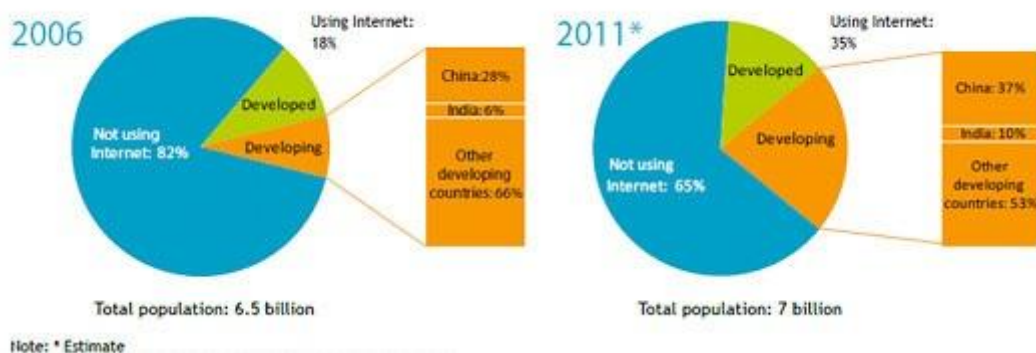


Fig. 21: Usuarios de internet a nivel mundial

Fuente: ITU (2011)

Es decir, la brecha digital aún afecta a prácticamente dos tercios de la población mundial.

En resumen, nos encontramos que las TIC no solo no están contribuyendo a la globalización del mundo, sino al aumento de la desigualdad entre las zonas más y menos desarrolladas.

Según Eurostat, el acceso a internet en España es del 71,6% del total de la población, que se compara con el 75% de la media de la UE. O sea, el 28% de la población española se encuentra entre los no conectados, porcentaje que aumenta rápidamente entre la población de más de 60 años.

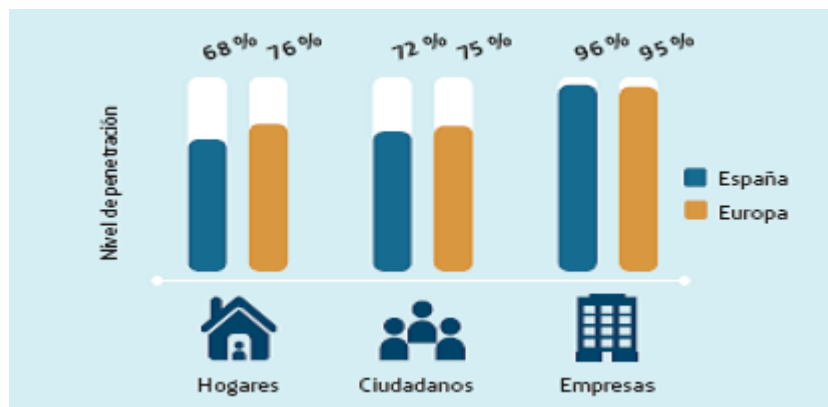


Fig. 22: Penetración de internet en España y Europa

Fuente: FUNTEL (2014)

El mejor ejemplo social que podemos constatar a nivel educativo al hablar de esta brecha cultural y generacional lo tenemos en que una Universidad sigue imponiendo unos esquemas docentes de tipo analógico (clases magistrales, apuntes dictados, tiza, uso de la pizarra tradicional, bolígrafos de tinta...o incluso proyectores de transparencias, pobres presentaciones en PowerPoint,...) dirigidos a unos alumnos que, en su inmensa mayoría, ya están incorporados a la docencia digital con el uso de PDIs, por lo que el aula universitaria les implica un “avance hacia los recursos del pasado” más que hacia los que utilizan en el presente y con los que construirán el futuro, con la lógica frustración, descenso de la motivación, escasez de atención y “brecha comunicativa” con los profesores.

Tanto a nivel nacional como global, la brecha digital es una fractura resultado del propio proceso de globalización que, en vez de de homogeneizar, aumenta las diferencias de comunicación e información, pues la interacción entre personas, o el intercambio de conocimientos y experiencias se hace cada vez más fomentando el uso de las TIC.

Para intentar paliar esa dificultad de acceso para determinados nichos de población (edad y género), se adoptaron acciones intentando llevar internet a toda la sociedad por igual, con resultados positivos en España como puede observarse en la siguiente figura

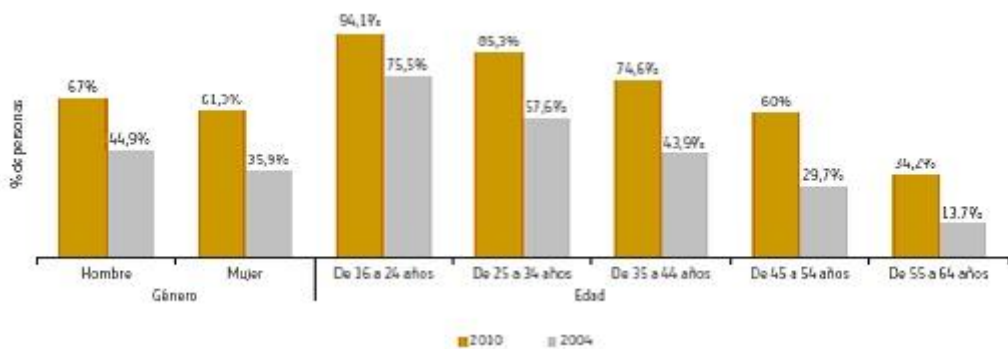


Figura 23: Acceso a internet en España por tramo de edad y sexo

Fuente: INE

Es de destacar que entre los más jóvenes (de 16 a 24 años) son las mujeres las que se conectan más, pero aparecen “nuevas” brechas con los servicios avanzados, como el acceso móvil, asociadas a los mismos grupos (edad, género, nivel educativo y social) (FUNTEL, 2012: 27).

Lo que demuestra que en este ámbito también es necesaria una formación continua que vaya paralela a las nuevas potencialidades de la tecnología para evitar el riesgo de caer en el “otro lado de la brecha” en el caso de no mantener la actualización de conocimientos.

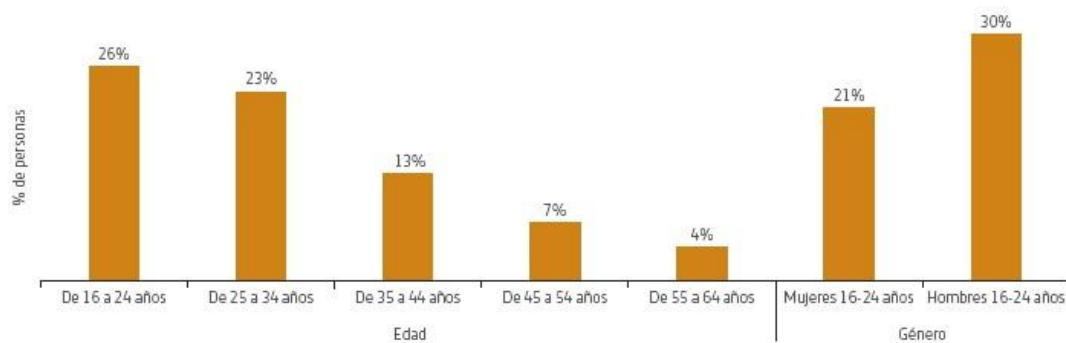


Fig. 24: Acceso desde el móvil en España

Fuente: Eurostat. Datos de 2011

2.2.3 Legislación (Europea / Americana / Española)

Dentro del marco de la Unión Europea, la norma inicial regulatoria de la Protección de Datos de Carácter personal fue la *Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1.995*, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

España fue pionera en esta materia en relación con otros países de la UE cuya primera experiencia legislativa en este campo surgió a raíz de la Directiva mencionada. Nuestro país ya contaba con la *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)*. En sustitución de esta, y ya siguiendo los preceptos de la normativa europea, actualmente la privacidad está regulada por la **LOPD** (ESPAÑA, 1999), así como por el *Real Decreto 994/1999 de 11 de junio*, por el que se aprobó el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Y más recientemente su Reglamento (ESPAÑA, 2008).

En esos momentos nos encontrábamos con que las legislaciones sobre protección de datos de los países miembros eran muy diferentes, siendo unas más rigurosas que otras. Por lo que se inició en Europa un debate entre los diferentes miembros tendentes a determinar si esa nueva directiva debería ser más restrictiva o no.

El programa de acción relativo a la delincuencia organizada, adoptado por el Consejo JAI (Justicia y Asuntos de Interior) en mayo de 1.997, aprobado por el Consejo Europeo de Amsterdam, invitaba a la Comisión a realizar un estudio sobre la delincuencia informática. La Comisión presentó en abril de 1.998 este estudio, conocido por su título abreviado «estudio COMCRIME».

El Consejo Europeo de Tampere reconoció que los esfuerzos para llegar a un acuerdo sobre definiciones y sanciones comunes de una serie de actos delictivos debían también referirse a la delincuencia que utiliza las nuevas tecnologías.

El legislador tuvo que atender una demanda creciente de normativa a la hora de garantizar la seguridad de los ciudadanos pues, como ya hemos anticipado, el desarrollo de las nuevas tecnologías de la información y la comunicación han dado lugar a cambios profundos en la economía y en la sociedad. El éxito de la Sociedad de la Información es decisivo para el crecimiento, la competitividad y la creación de empleos en Europa. Esta es la razón por la que la Comisión Europea lanzó la Iniciativa eEuropa (COMEU, 1999), cuyo objetivo era permitir a la UE utilizar todas las posibilidades. El plan de acción global sobre esta Iniciativa, aprobado por el Consejo Europeo de Feira en junio de 2000, destacaba la importancia de la seguridad de las redes y de la lucha contra los delitos informáticos (Alabau, 2001; URLEU, 2000).

Al mismo tiempo, esta importancia creciente de las infraestructuras de información y comunicación abría nuevos caminos a conductas delictivas. Esta es la razón por la que la Unión Europea lanzó una serie de medidas para luchar contra el contenido ilícito y perjudicial en internet con el fin de proteger los derechos de la propiedad intelectual y los datos de carácter personal, promover el comercio electrónico y reforzar la seguridad en las transacciones.

La propuesta del nuevo marco regulador de las comunicaciones electrónicas fue adoptada por la Comisión Europea el 12 de julio de 2.000 y se presentó formalmente en el Consejo de Ministros de Telecomunicaciones de 3 de octubre del mismo año (COMEU, 2000a). La propuesta relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, traslada los principios establecidos en la Declaración Universal de Derechos Humanos con respecto al derecho a la privacidad y a la protección de los datos en el citado sector, pues el artículo 12 de la misma dice: *“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”*

Se aprobaron una serie de medidas iniciales en el marco de la estrategia de la Unión en materia de lucha contra la delincuencia que se sirve de las altas tecnologías. (RECEU, 2001). Esta Comunicación define la delincuencia informática en un sentido amplio, como referido a todo delito que implique la utilización de las tecnologías informáticas. (COMEU, 2000b)

Si bien a lo largo del procedimiento legislativo hubo importantes diferencias en algunos aspectos entre el Consejo, el Parlamento y la Comisión, finalmente se llegó a la adopción de una posición común.

Los conceptos de «delincuencia informática», «delincuencia relacionada con la informática», «delincuencia de alta tecnología» y de «delincuencia cibernética» tienen el mismo significado en la medida que todos se refieren a:

- a) la explotación de las redes de información y comunicación sin ninguna dificultad geográfica
- b) la circulación de datos intangibles y volátiles.

Los principales delitos tratados por la legislación existente a nivel europeo así como a nivel nacional fueron los siguientes:

- a) delitos contra la intimidad: recogida, almacenamiento, modificación, revelación o difusión ilegales de datos personales;
- b) delitos relativos al contenido: difusión, especialmente por internet, de pornografía, y en especial de pornografía infantil, declaraciones racistas e información que incita a la violencia;
- c) delitos económicos, acceso no autorizado y sabotaje: Muchos países han aprobado leyes que abordan los delitos económicos perpetrados por ordenador y tipifican nuevos delitos relacionados con el acceso no autorizado a sistemas informáticos (por ejemplo, la piratería, el sabotaje informático y la distribución de virus, el espionaje informático, y la falsificación y el fraude informáticos);
- d) delitos contra la propiedad intelectual: delitos contra la protección jurídica de programas de ordenador y la protección jurídica de las bases de datos, los derechos de autor y derechos afines. (DIRCE, 2001)

La UE interviene para garantizar la seguridad de las redes y sancionar los ataques contra los sistemas de información mediante los siguientes tipos de medidas destinadas a luchar contra la ciberdelincuencia en general:

Lucha contra las actividades en línea ilícitas

- Programa “Safer Internet” (1.999-2.004)
- Programa para una Internet más segura (2.005-2.008) (“Safer Internet Plus”)
- Lucha contra el spam, los programas espía y los programas maliciosos (Comunicación de 2.006)

Seguridad específica de las Redes y de los sistemas de Información

- Estrategia para una S.I. segura (Comunicación de 2.006)
- Agencia Europea de Seguridad de las Redes y de la Información (ENISA²⁵)
- Ataques contra los sistemas de información
- Lucha contra los delitos informáticos

Con los objetivos “i2010 – Una Sociedad de la Información europea para el crecimiento y el empleo”, dentro del 7º Programa Marco, se subrayaba la importancia de la seguridad de las redes y de la información para la creación de un espacio único europeo de la información (COMEU, 2005; Alabau, 2006) y se invitaba al sector privado a definir responsabilidades de los productores de programas informáticos y los proveedores de los servicios de internet, suministrando unos niveles de seguridad adecuados y fiables, fomentando programas de formación para empleados con conocimientos y aptitudes para aplicar prácticas de seguridad y elaborar sistemas para certificar dicha seguridad en productos, procesos y servicios que respondan a las necesidades específicas de la UE y refuercen las investigaciones sobre seguridad creando un Programa específico europeo basado en el Safe Harbour.

²⁵ A fin de garantizar a los usuarios la mayor seguridad posible, la UE creó la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), desempeñando funciones de asesoramiento y coordinación de las medidas adoptadas por los Estados miembros para hacer más seguras sus redes y sistemas de información. El objetivo perseguido es lograr que la Unión, los Estados, y las empresas tengan mayor capacidad de reacción y gestión de los problemas relacionados con la seguridad de las redes y de la información. La Agencia inició su actividad en marzo de 2.004. (REGEU, 2004)

Se han ido adhiriendo nuevos países a la UE con diferentes niveles de recursos tanto legales como tecnológicos y hay que indicarles las estrategias, hacia dónde ir, cómo conseguirlo, facilitando ayudas de todo tipo (económicas, asesoría, colaboración, etc.).

Entre los mismos Estados, unos van más rápidos y otros menos en la incorporación de las directivas europeas a sus legislaciones locales. Acogerse a estas cláusulas contractuales es voluntario pero ofrece a las sociedades y organismos una forma de respetar su obligación de asegurar una protección adecuada a los datos personales cuando estos se transfieran tanto a países fuera de la UE como a países Miembros.

En general, se exige la aplicación de ciertos principios generales tales como que los datos sólo se recojan para fines específicos, explícitos y legítimos; que las personas cuyos datos se recaben estén informadas sobre el objeto de la recolección así como de la identidad del responsable del tratamiento; que todos tengan derecho a acceder a sus datos, modificarlos o borrar los que fueran incorrectos; y que, en caso de conflicto, las personas afectadas puedan disponer de vías de recurso apropiadas, incluida la posibilidad de recibir una indemnización.

Y, si dentro de la UE no es fácil ejercer toda esta coordinación, más complicado resulta acometer estas actuaciones coordinadas con el resto del mundo.

Pero hay que trabajar en esa dirección, denunciando actuaciones irregulares, analizando desde la perspectiva legal y/o ética los desarrollos de nuevas herramientas, poniendo en marcha todos los mecanismos necesarios para atajar su uso indebido. Es la única forma de eliminar las brechas entre unos y otros y tratar de alcanzar la sociedad competitiva y respetuosa que se persigue.

Pero si las dificultades de entendimiento entre los países europeos, con una mayor identidad cultural y legislativa, convergen con la meta de la Unión, con USA son más difíciles. Afortunadamente, tras largas negociaciones, el 29 de julio de 2000 la Unión Europea y EE.UU. llegaron al acuerdo llamado **“Safe Harbor”** (*Puerto Seguro*), por el que se establecían una serie de principios sobre el acceso y uso de los datos personales, así como las excepciones a su transferencia. En virtud de dicho acuerdo, las empresas norteamericanas que voluntariamente certificaran su sometimiento a estos principios entrarían a formar parte del llamado *Puerto Seguro* y no correrían el riesgo de que sus transferencias de datos fuesen bloqueadas (GOBUSA, 2000)

Sin embargo, como consecuencia de los ataques terroristas del 11-S, USA promulgó la *PATRIOT ACT* en octubre/2001 que hace prevalecer las necesidades de garantizar la seguridad sobre los derechos de privacidad que se otorgan en otros países. Los efectos de esta ley alcanzan más allá de las fronteras americanas y permite violar los derechos de privacidad de ciudadanos y empresas extranjeras. El artículo 215²⁶ autoriza al FBI la obtención de una orden judicial para que cualquier ciudadano norteamericano facilite la información requerida ya sea de sociedades ubicadas en USA o en el extranjero. Adicionalmente, en el mismo artículo se establece la prohibición de divulgar la existencia de esa orden judicial y la inmunidad total frente a posibles demandas por comunicar información privada.

Hacen falta acuerdos globales entre USA y la UE para conseguir el equilibrio entre la Seguridad nacional, el derecho a la privacidad y la potenciación del desarrollo tecnológico, de forma que se disponga de una regulación que garantice los derechos fundamentales del ciudadano pero que a la vez permita el desarrollo de nuevos modelos de negocio que faciliten el crecimiento económico (Portilla y Santaella, 2014).

Finalmente en nuestro país, según el Artículo 18 de la Constitución Española (ESPAÑA, 1978):

1. *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
3. *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
4. *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

El derecho al honor consiste en el aprecio que cada persona tiene en su contexto social y/o profesional y la intimidad implica la esfera privada de la que se puede excluir a

²⁶ *Access to records and other items under the Foreign Intelligence Surveillance Act*

terceras personas. Con respecto a la imagen se incluyen la voz, el nombre y nuestra imagen física.

Una Sentencia de nuestro Tribunal Constitucional dictaminó:

“Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del Derecho Fundamental a la protección de datos se concretan jurídicamente en la Facultad de consentir la Recogida, la Obtención y el Acceso a los datos personales, su posterior Almacenamiento y Tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo y, por otro lado, el poder oponerse a esa posesión y usos” (AEPD, 2000: 22).

Con la Ley Orgánica 5/2010, de 22 de junio, se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (ESPAÑA, 2010) incorporando nueva tipificación de ciberdelitos, de forma que en el título VII dice:

“Se regula de manera pormenorizada la responsabilidad penal de las personas jurídicas. Son numerosos los instrumentos jurídicos internacionales que demandan una respuesta penal clara para las personas jurídicas, sobre todo en aquellas figuras delictivas donde la posible intervención de las mismas se hace más evidente (corrupción en el sector privado, en las transacciones comerciales internacionales, pornografía y prostitución infantil, trata de seres humanos, blanqueo de capitales, inmigración ilegal, ataques a sistemas informáticos...). Esta responsabilidad únicamente podrá ser declarada en aquellos supuestos donde expresamente se prevea.”

...

“Por otra parte, la extensión de la utilización de Internet y de las tecnologías de la información y la comunicación con fines sexuales contra menores ha evidenciado la necesidad de castigar penalmente las conductas que una persona adulta desarrolla a través de tales medios para ganarse la confianza de menores con el fin de concertar encuentros para obtener concesiones de índole sexual. Por ello, se introduce un nuevo

artículo 183 bis mediante el que se regula el internacionalmente denominado «child grooming»²⁷, con la siguiente redacción:

«El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño».»

El título XIV dice:

“En el marco de los denominados delitos informáticos, para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos. El primero, relativo a los daños, donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. El segundo apartado se refiere al descubrimiento y revelación de secretos, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo.

En el artículo 197 se introduce un nuevo apartado 3, y se añade un apartado 8, con la siguiente redacción:

«3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

²⁷ Ciberacoso sexual infantil

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

[...]

8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado.»

En resumen, será delito *"borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos y el acceso sin autorización a datos o programas contenidos en un sistema informático"* y también *"obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno"* (p. e. un sitio web).

Asimismo se castiga *"Descubrir y revelar secretos: acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte de él."* En este delito podría incurrir por ejemplo quien accediese a la cuenta de una red social online de otra persona sin permiso, o quien robase sus fotos de sexting²⁸, con intenciones de realizar bullying, acoso o sextorsión, por citar algunos casos.

El artículo 183 bis tipifica como delito el grooming cuando se intenta llegar a un encuentro físico. Esta nueva figura delictiva pretende sancionar la conducta de quienes por medios telemáticos (internet o móviles) contacten con menores de 13 años (edad de consentimiento sexual legal en España) para encuentros con fines sexuales:

El sexting entre menores podría quedar recogido en el artículo 189, sobre la elaboración de material pornográfico o exhibicionista. El mismo artículo establece penas de prisión también para la posesión y difusión:

“El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico

²⁸ Envío de contenidos eróticos o pornográficos mediante teléfonos móviles

en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.”

Se tipifica como delito la *captación* de niños para participar en espectáculos pornográficos y la responsabilidad de quien se lucra. Esto podría incluir los casos en que se fuerza o convence (con pago o no) a menores para producir auto pornografía con sus cámaras web o teléfonos móviles.

Siguiendo con las estrategias emanadas de la Comisión Europea, el Plan i2015 trata de impulsar la difusión y uso de la e-administración contribuyendo al logro de la Agenda Digital Europea. La aplicación de esos objetivos en España se traduce en la aprobación de los sucesivos planes Avanza para los quinquenios 2005-2009 y 2011-2015 que, entre otras cosas incluyen extender la cultura de la seguridad entre los ciudadanos y las empresas (MINET, 2010)

Después de muchos años de sensibilidad hacia los delitos que se han ido tipificando como ciberdelitos, el propio Ministerio del Interior ha incorporado por primera vez en su historia la información relativa a los casos en los que ha intervenido, aunque de momento solo haya facilitado las cifras registradas por las Fuerzas y Cuerpos de Seguridad del Estado y la Policía Foral de Navarra, así como datos de los cuerpos de policía local que los facilitaron al Sistema Estadístico de Criminalidad durante el año 2013. (AEMI, 2014).

El título del apartado que referencia esta información es “Cibercriminalidad y principales tipologías penales cometidas con las Nuevas Tecnologías”, con este texto:

“Es una constante en nuestra sociedad actual el empleo de términos como delincuencia informática, cibercriminalidad, delitos informáticos, etc. Existen muchas tipologías penales que pueden cometerse mediante el uso de lo que ha venido a denominarse las «nuevas tecnologías». Para concretar unos criterios que metodológicamente fueran comparables con los países de nuestro entorno se ha decidido emplear las tipologías penales descritas en el Convenio sobre Cibercriminalidad de Budapest. A estos hechos se les han unido los delitos contra el honor, las amenazas y coacciones, y delitos contra la salud pública, dado el volumen y la importancia que están adquiriendo estos últimos. Los tipos penales concretos que abarca y los medios que se considera que deben

emplearse para su comisión, se detallan específicamente en el anexo metodológico. Entre los tipos penales que más se dan se sitúan los denominados «fraudes informáticos», seguidos a cierta distancia por las amenazas y coacciones.”

Resumiendo las cifras de los delitos computados en este apartado, dan la distribución representada en la figura 25 y, en las tipologías penales de la figura 26, se resalta en azul las relativas a estos delitos, con los artículos aplicables del Código Penal.

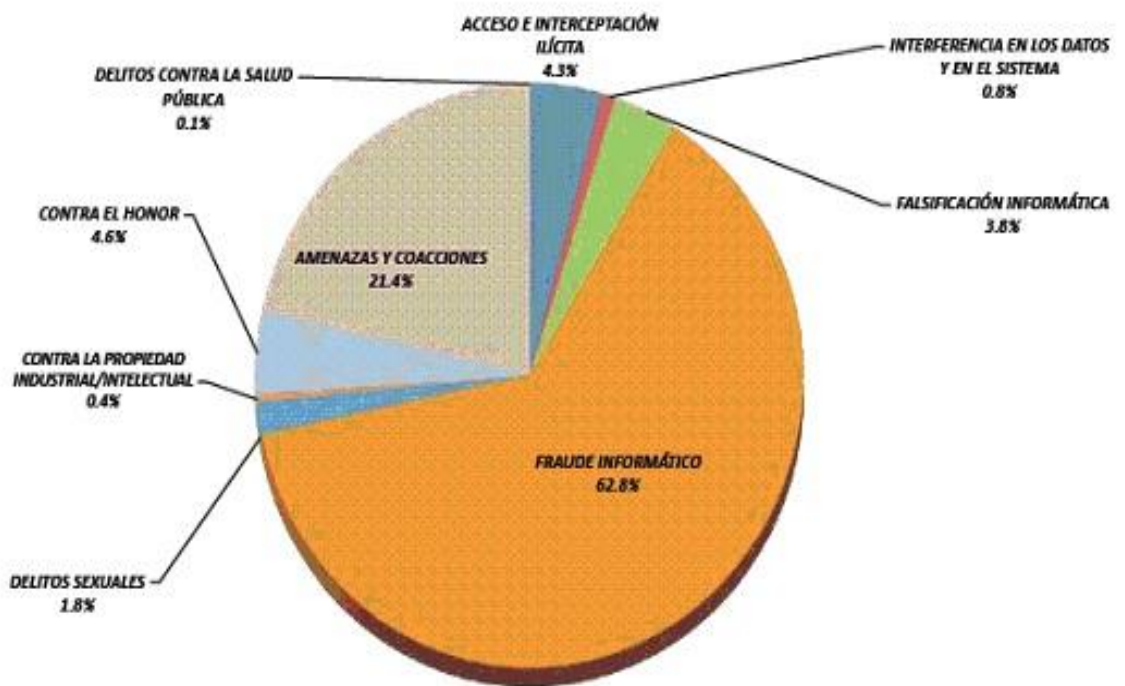


Fig. 25: Distribución del tipo de delitos informáticos

Fuente: AEMI (2014)

Acumulado (periodo temporal)	TITULO DEL CÓD. PENAL	TIPIFICACIÓN
I. Contra las personas	TIT. I, II, III, IV, V -CONTRA LAS PERSONAS: DEL HOMICIDIO Y SUS FORMAS, ABORTO, LESIONES, LESIONES AL FETO Y MANIPULACIÓN GENÉTICA	
1. Homicidios dolosos/asesinatos	art. 138, 139, 140	Delitos Título I. Homicidio doloso y asesinato.
Homicidios/asesinatos consumados		(grado consumado)
2. Lesiones	147 a 152	Delitos
3. Malos tratos ámbito familiar	153	Delitos
4. Otros contra las personas	142 a 146, 149.2, 154, 156 bis, 157 a 162	Delitos. Homicidio imprudente, inducción /cooperación suicidio, eutanasia activa, aborto, mutilación genital, rifa tumultuaria, obtención, trasplante o tráfico ilegal de órganos, lesiones al feto y manipulación genética
II. Contra la libertad	TIT. VI, VII, VII bis y X -CONTRA LA LIBERTAD. TORTURA Y OTROS CONTRA LA INTEGRIDAD MORAL Y DE LA TRATA DE SERES HUMANOS, OMISIÓN DEL DEBER DE SOCORRO Y CONTRA LA INTIMIDAD, EL DERECHO A LA PROPIA IMAGEN Y DE LA INVOLABILIDAD DEL DOMICILIO	
1. Malos tratos hab. ámbito familiar	173.2.3.	Delitos
2. Otros contra la libertad	163, 165 a 167, 169 a 176, 195 y 196	Delitos. Detención ilegal, secuestro, amenazas, amenazas a grupos étnicos, cultural o religiosos, coacciones, acoso inmobiliario, trato degradante, acoso laboral o funcional, tortura, trata de seres humanos con fines de explotación laboral o sexual o de extracción de órganos corporales, omisión del deber de socorro, descubrimiento /revelación de secretos, acceso ilegal informático y allanamiento de morada
III. Libertad sexual	TIT VIII -CONTRA LA LIBERTAD E INDEMNIDAD SEXUAL	
1. Agresión sexual con penetración	179	Delitos
2. Corrupción de menores o incapacitados	189.1.,4.,5.	Delitos
3. Pornografía de menores	189.1.,2.,7	Delitos
4. Otros contra la libertad/indemnidad sexual	178, 181 a 188	Delitos. Agresión sexual, abuso sexual (s/c penetración), acoso sexual, delitos de confianza mediante tecnología con menor de 13 años con fines sexuales, exhibicionismo, provocación sexual y relativos a la prostitución.
IV. Relaciones Ffiliarias	TIT XII -CONTRA LAS RELACIONES FAMILIARES	
V. Contra Patrimonio	TIT. XIII CONTRA EL PATRIMONIO Y CONTRA EL ORDEN SOCIOECONÓMICO	
1. Hurto	234 A 236	Delitos. Hurto y hurto en el interior de vehículo
2. Robos con fuerza en cosas	238 a 241	Delitos. Robo con fuerza en las cosas y robo con fuerza en las cosas en el interior de vehículo.
En vehículos		Delitos. Robo con fuerza en las cosas en el interior de vehículo.
En domicilios		(lugar específico: viviendas y otras dependencias comunes/anexos de viviendas)
En establecimientos		(lugar específico: establecimientos)
3. Robos violencia o intimidación	242	Delitos
En vía pública	242	(lugar específico: vía pública urbana)
En domicilios	242	(lugar específico: viviendas y otras dependencias comunes/anexos de viviendas)
En establecimientos	242	(lugar específico: establecimientos)
4. Sustracción de vehículos	244 y 252	Delitos. Sustracción de vehículos con/sin intimidación y apropiación indebida de vehículos.
5. Estafas	248 a 251	Delitos. Estafa bancaria, otras estafas y estafas con tarjetas de crédito, débito y cheques de viaje.
Estafas bancarias	248	Delitos. Estafa bancaria
6. Daños	263 a 267	Delitos. Daños y daños en vehículo.
7. Contra la propiedad intelectual e industrial	270 a 277	Delitos
8. Blanqueo de capitales	301 y 302	Delitos
9. Otros contra el patrimonio	243, 245.1., 2., 246, 247, 250.7, 252 a 254, 255 a 262, 264, 278 a 286, 289, 290 a 300 a 304	Delitos. Extorsión, usurpación, ocupación de inmuebles, estafa procesal, apropiación indebida, defraudación fluido eléctrico o análogas, insolvencia punible, alteración de precios concursos/subastas, ataques informáticos, estafa de inversores, corrupción entre particulares, corrupción en el deporte, acceso fraudulento a servicios radiodifusión, maquinaciones para alterar precios, otros relativos al mercado/consumidores, sustracción cosa propia, delitos societarios y recepción.
VI. Seguridad colectiva	TIT. XVII -CONTRA LA SEGURIDAD COLECTIVA	
1. Tráfico de drogas	368 a 371	Delitos
2. Contra la seguridad vial	379 a 385	Delitos. conducción a velocidad excesiva, bajo influencia de drogas/alcohol, negativa sometimiento a pruebas legales, conducción temeraria, conducir sin permiso o licencia, crear grave riesgo para la circulación, otros contra la seguridad vial.
3. Otros contra la seguridad colectiva	341 a 355, 359 a 367	Delitos. Riesgo catastrófico, incendios (Inc. Forestales) y otros contra la salud pública
VII. Falsedades	TIT. XVIII -DE LAS FALSEDADES	
VIII. Administración Pública	TIT. XIX y XIX bis -CONTRA LA ADMINISTRACIÓN PÚBLICA Y DE LOS DELITOS DE CORRUPCIÓN EN LAS TRANSACCIONES COMERCIALES INTERNACIONALES	
IX. Administración de Justicia	TIT. XX -CONTRA LA ADMINISTRACIÓN DE JUSTICIA	
X. Orden público	TIT. XXII -CONTRA EL ORDEN PÚBLICO	
XI. Legislación Especial	OTRAS DISPOSICIONES: caza, pesca, contrabando, navegación aérea, extranjería, seguridad ciudadana, espectáculos, seguridad privada, juego, armas y explosivos, deporte,.....	
XII. Otros delitos	DELITOS RESTO COD. PENAL	
TOTAL DELITOS	TODOS LOS DELITOS	
FALTAS	FALTAS CONTRA LAS PERSONAS	
1. Lesiones	617.1-621.1.,3	Faltas
2. Amenazas y coacciones	620	Faltas
3. Otras contra las personas	617.2, 618,2, 620, 621.2, 622	Faltas: Homicidio imprudente, malos tratos sin lesión, incumplimiento obligaciones familiares o asistenciales, vejaciones leves, infracción régimen custodia.
B. Patrimonio	FALTAS PATRIMONIO	
1. Hurto	623.1,2.	Faltas. Hurto y hurto en interior de vehículo
2. Daños	625.1	Faltas. Daños y daños en vehículo
3. Otras contra el patrimonio	623.3., 4., 624, 626	Faltas de: sustracción de vehículo sin intimidación, usurpación, estafa bancaria, estafa con tarjetas de crédito, débito y cheques de viaje, otras estafas, apropiación indebida (inc. Vehículos), defraudación fluido eléctrico o análogas, contra la propiedad industrial e intelectual y deslucimiento de bienes inmuebles.
C. Orden público	FALTAS ORDEN PÚBLICO	
D. Intereses generales y otros	FALTAS INTERESES GENERALES Y LEGISLACIÓN ESPECIAL	
TOTAL FALTAS	TODAS LAS FALTAS	
TOTAL	TOTAL DELITOS Y FALTAS	

Fig. 26: Tipologías penales
Fuente: AEMI (2014)

En la siguiente figura se muestra la información que el Ministerio del Interior ha comenzado recientemente a tabular separadamente de los principales delitos cometidos con el apoyo de las nuevas tecnologías

Denominación	Código Penal español	Tipo hecho SEC	Variables SEC a utilizar
Acceso o interceptación ilícita	Art. CP 197 A 201. Descubrimiento y revelación de secretos Art. CP 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial)	Descubrimiento/revelación de secretos	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		Acceso ilegal informático	Ninguna
		Otros relativos al mercado/consumidores	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Información en los datos y en el sistema	Arts. 263 a 267 y 625.1. Daños y daños informáticos	Daños	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		Ataques informáticos	Ninguna
Falsificación informática	Arts CP 388-389, 399 bis, 400 y 401	Falsificación de moneda, sellos y efectos timbrados Fabricación tenencia de útiles para falsificar Usurpación del estado civil	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Fraude informático	Arts. CP 248 a 251 y 623.4	Estafa bancaria	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		Estafas con tarjetas de crédito, débito y cheques de viaje	
		Otras estafas	
Delitos sexuales	Arts. CP 161, 183.1, 183. bis, 184, 185, 186, 189	Exhibicionismo	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		Provocación sexual	
		Acoso sexual	
		Abuso sexual	
		Corrupción de menores/incapacitados	
		Pornografía de menores	
Delito de contacto mediante tecnología con menor de 13 años con fines sexuales	Ninguna		
Denominación	Código Penal español	Tipo hecho SEC	Variables SEC a utilizar
Contra la propiedad industrial/intelectual	Arts 270 a 277 y 623.5 del CP(Contra la propiedad intelectual y contra la propiedad industrial)	Delitos contra la propiedad intelectual	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		Delitos contra la propiedad industrial	
Contra el honor	Arts. 205 a 210 y 620.2 del Código Penal	Calumnias	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		Injurias	
Amenazas y coacciones	Arts 169 a 172 y 620 del C.Penal	Amenazas	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		Amenazas a grupo étnico cultural o religioso	
		Coacciones	
Delitos contra la salud pública	Arts. 359 a 371 del Código Penal	Tráfico de drogas	Medio empleado: Internet/Informática, Teléfono/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		Otros contra la salud pública	

Fig. 27: Cibercriminalidad y principales delitos cometidos con Nuevas Tecnologías

Fuente: AEMI (2014)

SEC = sistema estadístico de criminalidad

2.3 Literatura revisada de otros investigadores

En este apartado vamos a ver diversos estudios realizados que miden motivaciones, aptitudes y actitudes, profundizando en las causas del comportamiento de los estudiantes a la hora de inclinarse hacia el estudio de diversas materias o realización de actividades. Nos han servido para guiarnos a la hora de utilizar los recursos en los que nos hemos apoyado para el desarrollo de la presente tesis.

Asimismo encontramos investigaciones que analizan cuáles son los factores que determinan el comportamiento de los usuarios a la hora de navegar por redes sociales o simplemente por internet. Referenciaremos algunos trabajos cercanos al nuestro, simultáneos en el tiempo en otros contextos universitarios, que denotan una creciente inquietud hacia el tema de nuestra investigación, que hacen patente la necesidad de abordarla y poner las medidas para garantizar un uso más seguro de la tecnología, obteniendo sus ventajas y minimizando sus posibles inconvenientes.

A través de la base de datos de tesis doctorales (TESEO) sobre posibles investigaciones que abordasen estudios parecidos hemos visto que sobre internet, en general, hay bastantes investigaciones sobre los usos y aplicaciones sectoriales que permite.

Más específicamente, sobre los conceptos de respeto a los individuos, encontramos las siguientes:

- “El derecho de autor en internet”, de junio/2004 en el deptº. de Derecho Constitucional de la Universidad Complutense de Madrid, en la que se establece que el régimen jurídico vigente es ineficaz y se hace necesario establecer nuevos controles técnicos y/o modificar la legislación (García, 2004).
- “El impacto de internet en el derecho fundamental a la protección de datos de carácter personal”, de diciembre/2004 en el deptº. de Derecho Constitucional de la Universidad de Granada, donde se estudia sobre el impacto que producen las nuevas tecnologías en el manejo y cruce de datos sensibles (Guerrero, 2004).

- “La gestión de la confianza en internet: un factor clave para el desarrollo de la economía digital”, de septiembre/2005 en el deptº. de Economía y Dirección de Empresas de la Universidad de Zaragoza, que versa sobre las dificultades de los usuarios a la hora de realizar transacciones mercantiles a través de la red debido a las dudas sobre las garantías de privacidad de los mismos (Guinaliu, 2005).
- “Derecho, internet y protección de los consumidores en la Unión Europea”, de mayo/2008 en el deptº. de Derecho privado en la Universidad de Extremadura sobre aspectos similares al caso anterior, más ceñidos al ámbito europeo. (de Villamor, 2008).

A su vez, en TDR (tesis doctorales en red), encontramos el estudio de una inquietud con un contenido más próximo a nuestro tema de investigación:

- “Security and privacy issues in some special-purpose networks”, de junio/2008 en el deptº. de Ingeniería Informática y Matemáticas de la Universidad Rovira i Virgili, tratando sobre los problemas de seguridad y privacidad que surgen al implantar en escenarios reales novedosas aplicaciones basadas en nuevos modelos de red que difieren significativamente de las redes de computadores clásicas y son catalogadas como redes de propósito especial. Específicamente, en este trabajo se estudian, entre otros aspectos, la seguridad de la información y la privacidad de los usuarios en redes sociales, facilitando el mantenimiento de la privacidad (Viejo, 2008).

Siendo un asunto muy sensible, dada la rápida extensión que el uso de nuevas tecnologías tiene entre los jóvenes, hemos visto un gran número de estudios relativos a este tema en diferentes países.

Utilizando recursos de la red como Polibuscador, Revista Psicothema, Dialnet, Scirus, Google Scholar, Pubmed, Journals, y utilizando conceptos de búsqueda tales como: Encuesta motivación aprendizaje seguridad internet / encuestas seguridad informática / redes / constructos / variables latentes / redes sociales / usuario impulsivo / perfil consumidor servicios / Cuestionario para medir el interés en aprender / aprendizaje / medición del interés en el aprendizaje / en aprender / de la confianza / Social networks (social media) risk....., encontramos algunos como los siguientes:

- En estudios sobre competición deportiva vimos el uso de factores cognitivo-afectivos como los motivacionales, la autoeficacia, la autoconfianza, la ansiedad, el logro, la complejidad de la tarea, etc. (Cervelló *et al*, 2002 y 2003).
- Jacqueline Eccles y Allan Wigfield (2002), de la Universidad de Michigan, generaron un modelo sobre las componentes del valor asociado a una actividad. Partiendo de que tanto las expectativas como los valores son creencias cognitivas relacionadas con las decisiones que los sujetos toman de forma consciente sobre sus logros, acaban influyendo en su comportamiento. El valor de logro lo definieron basándolo en cuatro aspectos: valor adquirido (importancia de hacerlo bien), intrínseco (diversión o entretenimiento que les produce la actividad), utilitario (fines obtenidos) y esfuerzo (dedicación, ansiedad). Con estos cuatro componentes asociados a una actividad concreta podemos definir el valor que dicha actividad puede tener para una persona.

Es decir, estamos ante un modelo racional de toma de decisiones sobre la motivación que influyen en el comportamiento de los estudiantes en las escuelas técnicas que vamos a estudiar.

- Cuestionarios con este tipo de variables fueron usados por Baca Lobera (2005) del deptº de Producción Económica de la Universidad Autónoma Metropolitana Xochimilco, de México en el estudio de los factores que influyen en el estudio de las Matemáticas, así como por Irene Sánchez Guevara (2009) del dptº de Política y Cultura de la misma universidad. Utilizando sensaciones de motivación, agradable, utilidad, confianza, ansiedad y conocimientos.
- “Variables motivacionales, estrategias de aprendizaje y rendimiento académico en estudiantes universitarios: Un modelo de relaciones causales”, de Ramón González *et al* (1998) de la Universidad de La Coruña.
- También usó estos conceptos para las variables Raquel Salim (2004 y 2006), de la Universidad Nacional de Tucumán (Argentina) en sus artículos sobre “Herramienta de evaluación de enfoques de aprendizaje en estudiantes universitarios” y “Motivaciones, enfoques y estrategias de aprendizaje en estudiantes de Bioquímica de una universidad pública argentina”, utilizando el cuestionario CEPEA (Cuestionario de Evaluación de Procesos de Estudio y

Aprendizaje) y analizando motivaciones de interés, logro, miedo al fracaso. O bien Gómez-Borja, (2011), en su estudio sobre las motivaciones de uso de redes sociales.

- Angeles Blanco (2008), en una investigación sobre las actitudes de los estudiantes universitarios hacia el estudio de la Estadística hace referencia a valores de Afecto (sentimientos), Competencia cognitiva (actitudes), Valor (utilidad) y Dificultad (complejidad, esfuerzo) y en su trabajo evoluciona hacia Utilidad, Ansiedad, Confianza, Agrado, Motivación, Interés.

Comprobamos que, en todos los estudios, se van concretando unas motivaciones similares en todos ellos.

Estudios posteriores de Bayot Mestre (2008) o de José García Clavel y Javier Balibrea (2010) se basaron en la investigación de factores como los descritos (adquirido, intrínseco, utilitario, esfuerzo).

En el primero de estos últimos estudios mencionados se destacaba la importancia del estímulo que supone la motivación para la educación, aunque no fuese medible directamente. Se definían los denominados intangibles de la educación (factores no cuantificables, inherentes al estudiante) y su influencia en el rendimiento académico, así como la forma en que son medidos por PISA²⁹ (interés, la autoconfianza y el disfrute que se obtiene con el estudio). Tengamos presente que los informes PISA no se limitan a una mera evaluación de conocimientos, sino que también tratan de medir las actitudes y la implicación de los alumnos respecto las ciencias usando intangibles como los mencionados.

En el segundo estudio se analizaron los factores latentes ante la actitud hacia el estudio de la Estadística por los estudiantes universitarios, obteniendo cuatro dimensiones básicas que definieron como: interés, ansiedad y utilidad inmediata y para su futuro. En este trabajo también se analizan las variables latentes a través del sesgo que supone el rendimiento académico de los estudiantes.

²⁹ Programme for International Student Assessment

El interés nos impulsa a explorar una determinada situación. Nos da la voluntad suficiente para suplir nuestras deficiencias o limitaciones, nos estimula y facilita la comprensión y el aprendizaje (Fink y Samuels, 2007).

La autoconfianza mide la propia imagen o percepción que cada uno tiene de sí mismo respecto ciertos retos.

El disfrute facilita el esfuerzo requerido para superar el aprendizaje.

- En un contexto diferente (investigación sobre siniestralidad laboral), vimos la combinación del uso de variables latentes (estrés, apoyo y seguridad) con variables mediadoras que tienen el papel de clusterizar a través de determinados comportamientos. (López-Araujo y Osca, 2010)
- Hoofnagle, C. *et al* (2010), de la Universidad de Berkeley, estudiaron el comportamiento sobre privacidad en internet que adoptan los jóvenes americanos.
- López *et al* (2010) de las universidades de Granada y la Autónoma de Yucatán elaboraron un cuestionario adaptado para conocer las actitudes respecto el aprendizaje de las Matemáticas.
- Investigaciones sobre el uso del PC por parte de los docentes utilizan criterios de utilidad, ansiedad, atracción. (Peinado; Bolívar; Briceño, 2011)
- “Teenagers, Legal Risks and Social Networking Sites”, desarrollado por los profesores Melissa de Zwart y David Lindsay (2011), de la Monash University en Victoria (Australia), abordaron el incremento de complejidad que está suponiendo el uso de redes sociales en la comunicación y los problemas de seguridad y de riesgos legales entre estudiantes que llevan consigo, además de las percepciones de los adultos.
- “Adopción de redes sociales virtuales: ampliación del modelo de aceptación tecnológica integrando confianza y riesgo percibido”, de Carlota Lorenzo Romero (2011), que establece relaciones causales entre confianza y riesgo percibido, como factores de incertidumbre del comportamiento y del entorno, a partir de un modelo de Aceptación de la Tecnología que contempla constructos actitudinales tales como utilidad y facilidad de uso.

Según íbamos avanzando, analizando nuestros propios resultados y sacando las correspondientes conclusiones, seguíamos buscando nuevos estudios similares al nuestro, encontrando los siguientes:

- “Youth, Privacy, and Reputation”, de los profesores Marwick, Murgia Díaz y Palfrey (2010), de la Universidad de Harvard, que estudia el riesgo con el que los jóvenes se comunican a través de redes sociales y sus motivaciones. Referencian estudios en los que han encontrado que el 47% de jóvenes incluyen información de “comportamiento de riesgo” que asocian a las actividades sexuales, el consumo de alcohol y drogas. También hacen referencia a estudios de 2006 en los que el 64% de jóvenes usuarios de Redes Sociales mantiene la configuración de privacidad que, por defecto, proporciona la plataforma.
- “Los efectos de la motivación, la confianza y la preocupación por la privacidad en las redes sociales”, de Shi-Woei Lin y Yu-Cheng Liu (2012), de la Universidad de Taiwán, relacionando parámetros medibles del nivel de uso de las redes sociales con parámetros emocionales. Hicieron dos pilotos con unos 30 encuestados y, finalmente, con 207. Utilizaron herramientas estadísticas básicas: correlaciones, índices de fiabilidad, regresión, constructos.... Hacen referencia a razones extrínsecas e intrínsecas (interés, estrés....), estudiando riesgos de privacidad en redes sociales, teniendo en cuenta confianza y motivaciones.

Es decir, comprobamos que prácticamente nuestros antípodas tienen unas inquietudes similares a las nuestras, se han dado cuenta también del riesgo, las están trabajando y utilizan teoría similar de apoyo a la que usamos nosotros, encontrando una intensa correlación entre la frecuencia de navegación por las redes sociales y la revelación de información (0,499), con significatividad³⁰ <1%, afirmando que sus resultados “*indican que la confianza puede efectivamente mitigar la preocupación de un usuario por su privacidad*”.

³⁰ La significatividad mide el grado de error

Finalmente, aún más recientemente, en la Universidad Nacional de Singapur encontramos otra investigación que reconfirma la preocupación sobre el tema objeto de la presente tesis:

- Jiang, Z. *et al* (2013), en sus trabajos sobre privacidad en Redes Sociales, hacen referencia a investigaciones en USA que indican que entre el 43 y el 51% de los encuestados dan información personal (domicilio, e-mail, creaciones personales, fotos, vídeos, asociaciones, opiniones) en las Redes Sociales.

Por otro lado, comprobamos que diversas universidades han detectado la demanda de una oferta formativa para paliar las carencias de los usuarios en temas de seguridad informática cercanos al objeto de esta tesis y están promocionando actualmente una parte de sus actuales cursos abiertos, masivos y en línea (MOOCs) para facilitar la formación de seguridad en internet.

Entre ellas, utilizando la plataforma coursera.org:

- Universidad de Michigan, con el curso “*Análisis de redes sociales*”³¹, que ayuda a proteger la formación de la identidad digital y la difusión de la información, o el curso sobre “*Historia, tecnología y seguridad en Internet*”³², que informa sobre como asegurar las comunicaciones en internet, proteger la información y establecer la identidad.
- Universidad de Washington, con “*Construcción de un sistema de gestión de riesgo para la información*”³³, que da enfoques de gestión de riesgo para guiar las decisiones de seguridad de la información, así como evaluar, desarrollar y mantener prácticas para mitigar los riesgos. También imparten cursos de “*Diseño y ejecución de estrategias para la seguridad de la información*”³⁴, con aplicaciones prácticas de casos actuales de riesgo, o “*La seguridad de la información y la gestión de riesgo puestas en contexto*”³⁵, para prevenir ataques de e-crime y mantener estrategias para defender la privacidad individual.

³¹ <https://www.coursera.org/course/sna>

³² <https://www.coursera.org/course/insidetheinternet>

³³ <https://www.coursera.org/course/inforisk>

³⁴ <https://www.coursera.org/course/infosec>

³⁵ <https://www.coursera.org/course/inforiskman>

[Consultadas el 19 de Marzo de 2015]

- Universidad de Maryland, dispone del curso “*Seguridad utilizable*”³⁶, que se centra en diseñar sistemas de seguridad desde la óptica más humana de riesgos, la más crítica por falta de sensibilidad o escasa atención a las habilidades cognitivas con respecto a contraseñas, protocolos de seguridad, compartición de información, etc., que son los factores que pueden entrañar mayor riesgo. Dan formación sobre los principios básicos de la interacción persona-ordenador, incluyendo principios de usabilidad, habilidad, aprendizaje y motivación.
- Universidad de Londres, que anuncia “*El software malicioso y su mercado negro: las dos caras de la moneda*”³⁷, con amplia información sobre la ciberdelincuencia y la concienciación de adoptar medidas preventivas y técnicas prácticas y efectivas de mitigación.
- Finalmente, a través de la plataforma miriadax.net, también se difunde el curso de la Universidad Europea de Madrid: “*Derecho y Redes Sociales*”³⁸, con una aproximación a las complejidades jurídicas y los retos para los usuarios que supone su navegación, así como a la forma de proteger factores como privacidad, identidad digital, o propiedad intelectual.

³⁶ <https://www.coursera.org/course/usablesec>

³⁷ <https://www.coursera.org/course/malsoftware>

³⁸ <https://www.miriadax.net/web/derecho-redes-sociales>

[Consultadas el 19 de Marzo de 2015]

3.- MODELO PROPUESTO

3.1 Estrategia para el desarrollo de la investigación

Con los antecedentes teóricos vistos, el soporte metodológico de nuestra investigación también será la Encuesta Social teniendo en cuenta que, tal y como definen la investigación experimental Hernández; Fernández, y Baptista (2003), es la que se lleva a cabo sin manipular variables; es decir, sin variar de forma intencionada variables independientes para ver su influencia sobre otras variables, estudiándolas tal y como surgen de forma natural para ser analizadas.

Su objetivo será conocer si los alumnos encuestados, que supuestamente tienen la suficiente formación (aptitud), son conscientes del riesgo que corren cuando navegan por internet y acceden a redes sociales con la suficiente inquietud (actitud) para evitarlos, o el deseo de conectarse es tan fuerte que no consideran prioritarias su propia seguridad e intimidad, Monsoriu (2008).

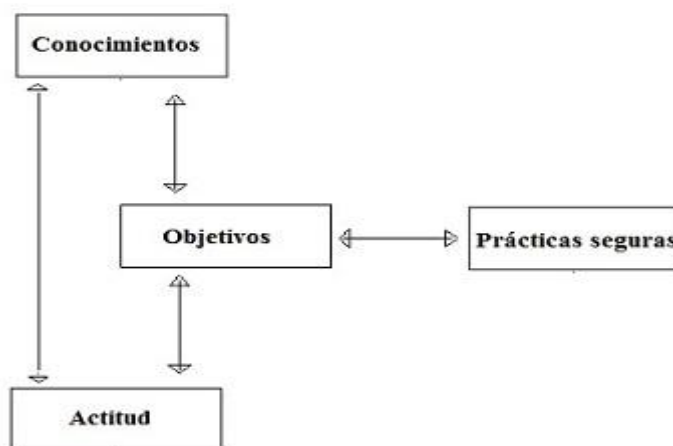


Fig .28: Objetivos del estudio (EP)

La encuesta es una herramienta adecuada para explorar en esta cuestión, corroborado suficientemente por la amplia teoría referenciada en el punto anterior, en la que cada una de las preguntas conlleva la construcción de una variable denominada latente, que será la representación de un conjunto de preguntas en un cuestionario que se calificará con la escala ordinal de Likert. Dichas variables latentes o constructos serán los que miden tanto la “aptitud”, mediante un test de conocimientos sobre seguridad, como la “actitud”, a través de los valores de motivación establecidos en la literatura revisada.

Concretamente, planteamos la relación entre las formas de navegar por la red y el conocimiento de los riesgos (factores actitudinales frente aptitudinales) teniendo en cuenta sus motivaciones y su posible preocupación para conocer los vínculos entre “privacidad / confianza - seguridad - temor por riesgo / utilidad / interés / conocimientos” que nos lleva a proponer un modelo teórico inicial que nos sirva de base y guía en la recopilación de datos y su análisis. Las variables independientes son las latentes que definiremos en nuestro modelo y la variable dependiente será la que mide los conocimientos sobre seguridad de los encuestados mediante un test, calificado a través de la variable “nota”, utilizando variables de control sobre seguridad y privacidad, que analizaremos conjuntamente.

En nuestro estudio debemos tener presente la forma en que esas componentes se combinan para darnos información sobre las actuaciones que influyen en el comportamiento de los estudiantes encuestados, planteándonos inquietudes tales como:

- la concepción que el alumno tiene sobre la necesidad de estar al corriente sobre técnicas de seguridad,
- la autoconfianza en su forma de adquirir conocimientos,
- la ansiedad que le produce alcanzar los conocimientos necesarios durante el proceso de aprendizaje, y
- también el gusto o no por la materia misma, objeto de aprendizaje.

Todos ellos determinantes, de manera conjunta, para el logro de la adquisición de conocimientos e información para poder seguir navegando con seguridad.

El tipo habitual de preguntas utilizado en los estudios referenciados (punto 2.3) se basa en los llamados cuestionarios CEPEA (Cuestionario de evaluación de procesos de Estudio y Aprendizaje) para el alumnado universitario, traducido por Alfonso Barca Lozano (1999) del original "*The study Process Questionnaire (SPQ): Manual Hawthorn*", de Biggs (1987), con una segunda versión (Biggs, 2001), y el MEVA (*Motivaciones, expectativas y valores-intereses relacionados con el aprendizaje*) publicado por Alonso (2005) así como el MSLQ (*Motivated strategies for learning questionnaire*) usado por Wolters, Pintrich y Karabenic (2003) para el autoaprendizaje en e-learning, enfocándolos a las necesidades específicas de cada investigación.

Por ejemplo la variable utilidad de la seguridad, se construye con preguntas del estilo:

- a) Considero la seguridad (informática o de navegación) como un tema muy necesario en el desenvolvimiento de mi actividad diaria
- b) La navegación por redes sociales puede ser útil tanto a nivel personal como para el que se dedique a la investigación o para el profesional.

El análisis de las variables manifiestas: edad, sexo, curso, tipo de acceso se hará de manera descriptiva e inferencial.

Hemos tenido en cuenta lo que dicen Medina Rivilla y Castillo Arredondo (2003: 258) al aplicar el cuestionario necesario para conocer fenómenos sociales: *« es una forma de encuesta caracterizada por la ausencia del encuestador, por considerar que para recoger información sobre el problema objeto de estudio es suficiente una interacción impersonal con el encuestado»*. Es decir, se trata de una técnica de recogida de información a través de las respuestas obtenidas de los encuestados que son interrogados y en la que las preguntas se realizan siempre en el mismo orden y con los mismos términos. Esto nos garantiza el orden y la terminología aplicada de forma sistemática a lo largo del tiempo, siendo válida para posteriores investigaciones que permiten obtener resultados comparables en el tiempo a poblaciones distintas.

Se utilizan escalas Likert (1932) para medir las variables identificadas como motivaciones, introduciendo preguntas de control para asegurar coherencias dado el eminente carácter subjetivo de las respuestas.

El alcance de los resultados obedece a la realidad Nomotética, o búsqueda cuantitativa de las leyes generales de la conducta, no debiendo olvidar que el descubrimiento solo se considera logrado cuando ha sido confirmado por los números y repetidas investigaciones. Como decía William Thomson, más conocido por su título nobiliario de Lord Kelvin (Holton, 1987: 275):

“Cuando se puede medir aquello de lo que se habla y expresarlo en números, es cuando se conoce algo de ello; pero cuando no se puede medir, cuando no puede expresarse en números, el conocimiento es poco satisfactorio; puede ser el comienzo del conocimiento, pero apenas se ha avanzado, con estos pensamientos, para llegar al estado de Ciencia, cualquiera que sea la materia de que se trate”

3.2 Táctica para el desarrollo de la investigación

El cuestionario a utilizar debe incluir preguntas para cubrir cada tema de interés, de tipo explicativo, abiertas y/o cerradas (dicotómicas o Likert), introductorias, de control, de relleno, tales como: Edad, sexo, curso, años por curso (para el curricular) y, las que miden las motivaciones, los sentimientos e intereses que producen al encuestado el aprendizaje de temas de seguridad informática, lo que llamaríamos variables actitudinales, además del test para medir el nivel de conocimiento de esos temas.

Dado el elevado número de candidatos a ser encuestados (varios centenares) utilizaremos medios electrónicos para el relleno y tratamiento de las respuestas por parte de nuestro público objetivo que serán los alumnos de la Facultad de Informática y la Escuela de Telecomunicación de la Universitat Politècnica de València. Elegimos esa población por tratarse de un conjunto de jóvenes que, por su edad y estudios realizados podemos considerar más afines al uso de las herramientas TIC, dentro del conjunto de usuarios habituales de estas facilidades puestas al alcance de cualquier individuo en nuestro entorno.

Nos plantearemos un primer análisis de tipo descriptivo (tablas de frecuencias, medidas de tendencia central, variabilidad, representaciones gráficas, etc.) con SPSS³⁹, para establecer perfiles diferentes dentro del grupo de estudio para continuar con un diseño correlacional (tabulaciones cruzadas, medidas de asociación, indicadores de correlación, explicación de varianzas), seguido de análisis exploratorios (factoriales) para entender el grado de influencia de unas variables en otras y conocer cómo se comportan los sujetos a partir de las variables relacionadas, asegurando la coherencia en las respuestas e idoneidad del planteamiento.

Cuando hablábamos de los objetivos de la investigación, en el punto 1.2, nos preguntábamos sobre los factores de actitud y motivación con mayor influencia sobre los conocimientos sobre seguridad informática necesarios para navegar con mayor tranquilidad y menor riesgo y si sería posible conseguir un cambio en dichas actitudes. A la vista de la literatura consultada y siguiendo su forma de proceder, para responder a

³⁹ *Statistical Package for the Social Sciences*

la primera pregunta y reflexionar sobre la segunda, se construirá y analizará un modelo conceptual con ecuaciones estructurales confirmatorio sobre las actitudes que influyen en el desempeño de los estudiantes. Dicho modelo incluirá un gráfico en el que se especifiquen las relaciones supuestas entre el conjunto de variables latentes (utilidad, ansiedad, confianza, interés, etc.) que se definirán en nuestro modelo inicial, en el que se incorporará una variable adicional con el resultado del test de conocimientos, calificado con una hoja Excel.

Comprobaremos si nuestro modelo inicial, que será similar a los de otras investigaciones, se ajusta a los datos y responde a nuestras hipótesis de forma que, comprobando la calidad del mismo, examine una serie de dependencias simultáneas con la capacidad de representar conceptos no observados en esas relaciones, indicando la medida de error en la estimación, a la vez que nos facilita averiguar las razones que justifican determinados comportamientos en los diferentes grupos de alumnos, así como sus hábitos y medidas adoptadas de acuerdo a su conocimiento sobre prácticas de protección, tanto durante el uso de las herramientas TIC como al navegar por la red, midiendo su preparación y concienciación.

Las estimaciones del modelo se llevarán a cabo usando los métodos del análisis multivariado (mínimos cuadrados generalizados), con el programa AMOS, de SPSS que esencialmente consisten en usar dos o más variables para representar el comportamiento interrelacionado, multidimensional y complejo del proceso de aprendizaje en sus vertientes individual, grupal y organizacional (Gil, 2005). Dicho análisis no se basará exclusivamente en criterios estadísticos, sino también en las formulaciones teóricas iniciales.

Con los resultados obtenidos podremos dar recomendaciones más ajustadas sobre seguridad a cada perfil, y establecer las normas que se deben seguir para poder navegar por internet y participar activamente en foros y redes, minimizando los perjuicios que puedan derivarse de esa misma actuación.

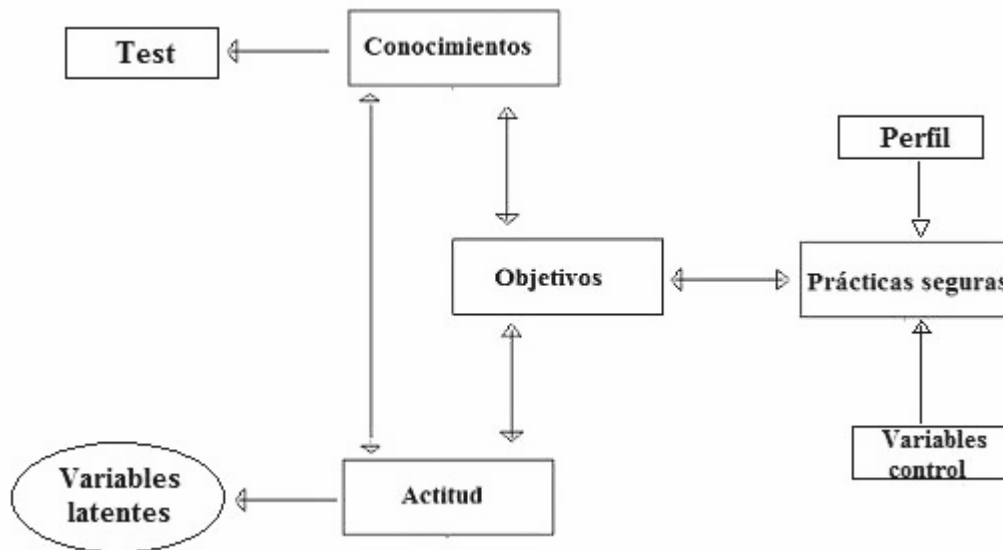


Fig .29: Parámetros de observación del estudio (EP)

Finalizaremos este apartado recordando que el objetivo de la presente tesis es confirmar que existe una relación directa entre los conocimientos sobre seguridad informática, en general, y la conciencia sobre los riesgos de privacidad que asumen los alumnos de las escuelas “más sensibles” de la UPV, como usuarios de redes sociales en internet, siendo precavidos al navegar por ellas. En función de los resultados que obtengamos deberemos estudiar y plantear las mejores opciones para minimizar los posibles riesgos detectados. Ya sean acciones formativas específicas, campañas de comunicación, recomendaciones sobre inclusión o modificación en temarios, dentro del ámbito universitario que nos ocupa. Lógicamente, de no confirmarse la hipótesis, deberemos indagar en las razones que justifiquen las lagunas de conocimiento o sensibilidad, a fin de proponer las soluciones que se encuentren más adecuadas para evitarlo.

3.3 Modelo inicial de estudio

En base a las investigaciones previas de otros autores, anteriormente descritas en el capítulo de Marco teórico, nos planteamos el modelo más apropiado para nuestros objetivos, que será con el que se estudie la muestra de la población seleccionada.

Los factores de motivación que queremos estudiar fueron definidos por Githua y Mwangi (2003) a través de las variables latentes: *interés, confianza, utilidad satisfacción*. A su vez, Jacqueline Eccles y Allan Wigfield (2002) ya habían utilizado esas mismas variables, así como posteriormente Baca Lobera (2005), Angeles Blanco (2008), Bayot Mestre (2008), García Clavel y Javier Balibrea (2010) y otros autores referenciados en el punto 2.3. También nos mostraremos receptivos a otras actitudes, como la *ansiedad*, estudiada por diversas teorías relacionadas con las anteriores, que se verán en la tabla 4, como parte de un constructo determinante de las actitudes de los sujetos, y la variable manifiesta *conocimiento real* tanto de *herramientas generales informáticas* como *específicas de navegación por redes sociales*.

Esos factores motivacionales que influyen en el comportamiento tienen las siguientes características (Eccles, 2002):

- El valor adquirido se basa en la importancia y confianza de hacer bien la actividad
- El valor intrínseco implica la diversión o entretenimiento de hacer la actividad
- El valor extrínseco es el valor utilitario que se relaciona con los fines obtenidos,
- El valor de esfuerzo, o costo, se refiere a la dedicación o ansiedad que genera hacer la actividad

Las preguntas adaptadas a nuestro caso serán del tipo que pueden verse en la tabla 3, utilizadas por otros investigadores en sus casos particulares (p.e. Baca, 2005 respecto las Matemáticas).

Tabla 3. Indicadores para medir las variables latentes

Constructo o variable latente	Variable observable o indicador
Interés (valor intrínseco)	<i>Estudiar sobre seguridad informática es entretenido</i>
	<i>Si tuviera oportunidad me inscribiría en cursos de seguridad</i>
	<i>Siento curiosidad por las noticias sobre seguridad</i>
Confianza (valor adquirido)	<i>Saber seguridad incrementa mis posibilidades de navegar tranquilo</i>
	<i>Me alegra poder resolver dificultades de seguridad</i>
	<i>Si me lo propongo llego a dominar bien la seguridad</i>
Ansiedad (costo)	<i>Me siento incapaz de comprender algunas cuestiones sobre seguridad</i>
	<i>Estoy preocupado por los riesgos de seguridad</i>
	<i>Me altero cuando tengo que resolver un problema de seguridad</i>
Utilidad (valor extrínseco)	<i>Pienso que la seguridad es muy necesaria para mi actividad personal</i>
	<i>Ídem para la profesional</i>
	<i>Pienso que los conocimientos sobre seguridad son previos a la utilización de PC's</i>
	<i>Pienso que debo saber utilizar los recursos de protección de mi PC</i>

Fuente: Cuestionario adaptado de Autoeficacia académica de Greene y Miller (1996)

Vamos a comparar en la tabla 4 la convergencia de criterio respecto los constructos utilizados en los modelos estructurales referenciados, y que corresponden a estudios similares encontrados en la teoría descrita sobre investigaciones, que utilizaban variables latentes equivalentes y que pueden verse más detalladamente en el Anexo 1.

Analizando las coincidencias respecto las motivaciones descritas por esos autores en el siguiente cuadro resumen comprobamos, en primer lugar, el factor común en la mayoría de ellos sobre la importancia de Utilidad y Confianza.

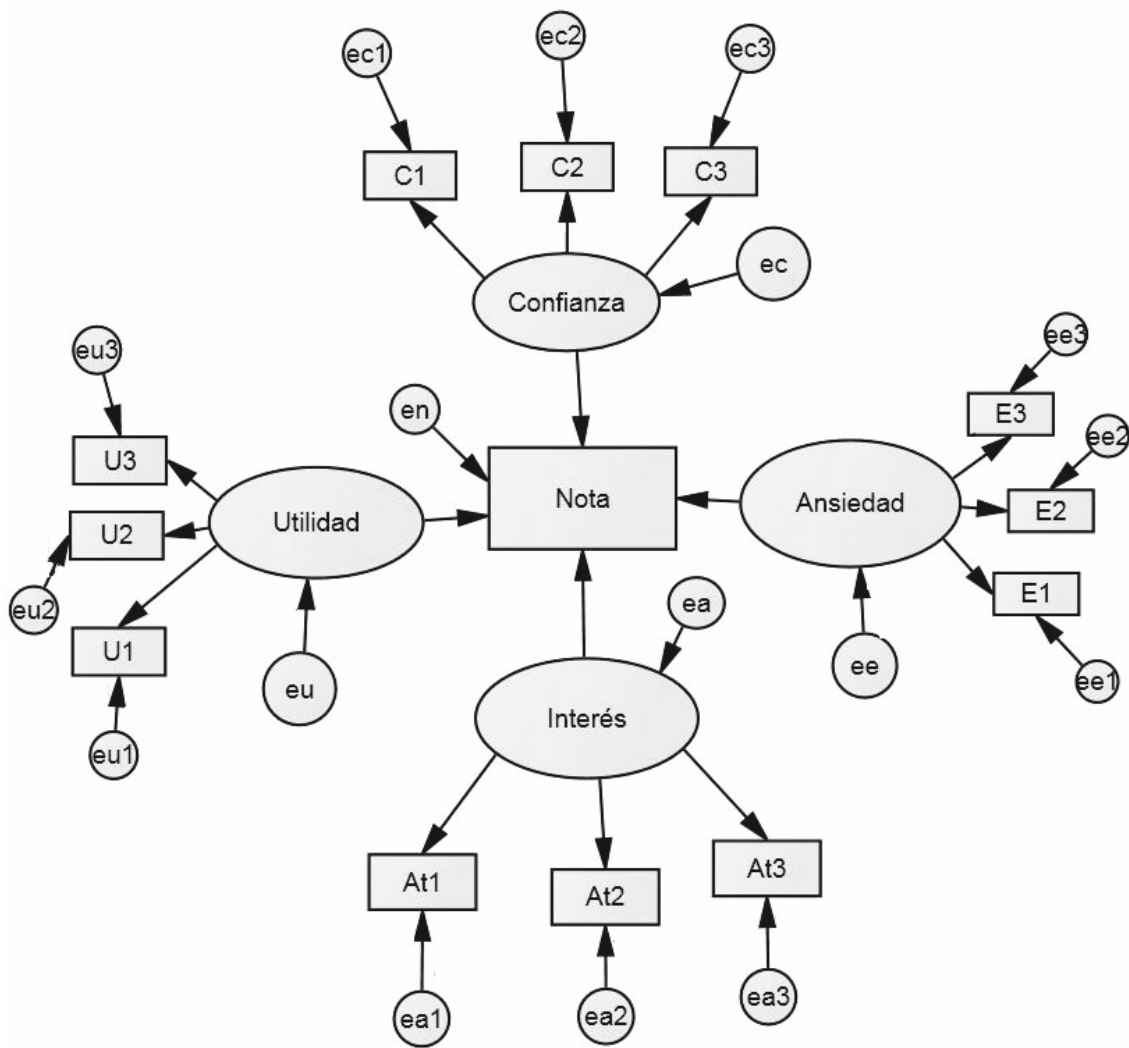
Tabla 4. Motivaciones descritas por autores consultados

Variable latente	Davis	Baca	Martínez	Sánchez	Lorenzo	Rejón
Utilidad	X	X	X	X	X	X
Facilidad	X				X	X
Actitud	X		X		X	
Interés		X				
Ansiedad		X		X		
Confianza		X	X	X	X	
Conocimientos		X		X		
Motivación				X		
Satisfacción				X		
Riesgo					X	
Intención					X	X
Normas						X
Imagen						X

Fuente: EP

En nuestro caso particular, debemos añadir la necesidad de la variable “Conocimientos” para cumplir con los objetivos de la investigación y también la del factor Interés pues tiene una componente de Motivación-Intención-Actitud definido por cada autor. Sin olvidar incluir en la Ansiedad el reflejo del Riesgo.

En consecuencia, vamos a partir de las variables definidas por Githua y Mwangi (2003) y utilizadas por Baca Lobera (2005) para definir nuestro modelo del grafo 1, sobre las que aplicaremos las variables de control, independientes y exógenas, para cada caso de estudio.

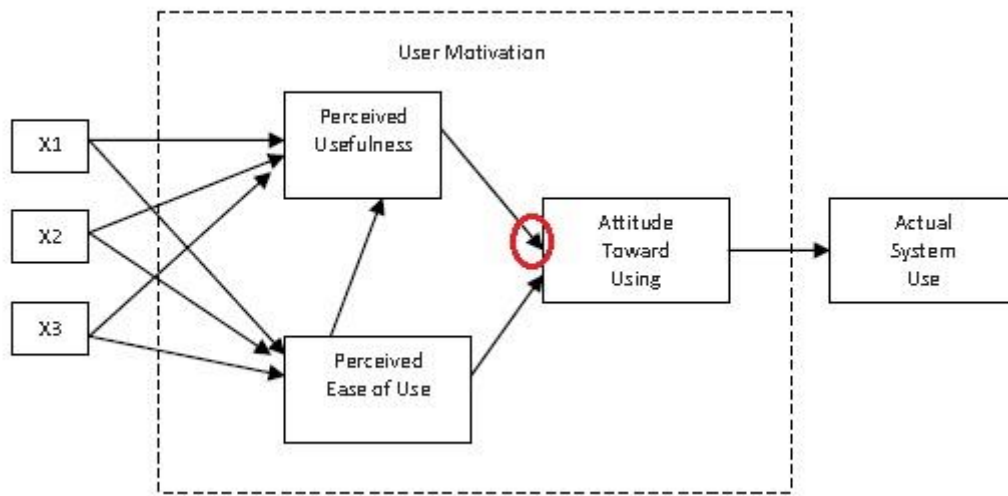


Grafo 1. Modelo estructural teórico – (EP)

También hemos tenido en cuenta que, como decía Sáez (2004: 252): “*en cualquier modelo conceptual hay que elegir los elementos que más convienen, según la situación para la que esté previsto aplicarse*”. Avalado por Beer (1985) quien confirmaba que un modelo no es verdadero o falso, sino más o menos útil, citado por Sáez (2004)

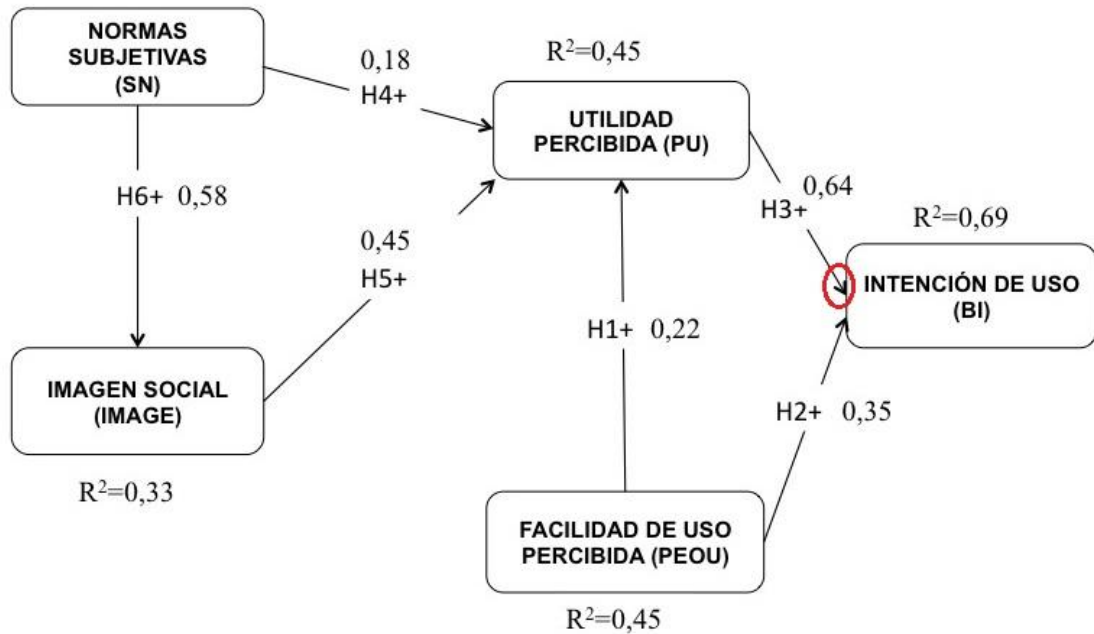
Revisando la convergencia de criterio respecto trayectorias de causalidad en los grafos mostrados en los modelos estructurales de estos mismos estudios y que, como hemos dicho, pueden verse más detalladamente en el Anexo 1, encontramos las analogías siguientes (para facilitar la comprensión del lector, se resaltan con círculo rojo las direcciones causales de los constructos de nuestro interés utilizados en cada estudio):

- Vinculación entre Utilidad y Facilidad, respecto la Actitud, indicando causalidad entre la Utilidad percibida y la Actitud hacia el uso (Interés)



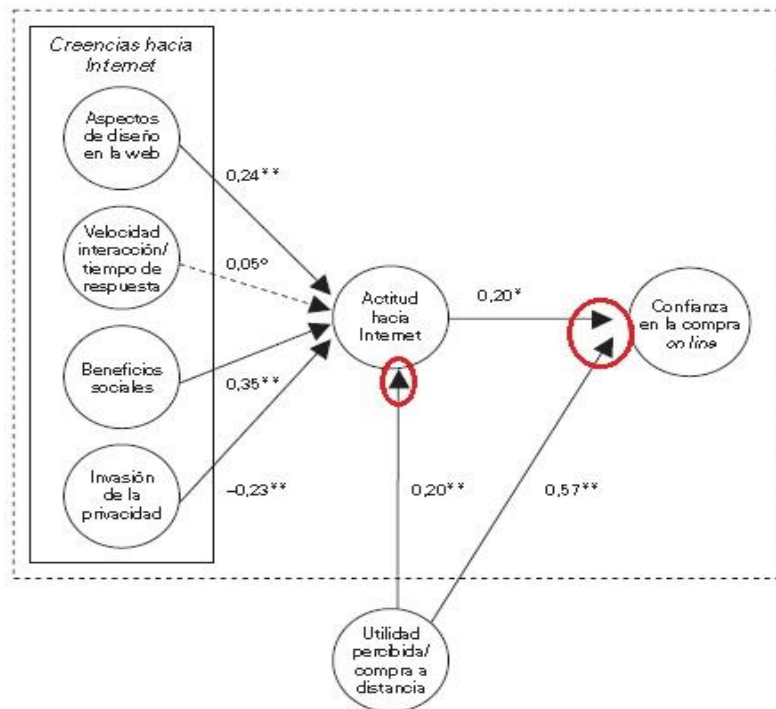
Modelo TAM de aceptación de la Tecnología (Davis, 1985)

- Relación entre Utilidad, Facilidad, Normas, Imagen e Intención, donde también se anticipa causalidad entre Utilidad e Interés por el uso



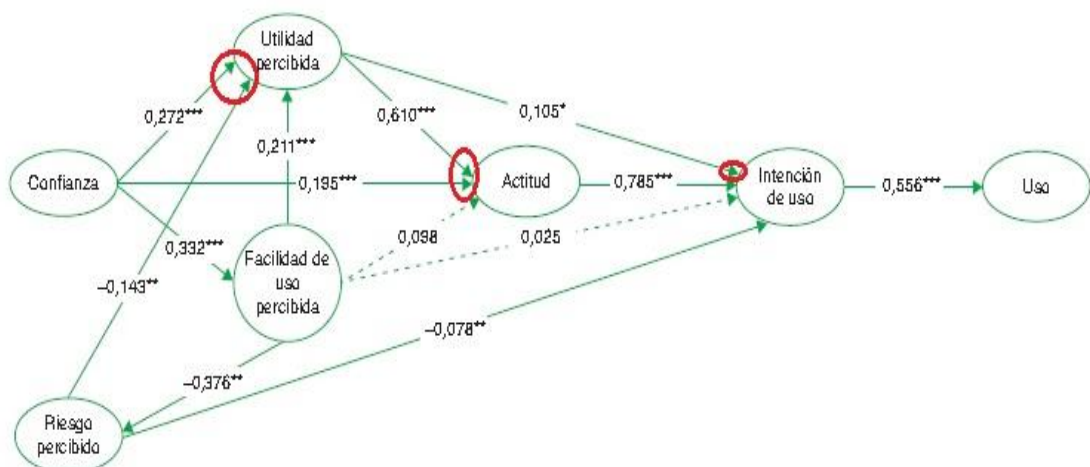
Modelo de aceptación de redes sociales de microblogging (μBTAM) (Rejón; Liébana y Martínez, 2011).

- Influencias entre variables Utilidad, Confianza y Actitud, siendo estudiada la Utilidad como causa de la Actitud (Interés) y de ambas sobre Confianza



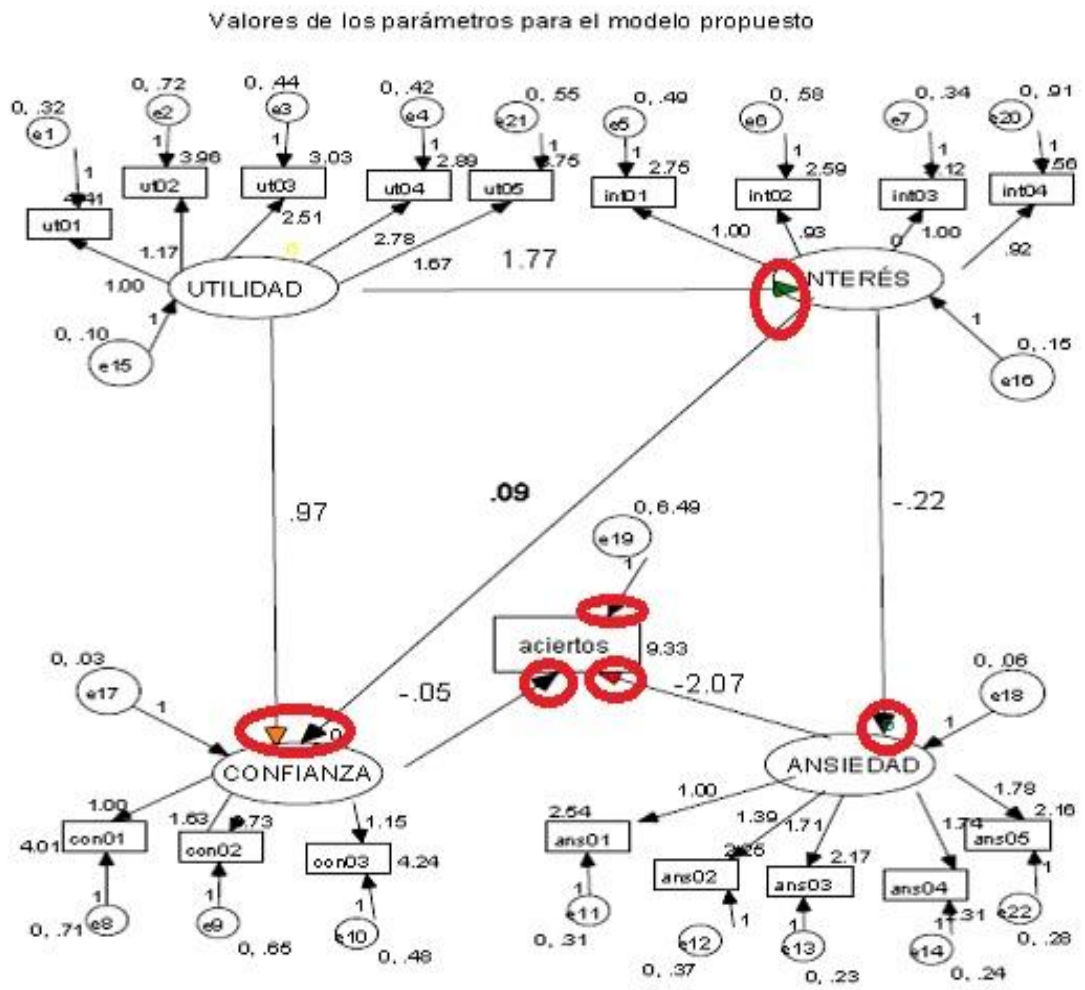
Modelo de confianza del consumidor en la compra a través de internet (Martínez *et al*, 2006)

- Efectos entre Utilidad, Confianza, Riesgo, Facilidad, Actitud e Intención, basado en el modelo de Davis con la Utilidad causa de la Actitud e Intención pero como efecto de Confianza, según un tipo de hipótesis no refrendado



Modelo causal utilizado en la adopción de redes sociales virtuales (Lorenzo, 2011)

➤ Relaciones entre Utilidad, Interés, Ansiedad, Confianza y Conocimientos



Modelo causal utilizado en investigación educativa (Baca, 2005)

Este modelo nos señala las siguientes causalidades:

Utilidad → Interés

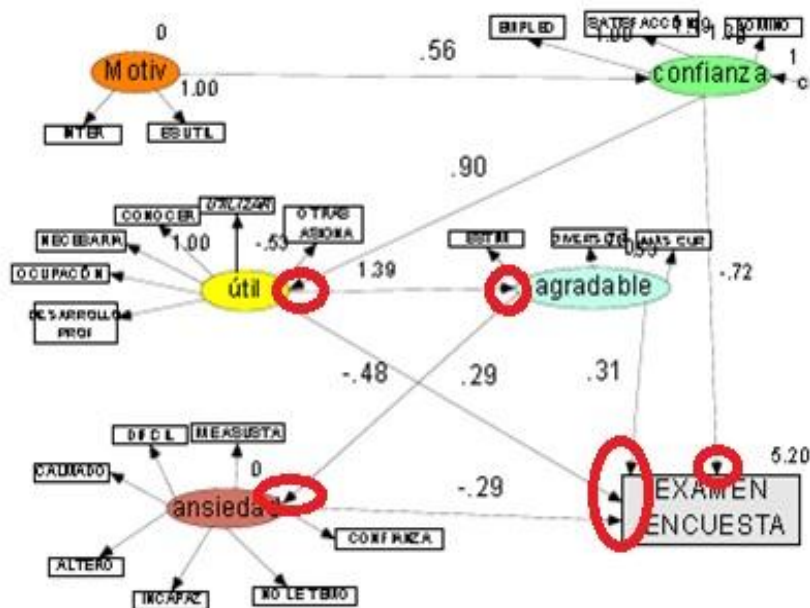
Utilidad → Confianza

Interés → Confianza

Interés → Ansiedad

Entre latentes y nivel de Conocimientos

➤ Motivación, Confianza, Utilidad, Ansiedad, Satisfacción, Conocimientos



Modelo causal utilizado en la enseñanza-aprendizaje de Matemáticas (Sánchez, 2009)

En este caso se invierte la causalidad entre Utilidad y Confianza, pero también se relacionan las latentes con el nivel de Conocimientos

Desde el modelo genérico inicial propuesto en el grafo 1, indicaremos en el siguiente grafo (1bis) las relaciones causales (resaltadas en rojo) que recogen las motivaciones de los modelos descritos por la teoría revisada, añadiendo la posible influencia entre Utilidad y Riesgo, o sensación de Ansiedad o estrés⁴⁰, propuesto adicionalmente por el modelo de Lorenzo (2011) para el caso de redes sociales (en el que obtiene resultado negativo → inverso) y siendo de interés para el nuestro.

⁴⁰ Recordando la nomenclatura:

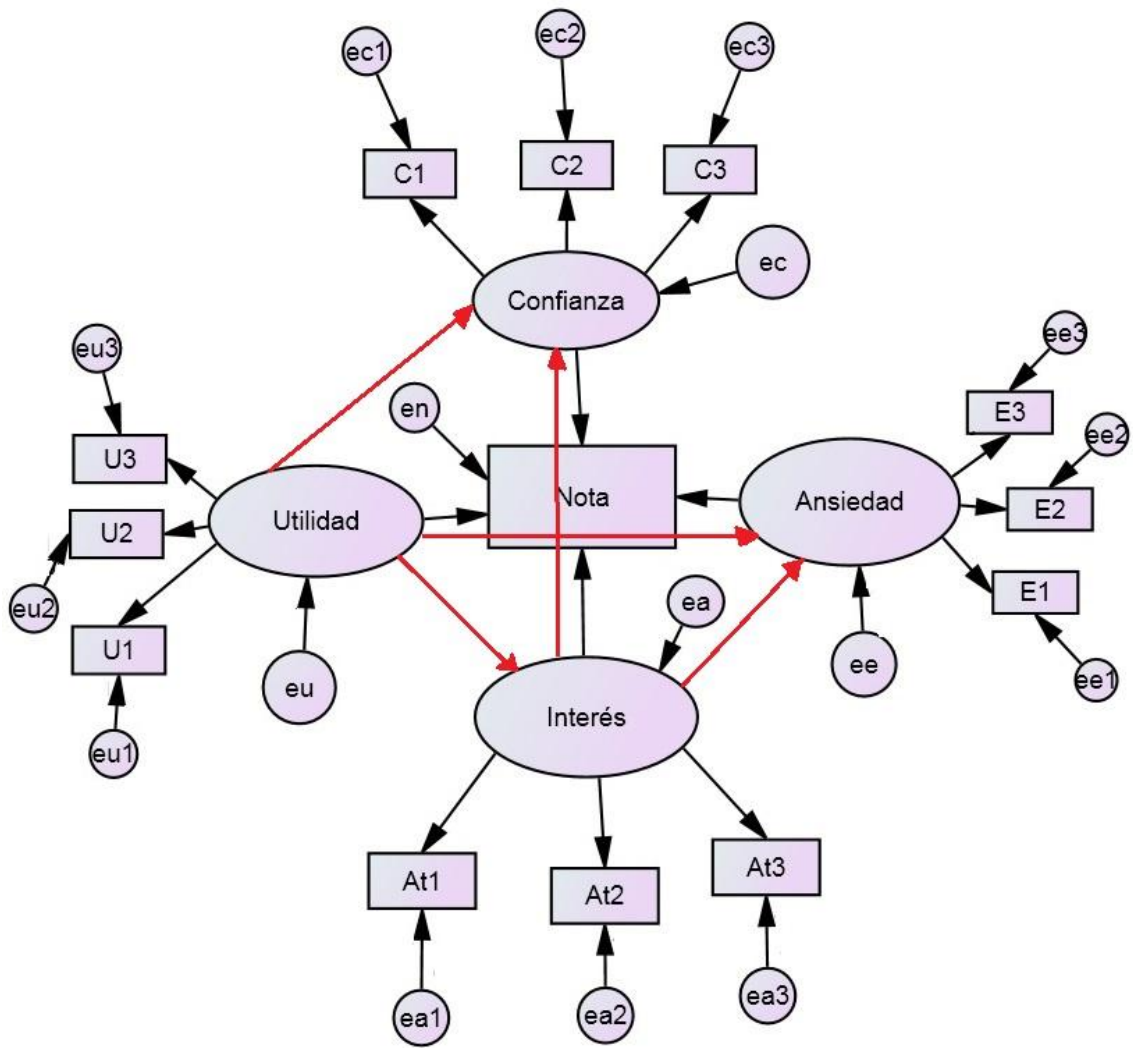
Ansiedad \cong estrés = .. = -facilidad percibida = riesgo

Interés = atractivo = agradable = actitud positiva hacia... = intención de uso

Confianza

Utilidad

Aciertos = nota



Grafo 1bis. Modelo estructural causal teórico – (EP)

3.4 Hipótesis

En muchos trabajos de investigación cuantitativa los objetivos de investigación se formulan como una o más hipótesis, pudiéndolas definir como una suposición sobre las características con las que se da en la realidad el fenómeno social en estudio; o bien como una conjetura de las relaciones que se dan entre características o variables de ese fenómeno. Como un problema de investigación es una pregunta que se plantea el investigador con el propósito de darle una respuesta correcta, también se puede decir que la hipótesis es la respuesta anticipada que el investigador propone a la pregunta, respuesta que someterá a verificación empírica con los datos que recoja, ya sea de manera directa o indirecta. Además, no toda suposición es una hipótesis, lo es cuando ella se formula dentro de un conjunto de conocimientos ya acumulados sobre el objeto de investigación o dentro de la problemática teórica o práctica que lo rodea. En este caso, esos conocimientos constituyen el fundamento de la hipótesis (Briones, 2002)

Las hipótesis científicas son enunciados teóricos supuestos, no verificados pero probables, referentes a variables o la relación entre variables que se pueden definir como soluciones probables previamente seleccionadas al problema planteado que el científico propone para ver si son confirmadas por los hechos, a través de todo el proceso de la investigación.

Nos guían y orientan el proceso de la investigación. Formular hipótesis, antes de recolectar los datos, es como hacer apuestas previas y luego echar los dados. El científico apuesta a que los hechos se producirán conforme a lo planteado en sus hipótesis y busca la evidencia de los hechos que las corroboren o contradigan. No es posible el camino contrario en el que un investigador recoge datos de la realidad y en función de ellos formula hipótesis adecuadas a los hechos hallados. Las hipótesis se deben plantear antes de recoger la evidencia empírica y el investigador debe orientarse, en su actuación, según lo hipotéticamente planteado. En definitiva, como decía Darwin: *“todas las observaciones han de ser a favor o en contra de algún punto de vista si se quiere que sean útiles”* (Kerlinger, 2002: 26).

Según Ruiz (2006), la hipótesis es una suposición que establece relaciones entre los hechos o fenómenos, mediante dos o más variables (independiente y dependiente), y a la que todavía falta una comprobación, usando términos inequívocos, sin ambigüedades en la interpretación y debiendo evitar el uso de términos valorativos.

Existe una estrecha relación entre la determinación del problema a investigar y las hipótesis. Podríamos incluso decir que la formulación de hipótesis es la operación subsiguiente a la determinación del problema en el proceso investigador.

En la literatura referenciada se formulan diversos tipos de hipótesis que intentan averiguar las relaciones entre las percepciones (Utilidad, Confianza, Ansiedad e Interés) por los diversos aprendizajes, con los conocimientos adquiridos o pendientes de conseguir y se analizan para distintos grupos de alumnos.

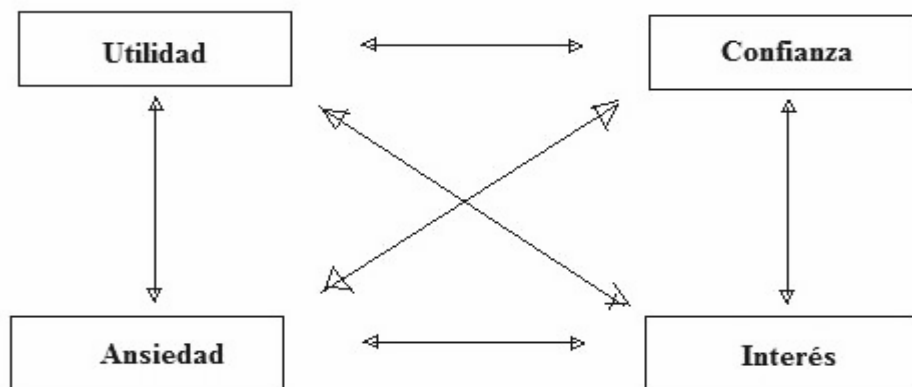


Fig .30: Latentes comunes (EP)

Hemos visto algunas agrupaciones de hipótesis que convergen con las principales dimensiones (utilidad, facilidad de uso y actitud) del modelo TAM (Davis, 1985) con la confianza y la percepción de riesgo.

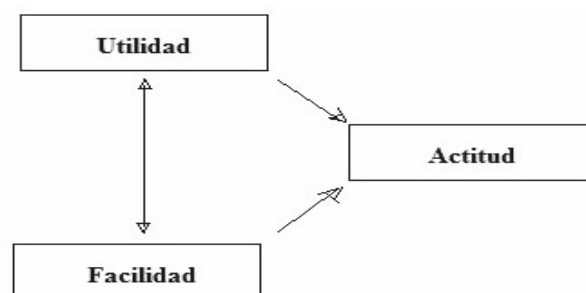


Fig .31: Influencias en la actitud (EP)

La facilidad de uso tiene una relación directa con la actitud, reduce el esfuerzo para conseguir los resultados (Davis *et al*, 1992) e implica también a la utilidad (Davis, 1989; Davis *et al*, 1989; Shih, 2004; Liaw y Huang, 2003). Es decir, deberíamos plantear una hipótesis sobre las relaciones entre la facilidad de uso percibido respecto las redes sociales y su influencia positiva sobre la actitud y la utilidad hacia estas plataformas. En nuestro caso concreto, la sensibilidad por la protección de su información y privacidad son factores a considerar.

A su vez, tanto la facilidad de uso, como la utilidad percibida forman parte de la actitud (Davis *et al*, 1989) lo que nos lleva a considerar que la utilidad percibida tiene influencia positiva sobre la actitud hacia las redes sociales.

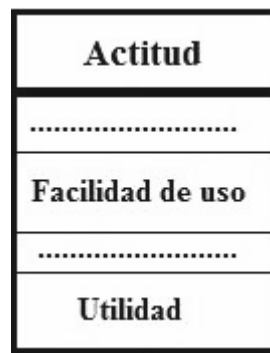


Fig .32: Relaciones actitudinales (EP)

Por otra parte, la confianza es importante para conseguir nuevos usuarios. De hecho ya lo definimos en el apartado 2.1.2 de desarrollo del uso de internet. Ejerce un efecto determinante sobre la intención de uso y la actitud, demostrado empíricamente (Alsajjan y Dennis, 2006; Shin, 2008). Con una mayor confianza necesitamos menos esfuerzo para navegar por las redes sociales y son más fáciles de usar, lo que nos lleva a que la confianza tiene efecto sobre la utilidad percibida (Alsajjan y Dennis, 2006; Pavlou, 2003). Con lo cual, deberíamos enunciar hipótesis sobre la influencia de la confianza sobre la actitud hacia la utilización de redes sociales, sobre la utilidad percibida y sobre la facilidad de uso.

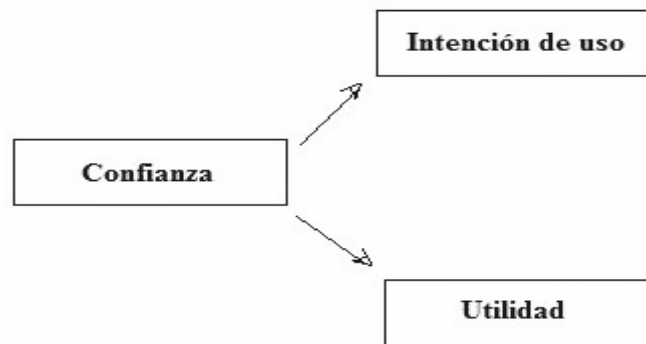


Fig .33: Influencias de la confianza (EP)

Con respecto al riesgo, disminuye la utilidad percibida, la intención y facilidad de uso (Pavlou, 2003) y nos lleva a plantearnos hipótesis sobre estos efectos negativos.



Fig .34: Influencias del riesgo (EP)

En nuestra investigación, *la lógica de los programas educativos de las respectivas titulaciones nos debe llevar a formular las afirmaciones* que, como propuesta de hipótesis, queremos contrastar.

El orden en que las vamos a enunciar no indica su importancia sino que es más bien un orden lógico en el que comenzamos planteando las hipótesis relacionadas con los objetivos específicos (Henº), agrupándolos por los perfiles básicos de seguridad, seguimos con las hipótesis (Hnº) vinculadas a las motivaciones de los alumnos al utilizar las herramientas TIC y terminamos con las hipótesis vinculadas con el objetivo general (Hgnº):

a) Para los objetivos específicos:

- Respecto la protección de sus equipos vamos a comprobar las siguientes afirmaciones, observándolas en función de sus conocimientos:

- ✓ He1: Los alumnos TIC aprovechan el uso de contraseñas para proteger sus equipos y/o archivos
 - ✓ He2: Los alumnos TIC utilizan copias de seguridad para salvaguardar su información
 - ✓ He3: Los alumnos TIC mantienen actualizados recursos de protección
 - ✓ He4: Los alumnos TIC están informados de las novedades de seguridad informática
 - ✓ He5: Los alumnos TIC cuidan la privacidad de su actividad en la red, procurando no dejar rastro de la misma
- Respecto los factores de motivación o percepciones de Utilidad, Confianza, Ansiedad e Interés:
- ✓ H1: Podemos establecer que existe covarianza positiva entre los valores de utilidad percibida por los alumnos encuestados, interés por el conocimiento de prácticas de seguridad y preocupación por las posibles consecuencias de la navegación por internet.
 - ✓ H2: La percepción de utilidad de las herramientas de seguridad favorece el acercamiento a su conocimiento; es decir, comporta mayor interés
 - ✓ H3: La confianza alta se asocia positivamente con la privacidad
 - ✓ H4: La confianza alta se asocia positivamente con la protección
 - ✓ H5: La preocupación alta por la privacidad se asocia positivamente con las medidas de protección
 - ✓ H6: Los alumnos con más conocimientos se sienten más atraídos por el uso de medidas de seguridad
 - ✓ H7: Los alumnos con más conocimientos sienten más útiles las medidas de seguridad
 - ✓ H8: Los alumnos con mayores conocimientos cuidan más su privacidad

- ✓ H9: Los alumnos con mayores conocimientos cuidan más su protección
- ✓ H10: Los alumnos con menos conocimientos se estresan más fácilmente
- ✓ H11: Los alumnos con menos conocimientos tienen menos confianza
- ✓ H12: El modelo teórico queda ajustado a través de los factores de conocimientos, interés, utilidad y preocupación
- ✓ H13: Los alumnos que cuidan su privacidad ajustan mejor el modelo propuesto
- ✓ H14: Los alumnos que protegen sus datos ajustan mejor el modelo propuesto

b) Para el objetivo general, además de los específicos vistos y completarán la respuesta a nuestras preguntas, utilizaremos las siguientes hipótesis para cuando navegan por redes sociales:

- ✓ Hg1: Los alumnos TIC definen su perfil, adaptándolo a sus necesidades y/u objetivos
- ✓ Hg2: Los alumnos TIC son cuidadosos con sus datos personales
- ✓ Hg3: Los alumnos TIC son prudentes cuando se expresan

Los propios resultados podrán recomendar nuevas aseveraciones a tener en cuenta.

4.- METODOLOGÍA

"Probamos por medio de la lógica, pero descubrimos por medio de la intuición"
(Henri Poincaré)⁴¹

⁴¹ Matemático, físico, científico teórico y filósofo de la ciencia francés. (1854-1912)

4.1 Metodología para el estudio de campo de la tesis doctoral

En toda investigación es fundamental asegurar que los hechos y relaciones que establecemos, o los resultados y nuevos conocimientos obtenidos, tengan la mayor exactitud y confianza. Para lograrlo planificamos la metodología, o procedimiento ordenado, que tuvimos que seguir para establecer las conclusiones hacia las que encaminamos nuestra investigación.

Desde un punto de vista meramente científico, podemos asegurar que la metodología es el procedimiento general para lograr de una manera precisa el objetivo de la investigación. En consecuencia, la metodología nos servirá para determinar los métodos y técnicas para la investigación.

El tipo de investigación de nuestro caso será el descriptivo correlacional con el propósito de describir cierta situación, especificando propiedades de personas bajo el fenómeno sometido a análisis, para lo que seleccionaremos una serie de cuestiones que serán medidas para poder detallar lo investigado, analizando las variables propuestas y el grado de relación entre varias de las propuestas, verificando si están relacionadas o no en los mismos sujetos para intentar conocer cómo se comportan sabiendo la evolución de otras variables relacionadas. Esta correlación podrá ser positiva o negativa según sigan la misma tendencia, o contraria o ninguna, en las variables analizadas.

La población quedará determinada por las características que la definen, llamando así al conjunto de sujetos que tengan algo en común, en nuestro caso la de estudiantes de técnicas TIC de la UPV. Esta población es la que recibe mayor formación sobre el fenómeno que vamos a estudiar y es la que da origen a los datos de la investigación.

Una vez obtenidos los datos por los medios definidos para este fin hay que procesarlos; o sea, elaborarlos matemáticamente, ya que su cuantificación y su tratamiento con herramientas estadísticas nos permitirán llegar a conclusiones en relación con las hipótesis planteadas. Para dicho proceso de datos, utilizaremos algunos de los programas de ordenador más habituales y de reconocido prestigio.

Es necesario elaborar muy detalladamente la investigación de campo que vamos a seguir (cuestionarios, encuestas...) compatibilizándola con una investigación más de tipo documental, concretamente hemerográfica (basada en artículos y estudios en revistas y periódicos especializados). Este conocimiento hace posible evitar equivocaciones en la elección del método adecuado para un procedimiento específico.

Abordamos la investigación partiendo de los conocimientos de educación básica sobre procedimientos TIC de los estudiantes, ya que van a estar siempre presentes en la forma de actuar de nuestra población y nos informan sobre el alcance que se debería dar a nuestro estudio. Sin querer cometer uno de los fallos más comunes en muchas investigaciones que hemos anticipado anteriormente, la falta de delimitación del tema o exceso de ambición, por lo que es necesario tener muy claros los objetivos y el camino que se va a recorrer con la investigación para que esta pueda terminar donde queremos.

Vamos a exponer las etapas metodológicas utilizadas para evaluar y analizar el modelo de nuestra investigación. Para facilitar el soporte teórico hemos incluido en el Anexo 2 (puntos A.x) una descripción de las razones del uso cada vez más frecuente de los métodos cuantitativos dentro de las Ciencias Sociales mediante un pequeño preámbulo de la investigación científica en las ciencias, así como los conceptos estadísticos utilizados en la presente tesis (Anexo 2 puntos D.x). Con este fin, presentamos los conceptos básicos para ayudar a la comprensión de la metodología. Además se plantearon los pasos a seguir para un análisis multivariante con ecuaciones estructurales (Anexo 2 puntos E.x). Las ecuaciones estructurales se aplican en estudios sociológicos acerca del uso de las redes sociales y en investigación educativa se utilizan para el estudio de la motivación por el aprendizaje y el uso de las nuevas tecnologías para la enseñanza, entre otras. Manzano y Zamora (2009).

El primer paso es la elección de tipo de encuesta a realizar (Anexo 2 puntos B.x), para continuar con la elaboración de cada uno de los elementos del cuestionario sobre las estructuras organizativas y sobre el constructo.

El modelo estructural y los modelos de medida de las variables exógenas y endógenas del tema a investigar se desarrollan en los siguientes apartados del presente estudio y, junto con las Hipótesis que deberemos verificar, dan lugar al modelado de ecuaciones estructurales a analizar. Dicho modelo se expone a través de diversas representaciones

como en un diagrama de caminos, a través de ecuaciones y en forma matricial. Una vez definido el modelo de ecuaciones estructurales, se procede a diseñar el cuestionario para la obtención de información cuantitativa para el análisis del modelo anterior.

En el presente Capítulo se exponen los criterios seguidos para la selección de la muestra utilizada en la investigación, así como el tamaño mínimo necesario para obtener un valor significativo razonable, estadísticamente válido.

4.2 Herramientas estadísticas utilizadas

Las Ciencias Sociales, con frecuencia estudian conceptos no físicos y abstractos denominados *constructos*, que sólo pueden medirse de forma indirecta a través de indicadores. Para tratar el conjunto de muestras necesarias para poder captar de forma adecuada la complejidad de los fenómenos en estas áreas, se han implantado métodos multivariantes o multivariados, los cuáles permiten analizar simultáneamente conjuntos amplios de variables. El número de métodos y técnicas multivariantes utilizado es muy amplio. Entre las más comunes destacan la regresión múltiple, el análisis factorial, el análisis multivariante de la varianza, y el análisis discriminante para determinar que cada constructo es significativamente diferente del resto (Anexo 2 puntos D.x). Utilizaremos el software SPSS para el análisis de nuestro caso. Cada una de estas técnicas es una poderosa herramienta a la hora de tratar un amplio abanico de cuestiones prácticas y teóricas, sin embargo todas las mencionadas tienen una limitación en común: sólo pueden examinar una relación al mismo tiempo.

La utilización del modelo de ecuaciones estructurales se considera una extensión de varias de las técnicas multivariantes como la regresión múltiple, el análisis factorial principalmente y el análisis de senderos. El modelo de ecuaciones estructurales abarca una familia entera de modelos conocidos por muchos nombres, entre ellos análisis de la estructura de covarianza, análisis de variable latente y análisis factorial confirmatorio.

Los Modelos de Ecuaciones Estructurales son muy útiles para estudiar las posibles relaciones causales de tipo lineal sobre estos conceptos. No prueban de forma determinante la causalidad, pero facilitan la labor del investigador en la toma de decisiones, negando las hipótesis causales cuando se contradicen con los datos, esto es, con la estructura de covarianzas o correlaciones subyacente entre las variables. Se trata de una técnica que combina tanto la regresión múltiple como el análisis factorial (Casas, 2002)

Combinando todos esos conceptos podemos describir, gráfica y analíticamente las relaciones que creemos existen entre nuestras variables observables y entre estas y las no observables, tomando en cuenta la dirección de cada una de tales relaciones. A partir de nuestra información muestral podemos estimar tales relaciones y juzgar su importancia simplificando los diagramas iniciales hasta obtener un modelo parsimonioso, el más simple, en el que cada variable tiene cierta relación con las demás pero sin redundancias que miden lo mismo y con correlaciones que explican el modelo.

Paralelo al camino estadístico hacia estos modelos de ecuaciones estructurales (SEM, por Structural Equations Model) ha habido un desarrollo computacional representado por software como AMOS asociado al paquete estadístico SPSS. Se trata de una aplicación que crea modelos de ecuaciones estructurales para apoyar teorías e investigaciones yendo más allá de los métodos de análisis multivariante, regresión, análisis factorial, correlaciones o análisis de varianza. Al presentar nuestro modelo a través de AMOS obtendremos las posibles relaciones entre las variables. De hecho, cualquier variable numérica, tanto observada como latente, se podrá utilizar para predecir otra variable numérica, desarrollando modelos de actitud y comportamiento que reflejen relaciones complejas de forma realista. AMOS incluye opciones ampliadas de estadística basadas en la estimación Bayesiana. Aprovecharemos la funcionalidad que permite analizar datos de distintas poblaciones simultáneamente, tales como grupos étnicos múltiples. No solo se evalúan esas complejas interrelaciones de dependencia, al mismo tiempo también se incorporan los efectos del error de medida sobre los coeficientes estructurales.

La estimación de cualquier tipo de modelo estadístico es su interrelación al planteamiento de una teoría debidamente asentada en el área de conocimiento pertinente

Esto es particularmente exigible en un área de modelamiento tan flexible como la de las Ecuaciones Estructurales, lo que se refleja en la preocupación por especificar e identificar el modelo. El primer aspecto se refiere al correcto planteamiento del sistema de ecuaciones en función de la teoría subyacente (cumplimiento de supuestos básicos, definición de algunos parámetros como fijos y otros como libres o estimables); el segundo tiene que ver con que la cantidad de información disponible sea suficiente para tener una estimación única de los parámetros libres, más de una o ninguna.

La metodología de Modelos de Ecuaciones Estructurales es un área de la Estadística en desarrollo siendo muy joven frente a los modelos de regresión o el análisis factorial. Tiene un carácter más confirmatorio que exploratorio; de hecho, el Análisis Factorial Confirmatorio es un caso particular de los Modelos de Ecuaciones Estructurales. La mayoría de las técnicas multivariadas son de carácter exploratorio, ya que buscan patrones generales definidos por los propios datos observados. El SEM, por el contrario es de carácter confirmatorio: el diseño de relaciones entre las variables debe ser explicitado a priori sobre la base de expectativas teóricas, como hemos hecho en nuestro caso desde los modelos descritos del Anexo 1. Esta característica distintiva de este tipo de modelos, los hace especialmente adecuados para testear modelos teóricos mediante la utilización de datos empíricos.

Se parte de una hipótesis, teóricamente pertinente en el contexto de interés. Una ventaja de este enfoque es su capacidad de elaborar constructos que estiman las variables latentes en función de algunas variables medibles. Los modelos SEM expresan la relación entre distintas variables, las cuales pueden ser directamente observables o no observables (Loehlin, 1992; Schumacher y Lomax, 1996).

Los modelos de ecuaciones estructurales se componen de dos modelos que son complementarios, el de medición y el estructural, propiamente dicho. El modelo de medición incluye las correlaciones entre cada constructo y las variables observables que lo definen. El modelo estructural es aquel componente del modelo general que describe relaciones causales entre variables latentes. Las relaciones entre las variables dependientes e independientes, sean medibles o latentes, se incluyen cuando estas variables no actúan como indicadores de las variables latentes (Bentler y Bonett, 1980).

El modelo estructural se representa como: $\eta = \beta \eta + \Gamma \xi + \upsilon$, donde:

η representa el vector de las VLs endógenas, ξ el de las exógenas,

β es la matriz de impactos para η , y Γ para ξ , con υ como vector de residuos

Las ecuaciones estructurales lineales representan las relaciones estructurales representando la línea de causalidad entre las variables latentes, endógenas. Hay tantas ecuaciones como constructos endógenos que sean explicados por otras variables exógenas (latentes u observadas).

Los siguientes seis pasos caracterizan el desarrollo de un SEM:

- Especificación del modelo
- Estimación de los parámetros libres
- Evaluación del ajuste del modelo
- Modificaciones del modelo
- Interpretación y comunicación
- Replicación y revalidación.

Lo esencial es tener un amplio conocimiento (teórico y práctico) del área de aplicación para poder formular una hipótesis razonable y sostenible desde la que iniciar el modelo. Silva y Schiattino (2008).

Basándonos en el conocimiento teórico, diseñaremos el modelo que intente representar de forma sencilla la realidad subyacente en las variables latentes, especificando las relaciones entre ellas. El modelo es la representación gráfica de las relaciones existentes entre los factores y variables que nos van a permitir establecer el diagrama estructural de forma que simplifiquemos la realidad compleja que implica. La hipótesis de partida de todos estos modelos es que reproducen exactamente la estructura de varianzas y covarianzas de las variables objeto de estudio, aunque como ya se ha dicho no corroboran ni contradicen la existencia de causalidad.

Se formulan enunciados sobre el conjunto de parámetros, decidiendo entre los que serán libres para ser estimados o fijos, a los que se les asignará un valor dado, normalmente cero. Especificamos los supuestos estadísticos sobre las fuentes de variación y en concreto sobre la forma de distribución conjunta, que en la mayoría de las técnicas empleadas se considera normalidad multivariante. Y precisaremos el comportamiento de las variables no incluidas en el modelo, cuyo efecto se recoge en los términos del error de medida o de perturbación (Cupani, 2008). Habremos cubierto las etapas que aparecen en la figura 35.

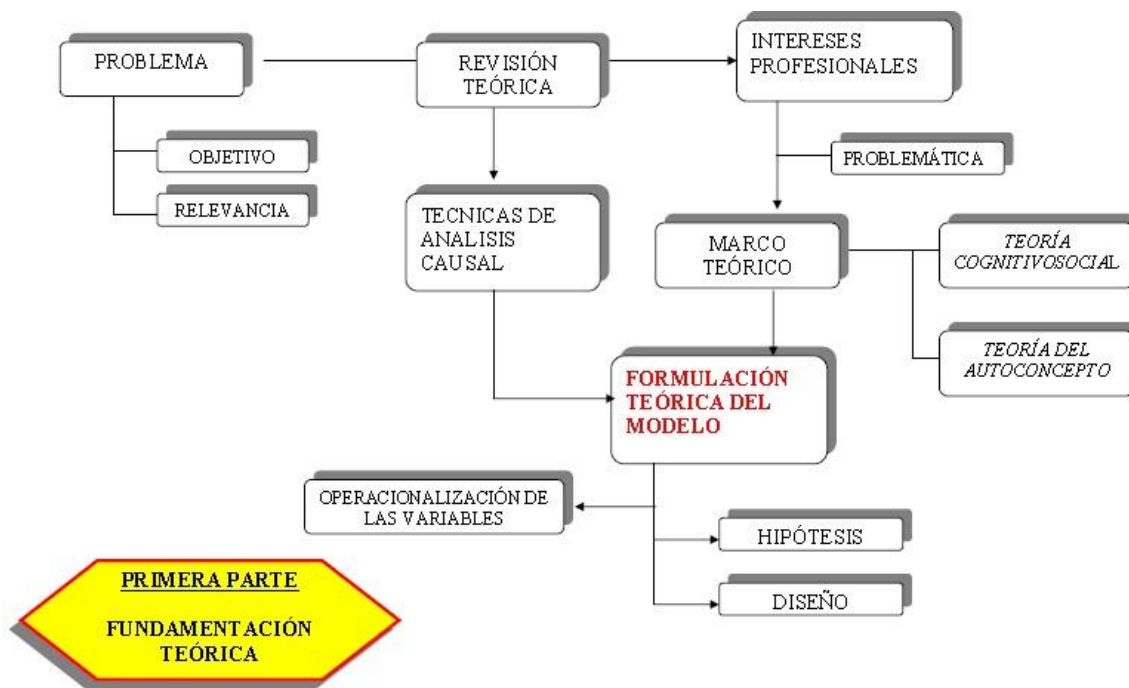


Fig. 35: Fundamentación teórica del modelo de ecuaciones estructurales

Fuente: Hernández (2001).

El siguiente paso será probar el modelo, realizar la medición de la bondad de ajuste entre el modelo inclusivo y el restringido que nos dará la diferencia existente entre el modelo descrito con todas las variables correlacionadas entre sí y el modelo propuesto en el que se limitan esas correlaciones. El resultado debe implicar que el modelo restringido propuesto no debe ser diferente del modelo teórico, inclusivo, en términos de poder explicativo. Las medidas absolutas de ajuste determinan la aproximación con la que conseguimos que el modelo global (de medida y estructural) sea predictor de la matriz de datos. Este modelo lo generará el propio programa estadístico.

Para especificar el modelo de medición del sistema de ecuaciones estructurales, se hace una transición desde el análisis factorial, en el que el investigador no tiene el control sobre qué variables describen cada factor utilizando un análisis exploratorio, a un modo confirmatorio, en el que el investigador si especifica qué variables definen cada constructo.

Por lo tanto, el modelo de medición representa las relaciones de las variables latentes (o constructos) con sus indicadores (o variables empíricas). Para cada constructo que aparezca en el modelo es necesario determinar cuáles serán sus indicadores. Estas variables latentes son variables no observadas, que resultan de las covarianzas entre dos o más indicadores. Son las que representan a los conceptos en los modelos de medición.

El objetivo fundamental del modelo de medición es corroborar la idoneidad de los indicadores seleccionados en la medición de los constructos de interés (figura 36).

La ecuación del modelo de medición mide la relación entre variables exógenas latentes y manifiestas. Las interrelaciones entre las variables latentes se indican mediante sus covarianzas. Las relaciones de las variables latentes con sus indicadores se definen como “direccionales”, de cada variable latente a su manifiesta, y no a la inversa.

La claridad del modelo viene determinada por el grado de conocimiento teórico que tengamos sobre el tema de estudio, si la información es poco exhaustiva o detallada, la asignación de los parámetros será confusa a priori, por lo que tendríamos que realizar diversos análisis exploratorios de los datos hasta configurar el modelo, y efectuar el análisis confirmatorio del mismo. Diversos indicadores nos darán información sobre el ajuste (bondad) del modelo en cuestión (Anexo 2 puntos E.x).

El modelo de ecuaciones estructurales es el que realmente se quiere estimar y es resultado de la combinación del modelo estructural y del modelo de medición de cuyo resultado aparece un modelo comprensivo de relaciones entre variables endógenas y exógenas, latentes y manifiestas. Contiene los efectos y las relaciones entre los constructos (variables latentes) y es similar a un modelo de regresión que puede contener efectos concatenados y bucles entre variables, además de los errores de predicción. Ruiz (2010).

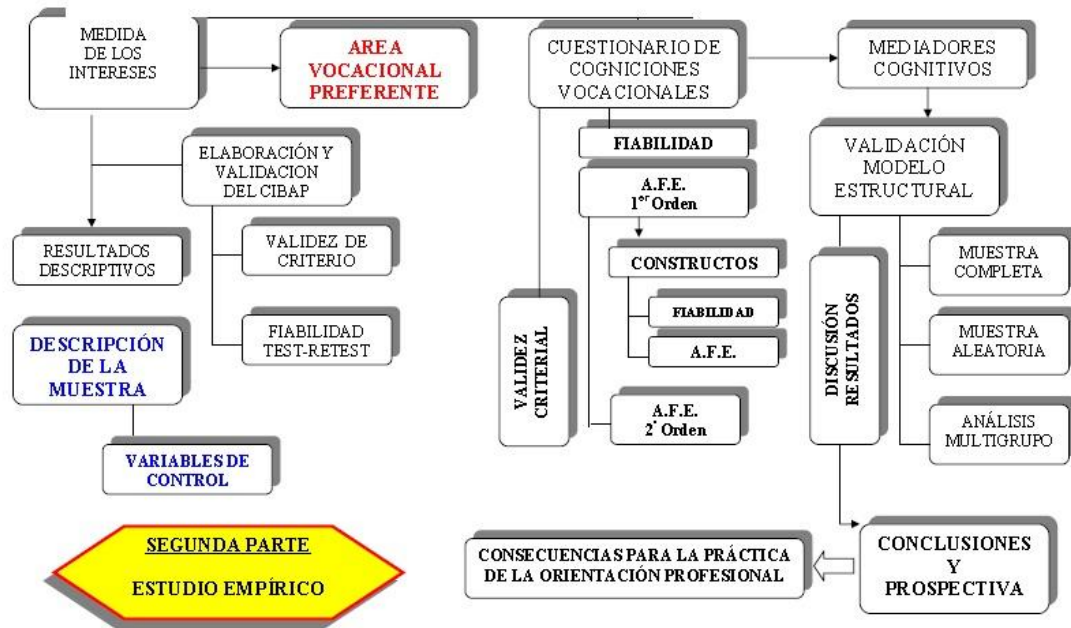


Fig. 36: Fundamentación empírica del modelo de ecuaciones estructurales

Fuente: Hernández (2001)

4.3 Calendario de actuaciones

Durante el verano de 2010 y primer semestre del curso 2010-11, elaboramos el diseño de la Metodología a seguir, supervisada por los directores, profesores del dptº. de Organización de Empresas, D. Juan Vicente Oltra y D. Hermenegildo Gil Gómez, buscando soporte complementario en el profesorado del Dpto. de Estadística e Investigación Operativa Aplicada y Calidad.

Como etapa inicial para abordar el estudio del alcance del riesgo asumido por los usuarios en la navegación por redes sociales, consideramos prioritario asegurarnos de que los conceptos básicos sobre seguridad informática (protección de accesos, adopción de contraseñas, instalación de antivirus y firewalls, generación de copias de seguridad, etc.) se cumplen de forma que podamos continuar nuestro estudio sobre la forma de desenvolverse a la hora de utilizar recursos más complejos, estableciendo comparaciones entre la forma de navegar por internet, publicar información y/o sincerarse en función de su perfil previo de seguridad básica de actuación.

Se prepararon algunos cuestionarios para los alumnos con el objeto de responder a las diferentes cuestiones planteadas, haciendo varias preguntas para cubrir cada tema:

1. Para el ambiente sociocultural del alumno, se preguntaba *la edad, el sexo y la dedicación a navegar por internet.*
2. Para el ambiente curricular de sus antecedentes escolares, se hacían preguntas sobre: *curso y años por curso hasta la fecha.*
3. Para las motivaciones, intereses y sentimientos que le produce el aprendizaje de temas de seguridad informática; es decir, las *variables actitudinales*, se aplicó un cuestionario con cinco variables observables, con escala de Likert (Anexo 2 puntos C.x), para construir las variables latentes de: *ansiedad (esfuerzo, costo), confianza (valor adquirido), interés (valor intrínseco) y utilidad (valor extrínseco)*, sobre los beneficios que el alumno percibe con sus conocimientos de seguridad.
4. Para medir los conocimientos utilizamos un cuestionario que consta de varias preguntas calificadas, dentro de un test en el que se plantean procedimientos

básicos de seguridad, desde establecer passwords hasta conocimientos un poco más profundos, que servirá para contrastar la idoneidad de las respuestas actitudinales, y determinar el nivel de una nueva variable llamada “*nota*”, calificando el test usando funciones de Excel (Buscar-Reemplazar por columnas comparando y asignando +/- 1 y sumando posteriormente las columnas de cada encuestado).
Anexo B2

La información solicitada a través del cuestionario de la encuesta es la incluida en el Anexo A3 y se redactó partiendo de preguntas referidas a los puntos que se quieren analizar.

En la primera quincena del mes de mayo de 2011 desarrollamos un borrador de cuestionario de la encuesta. Aprovechamos la información obtenida al hacer un piloto de la misma con un grupo de alumnos de la Licenciatura de Comunicación Audiovisual del campus de Gandía. Esta experiencia nos permitió verificar la bondad de la misma, tanto desde el punto de vista de comprensión, extensión, etc., como desde el punto de vista de recogida de información, proceso y conclusiones.

En paralelo, debíamos concretar el alcance y perfiles en las respectivas Escuelas / Facultades sobre los cursos a los que pasar la encuesta, realizando las gestiones necesarias para tal fin.

Hicimos dos pilotos previos de carácter presencial con pequeños grupos de alumnos de cuarto de ingeniería de Telecomunicación al final del curso 2010-11 y principio del 2011-12 para asegurar la comunicación, idoneidad de la redacción de las preguntas de la encuesta, así como el entendimiento de las mismas, y/o propuestas que pudiesen hacer los propios encuestados que nos permitiese confiar en el entendimiento de la redacción, aprovechando cuestionarios adaptados para estudios en universidades sudamericanas.

El primer piloto se hizo en clase a 25 alumnos, aprovechando unas tutorías en el mismo mes de mayo-2011. Se propuso el cuestionario a los “alumnos objetivo”, siendo rellenados por los que, voluntariamente, quisieron participar, en soporte de papel, y con un número excesivo de preguntas y perfiles de usuarios (Anexo A1).

Solicitamos a los encuestados que nos hicieran comentarios sobre el cuestionario para mejorar su entendimiento y, con sus sugerencias (resaltadas en el Anexo A1) y la observación de las respuestas, modificamos la redacción de algunas preguntas para facilitar su cumplimentación.

A lo largo de los meses de verano de 2011 (julio-agosto) codificamos las encuestas (Anexo A), tal como se indica en el siguiente apartado para su tratamiento por la aplicación estadística SPSS disponible en la UPV, y las analizamos con ese software ya que proporciona los resultados estadísticos necesarios para evaluar la situación real de riesgo que tratamos de analizar y nos facilita las conclusiones necesarias que indiquen el camino a seguir para minimizarlo.

Mejoramos la siguiente versión de encuesta con algunas cosas como las siguientes:

- Se concretaron mejor algunas alternativas de respuesta para diferenciar mejor, eliminar ambigüedades y no tener ortografías ininteligibles en preguntas abiertas.
- Algunas preguntas con respuesta dicotómica se adaptaron utilizando escalas Likert de cinco posibilidades para mayor información y coherencia en el análisis.
- Se simplificó reagrupando preguntas que medían variables similares.
- Modificamos la redacción de algunas preguntas para clarificarlas.
- Incluimos preguntas de control (sobre protección de acceso al PC) para asegurar coherencias.
- Se eliminaron preguntas de percepción puntual dependientes de causas externas o relativas a incidencias tenidas en el pasado.
- Se reordenaron, juntando las variables que medían percepciones homogéneas.

Incluso algunas preguntas vimos que no nos aportaban información sobre actuación, como por ejemplo:

La 51: “*Usando Wi-fi en casa noto que, a ratos, varía la velocidad*”, cosa que puede producirse por pirateo o por servicio

La 53: “*En alguna ocasión he tenido problemas con algún virus*”, cuando lo importante es saber si he aprendido

Las 58 y 59: “*Cuando envió un mail a varios destinatarios, utilizo la copia oculta*” / “*Cuando envió un mail a varios destinatarios, direcciono a todos directamente para que sepan a quien se lo he enviado*”, lo cual puede ser intencionado o no; es decir, depende de la circunstancia.

La 75: “*Me las leí en su totalidad y las acepté*”, no significa nada reseñable, podrían parecerle bien

El segundo piloto (Anexo A2), se hizo con otros 35 alumnos del mismo curso que los anteriores y también en soporte de papel, nos sirvió para matizar algunos aspectos tales como:

- Excesivo tiempo dedicado a la codificación manual y relleno de la hoja Excel.
- Alto riesgo de errores que exigía repasar los datos, con mayor dedicación.
- Facilitar la codificación eliminando alternativas que permitiesen marcar varias respuestas por variable y tuviésemos que considerarla categórica y analizar por separado
- Pudimos eliminar algunas preguntas que resultaban muy generales, válidas para otros ámbitos, pero que en la población encuestada eran obvias.
- Homogeneizamos la dirección de las escalas (creciente-decreciente).
- Había que recolocar alguna pregunta condicional (la de finalizar la encuesta si no se era usuario de redes sociales)
- Alguna pregunta podía inducir a interpretaciones diferentes. La 47 (*Cuando envió un mail a varios destinatarios, algunas veces utilizo la copia oculta*) y la 48 (*Cuando envió un mail a varios destinatarios, algunas veces direcciono a todos de forma abierta para que sepan a quien se lo he enviado*) con alternativas tipo algunas veces (que puede ser lógico) versus siempre o nunca

Mantendremos las dos preguntas sobre la protección de acceso al PC para verificar coherencia de respuestas al 100%

Hemos reducido de 95 a 66 las cuestiones planteadas, fundamentalmente en:

- 1) Perfil de usuario (hemos pasado de 33 a 17, de los que 8 son las redes sociales a las que se conectan y 6 definen el tipo de usuario de red)
- 2) Actuación, forma de actuar en el día a día, donde hemos reducido de 32 a 25.
- 3) el test de conocimientos lo hemos reducido de 13 a 11 preguntas, eliminando ambigüedades y cambiando alguna. Anexos B y B1.

Entre las preguntas eliminadas se encuentran:

- Si el usuario utiliza PC portátil o sobremesa,...por carecer de interés en el estudio
- La de percepción de variación de velocidad de WiFi, por depender del servicio del operador, de la hora de conexión....
- Tampoco aporta nada el hecho de que “alguna vez” haya tenido virus.
- Se han fusionado las condiciones de registro en redes sociales y las referidas a la privacidad

También cambiamos el orden de las posibles respuestas en algunas preguntas para mantener un sentido homogéneo en los perfiles, de forma creciente o decreciente.

Especificamos más algunas respuestas, a petición de los alumnos, tales como: matizar el nº de asignaturas arrastradas de un curso a otro, los días por semana conectados, la frecuencia de cambio de contraseñas, el tiempo dedicado a redes sociales, los envíos de correos CCO o no y sobre las copias de seguridad.

Redujimos algunas de las opciones ofrecidas con el fin de que se diferencien lo suficientemente como para que no tengan que marcar más de una respuesta, como ocurrió con varios casos en el primer cuestionario con las referidas a frecuencia de establecimiento de contraseñas, sobre si se utilizan reglas mnemotécnicas, accesos al PC, sitios de almacenaje de las copias de seguridad, la frecuencia de las mismas, o la forma de informarse sobre vulnerabilidades.

En resumen, se redujo el número de preguntas, se les dio una redacción más sencilla y se simplificaron las opciones, para hacer más fácil el cuestionario y disminuir el grado de concentración al cumplimentarlo. Adicionalmente, tanto en los cursos de SPSS en el CFP de la UPV, como en diversas referencias, siempre se aconseja que el cuestionario no tenga un excesivo número de preguntas.

Comenzamos con una serie de cuestiones de clasificación sobre variables explicativas (edad, sexo, formación previa, nacionalidad, etc.), continuando con preguntas sobre variables respuesta en las que se incluyeron las de tipo abierto (sin indicación de posibles respuestas), las cerradas (con una relación exhaustiva de respuestas, ya fuesen dicotómicas o de elección múltiple) y las semiabiertas (en las que se incluye la posibilidad de “otras respuestas”).

También se han utilizado:

- Preguntas introductorias (para “situar” al encuestado)
- Preguntas de control (para chequear la coherencia de respuestas)
- Preguntas de relleno (sin mayor trascendencia)

Además, se tuvo en cuenta que algunas respuestas serían no métricas, para las que debemos determinar la forma más adecuada para codificar su estudio, normalmente homogeneizando respuestas mediante palabras clave, y otras si serían métricas o cuantitativas para las que hemos utilizado mayoritariamente las escalas tipo Likert, sencillas de uso y muy adecuadas para medir actitudes.

En definitiva, elaboramos el cuestionario propuesto, tras las modificaciones aconsejadas por las encuestas-piloto, y cuyas respuestas fueron determinantes para obtener la información objeto de nuestro trabajo.

Siendo conscientes de que analizar estadísticamente muestras tan poco significativas (<50 sujetos y con escasa proporción sujetos/variables) no proporcionaría resultados válidos ya encontramos algunos detalles de frecuencias que eran motivo de preocupación.

- La inmensa mayoría (82,8%) mantiene fijas las contraseñas en los diferentes accesos y ninguno las cambia con una frecuencia por debajo de los seis meses y, analizando el comportamiento según la nota obtenida, ni siquiera los mejor calificados cambian las contraseñas con frecuencia y las mantienen fijas en los diferentes accesos. Incluso los de mejor curriculum son poco proclives a cambiarlas.
- La mayoría (79,3%) no se preocupa por hacer copias de seguridad
- También la mayoría (72,4%) guarda las copias en soportes externos, ninguno en la red
- Muchos desconocían el riesgo de conectarse vía Wifi
- Se registran en las Redes Sociales, aceptando las condiciones tal cual, mayoritariamente. Nunca analizan primero esas condiciones, lo importante es estar.
- La mayoría de los alumnos (75,9%) se dio de alta en redes sociales para estar comunicado con los amigos. Resultado de un parecido orden de magnitud (63%) realizado por el análisis “cocktail” patrocinado por Microsoft y BBVA en nuestro país, a población en general, en 2011, que llega al 95% en el caso de Facebook en 2012. (Observatorio, 2011-2012)

Obtuvimos unos resultados muy similares a los reflejados en la tesina del Máster CALSI referenciada anteriormente. Es decir:

- a) Mayoritariamente mantienen fijas las contraseñas, modificándolas con muy poca frecuencia
- b) Son muy escasos los que se preocupan por hacer copias de seguridad
- c) Desconocen los riesgos y, en consecuencia, las medidas a adoptar para protegerse en caso de accesos inalámbricos
- d) Se registran en Redes Sociales sin preocuparse por las condiciones de registro y, en consecuencia, por adaptar su perfil

Por otra parte, observando los resultados que íbamos obteniendo para formar los constructos que queríamos observar (Anexos A1.1 y A2.1), notamos que:

- El constructo “Interés”, observado a través de las preguntas 28, 29 y 30, en el primer piloto daba 0,835 como alfa de Cronbach⁴², así que no cambiamos nada en la redacción de esas variables observables, y en el segundo piloto obtuvimos un valor de 0,721.
- En el caso del constructo “Confianza”, descubrimos que, tras los primeros análisis, la redacción de la pregunta 33 (*Adopto suficientes medidas de seguridad*) podía sugerir las mismas respuestas para alumnos tanto “celosos” como “despreocupados” respecto la variable latente Confianza en la seguridad. De hecho, excepto un encuestado, los que consideraban que no adoptaban suficientes medidas de seguridad se manifestaban preocupados por ese constructo. Y por otra parte había una mayoría entre el resto de los que también se preocupaban, que consideraba que sí adoptaban suficientes medidas. Para mantener la coherencia habrá que redactarla como “prefiero”, o “me gusta”, adoptar las máximas medidas de seguridad.
- El Constructo “Ansiedad”, medido por las respuestas a las preguntas 34, 35 y 36 da un alfa de Cronbach de 0,552, similar al del primer piloto (0,559), por lo que no es necesario modificar ninguna redacción.
- Y, finalmente, en el constructo Utilidad una de las variables era de distinto signo a las demás, lo que nos aconsejaba cambiar su codificación por la complementaria teniéndolo en cuenta a la hora de redactarla nuevamente, llegando a un alfa de 0,632.

Al revisar redacciones y analizar respuestas, en algunos casos surgió la confusión sobre la propia denominación de las variables latentes observadas a través del cuestionario. Hasta este momento, definíamos Interés, Confianza, Ansiedad y Utilidad. Pero, al acudir al Diccionario de Sinónimos (1983), pudimos observar que Interés y Utilidad tienen una significación parecida que puede generar dudas. Así que, pensando en el

⁴² Mide la consistencia de las relaciones entre variables medidas y latente representada verificando si tienen una intensidad equivalente

lenguaje más próximo y actual para la población encuestada, modificamos las denominaciones de esas variables de la siguiente forma:

Interés, por → Atracción (los alumnos se sienten atraídos por una u otra carrera o especialidad o asignaturas opcionales, generando sentimientos afectivos, emocionales)

Confianza, la mantuvimos, pues sus sinónimos son: fe (que puede tener otras connotaciones), seguridad (que puede confundirse con el objeto total del estudio), crédito (que se puede interpretar como capacidad de préstamo, o implicados en un objeto audiovisual), amistad (que ya va por otras acepciones).....

Ansiedad, por → Estrés, término muy en boga en estos tiempos y refleja, perfectamente, lo que queremos dar a entender (agobio, angustia, tensión, desazón, preocupación, zozobra, incertidumbre, agitación...)

Utilidad, habiendo cambiado Interés, que es con la que se confundía, también la dejamos pues queremos significar algo provechoso, práctico, eficaz, conveniente, ventajoso. Refleja el grado por el que una persona cree que al usar un determinado recurso aumentará su rendimiento o productividad.

En definitiva, hablaremos de Atracción, Confianza, Estrés y Utilidad.

Durante el segundo semestre de 2011 buscamos soluciones para conseguir facilitar el rellenado de las encuestas definitivas por medios electrónicos, para evitar el esfuerzo de transcripción y los errores asociados con los que nos encontrábamos respecto a tener que rellenarlas a mano. En su caso, evaluamos aplicaciones disponibles, de libre uso, en internet.

Finalmente se hizo la encuesta vía internet (Portaldeencuestas.com), que nos daba la hoja Excel ya codificada para su tratamiento directo por SPSS y AMOS, incluyendo alguna pregunta adicional, rescatando algunas de las descartadas anteriormente al no haber tenido en cuenta el número de la muestra y obtener resultados insuficientes para completar cinco variables observables por constructo de forma que, con las apreciaciones tanto de los profesores Hervás como Montoro, quedarnos con las tres o cuatro que las correlaciones y el análisis factorial nos recomiendan, y que AMOS necesita (Anexo A3) y en las que quedaron como preguntas de control la 5, 11 y 60. Se pasó esta encuesta al conjunto de alumnos de 2º curso de la Facultad de Informática del

curso 2011-12. En total 235 alumnos. Esta forma de obtener datos mediante encuestados aleatorios voluntarios a través de entornos online se está convirtiendo en práctica habitual en investigaciones que lo permiten. Bagozzi y Dholakia, (2006); Steenkamp y Geyskens, (2006).

Dimos como válidos 204 cuestionarios, al eliminar trece por falta de coherencia en las preguntas de checking (sobre uso de password para acceder a la sesión), ya fuese por falta de concentración, apatía o escaso deseo de colaborar. Otros diecisiete cuestionarios también los eliminamos por falta de respuesta generalizada en un gran número de variables, y un último cuestionario por indicar una edad fuera de rango. En los casos (diez) de encuestas válidas en los que faltaba la respuesta a alguna de las variables necesarias para nuestro estudio utilizamos el método de regresión para con, respuestas similares a las codificaciones disponibles, aproximar los valores ausentes (Anexo C).

Se hizo un primer análisis de tipo descriptivo cuyo fin era establecer perfiles diferentes dentro del grupo de estudio y, a continuación, un diseño correlacional para entender mejor el grado de influencia de unas variables en otras para intentar conocer cómo se comportan los sujetos a partir de las variables relacionadas.

Para el descriptivo se utilizaron tablas de frecuencias, medidas de tendencia central, de variabilidad, representaciones gráficas, etc.

Para el relacional, tabulaciones cruzadas, medidas de asociación, correlaciones, factoriales, etc.

Los resultados estadísticos obtenidos referentes a calidad, explicación de las varianzas e indicadores de correlación obtenidos son muy altos, lo que indica la coherencia de las respuestas y la idoneidad del planteamiento.

Finalmente se diseñaron modelos causales, con análisis de senderos, que fuimos ajustando hasta obtener unos valores muy satisfactorios que aseguraban la bondad del mismo. Desde un modelo inicial en el que utilizábamos todos los valores de las variables observadas (medidas, manifiestas o indicadores), evolucionamos a un modelo más complejo (con mayor número de variables) pero que simplificamos utilizando los valores numéricos de los factores comunes de los constructos que las representaban y que eran suficientes (3-4 variables por constructo) y un número de encuestas válidas que

superaban ampliamente en más de las cinco veces, como mínimo, las variables de estudio.

Tanto en el proceso de los datos con SPSS (Anexo A3.1) como con AMOS, nos apoyamos en los conocimientos desarrollados en los cursos del CFP de la UPV así como en la metodología teórica tratada en diversas aportaciones como las de Carot y otros (2009), Cupani (2008) o Ruiz (2010) para facilitar el estudio de casos en general o la de Corral-Verdugo (1995) aplicada a temas de conducta. Así como las directrices que, para evaluación educativa, reseña Torres (2010) y las directrices del uso estadístico del software orientado hacia las motivaciones (Gardner, 2003).

El soporte teórico estadístico puede consultarse en el Anexo 2

Los resultados obtenidos aconsejaron su constatación mediante nueva encuesta realizada en el curso siguiente (2012-2013) a los alumnos actuales de 2º curso de Informática y a un grupo de alumnos de varios cursos de la ETSI de Telecomunicación. Obtuvimos un total de 192 encuestas válidas, con 87 respuestas de Teleco (28 de primer curso, 39 de cuarto y 20 de quinto) y 105 de Informática, eliminando las demás por razones similares a las comentadas anteriormente. Utilizamos la misma metodología y obtuvimos unos resultados que confirmaban la coherencia con los ya obtenidos con los alumnos del curso anterior (Anexo A3.2).

4.4 Codificación de la encuesta de la tesis

Se detalla el significado de cada una de las variables utilizadas en la encuesta definitiva procesada así como la denominación de las posibles alternativas ofrecida por cada una.

1.- Edad

2.- Sexo: 1=hombre 2=mujer

3.- Rendimiento académico: curso por año / alternativas de repetición

4.- Uso de internet: frecuencia de conexión

5 - 7.- Utilización de contraseñas: Uso / actualización / grabación

8 - 10.- Copias de Seguridad: frecuencia / almacenamiento / actualización

11.- Protección acceso PC (actuación): mínima / media /alta

12.- Prevención mail “ : poca (riesgo alto) / media / alta (riesgo bajo)

13.- Vulnerabilidades “ : “ “ “

14 - 16.- Actividad en internet: básica de navegación / activa en web 2.0 / comercial

17 - 27.- Test de conocimientos (da origen a la variable “notas”)

Redes sociales:

28.- Tipo de usuario: frecuencia de conexión

29.- Motivación: curiosidad / comunicarse / otros

30.- Condiciones de registro: no leí / no leí todo /leí después / rechacé

31 - 35.- Redes usadas / ámbito / presencia / actuación

36 - 38.- Actividad: comparto-subo (mucho riesgo) / media / baja (poco riesgo)

Seguridad TIC:

39 - 43.- Atracción: muy alta / alta / media / baja / muy baja

44 – 48.- Confianza: “ “ “

49 - 53.- Estrés: “ “ “

54 – 58.- Utilidad: “ “ “

59 – 66.- Diversos tipos de protección: contraseñas/antivirus-firewalls/privacidad/e-mail

Cada número de pregunta se corresponde con las variables observables del cuestionario incluido en el Anexo A3 utilizado para la tesis, con la denominación de cada variable utilizada en la hoja Excel generada resaltada en rojo. Esa denominación será la utilizada por los programas estadísticos para su análisis y serán las referencias que encontraremos tanto en los resultados como en los anexos que los reflejan.

El **perfil** de los usuarios queda determinado por las respuestas a las preguntas 1 a 4, 28-29 y 31-32 (edad, sexo, rendimiento académico, frecuencia de conexión, redes sociales usadas).

Las diversas formas de **actuar** se reflejan en las respuestas a las variables por los conceptos consultados (contraseñas, copias de seguridad, protección de accesos, adquisición de información, actividad al navegar, registro en redes sociales, aportación de información y medidas de protección).

Los **conocimientos** se evalúan con las respuestas al test propuesto entre las preguntas 17 y 27.

Los resultados de los diversos tipos de encuestados, ya sea por perfil, por comportamiento o conocimientos son los que nos guiarán respecto a las **variables independientes de control** más convenientes para observar el modelo.

A su vez, las variables observables relacionadas con las latentes quedan asociadas de la siguiente forma:

- **Atracción**, se construye desde los indicadores de las variables observables At1 a At5; es decir, con las respuestas a:

Me gusta hablar con otros de seguridad
Si tuviera oportunidad me inscribiría en cursos de seguridad
Siento curiosidad por las noticias sobre seguridad
Estudiar sobre seguridad es entretenido
Me gustaría dedicar más tiempo a aprender temas de seguridad

- **Confianza**, definida por las variables C1 a C5

Saber seguridad incrementa mis posibilidades de navegar tranquilo
Me alegra poder resolver dificultades de seguridad
Soy capaz de ayudar a otros a resolver muchos de sus problemas de seguridad
Me gusta adoptar suficientes medidas de seguridad
Si me lo propongo puedo dominar bien los aspectos sobre seguridad

- **Estrés**, variables E1 a E5

Estoy preocupado por los riesgos de seguridad
Me altero cuando tengo que resolver un problema de seguridad
Me siento incapaz de comprender algunas cuestiones sobre seguridad
Tengo que encontrar más tiempo para implementar temas de seguridad
Si me surge un problema de seguridad debo buscar ayuda

- **Utilidad**, variables U1 a U6

La seguridad es muy necesaria para mi actividad personal
La seguridad es muy necesaria para mi actividad profesional
Los conocimientos sobre seguridad deben ser previos al uso de PC's
Debo saber utilizar los recursos de protección al navegar por internet
Debo saber utilizar los recursos de seguridad al navegar por redes sociales

De esa forma, las variables observables que se relacionan con nuestras hipótesis, y conforman cada latente quedan como sigue:

Tabla 5. Relación de Hipótesis con variables

Hipótesis	descripción	variables observables	Constructos o de control	pregunta encuesta
He1	Protección accesos	AUP1, AUP2, AUP3, A1, A2, A4, A5	Estadísticos básicos (passwords)	5, 6, 7, 11, 12, 59, 60
He2	Backups	ABU1, ABU2, ABU3	“ (copias)	8, 9, 10
He3	Antivirus, firewall	A6, A7	“ (autoprotección)	61, 62
He4	Información vulnerabilidades	A3	“ (inquietud x info)	13
He5	Privacidad de actividad	A8, A9	“ (privacidad)	63, 64
H1	Covarianza entre latentes	Atx-Cx-Ex-Ux	Atracción, Confianza, Estrés, Utilidad	39 - 58
H2	Utilidad implica mayor atracción	Ux - Atx	Utilidad, Atracción	39-43, 54-58
H3	Confianza \leftrightarrow privacidad	Cx - A8, A9	Confianza, Privacidad	44-48, 63-64
H4	Confianza \leftrightarrow protección	Cx - A6, A7	Confianza, Protección	44-48, 61-62
H5	Privacidad \leftrightarrow protección	A6 - A9	Privacidad, Protección	61 - 64
H6	A mayor nota más atracción	P1-P11-Atx	Nota, Atracción	17-27, 39-43
H7	A mayor nota mayor utilidad	P1-P11-Ux	Nota, Utilidad	17-27, 54-58
H8	A mayor nota más privacidad	P1-P11, A8-A9	Nota, Privacidad	17-27, 63-64
H9	A mayor nota más protección	P1-P11, A6-A7	Nota, Protección	17-27, 61-62

H10	A menor nota más Estrés	P1-P11-Ex	Nota, Estrés	17-27, 49-53
H11	A peor nota menos confianza	P1-P11, Cx	Nota, Confianza	17-27, 44-48
H12	Buen ajuste de latentes	Atx-Cx-Ux-Ex	Atracción, Confianza, Estrés, Utilidad	39-58
H13	Más privacidad → más ajuste	A8-A9, Atx - Cx-Ux-Ex	Atracción, Confianza, Estrés, Utilidad, Privacidad	39-58, 63-64
H14	Más protección → más ajuste	A8-A9, Atx - Cx-Ux-Ex	Atracción, Confianza, Estrés, Utilidad, Protección	39-58, 61-62
Hg1	Condiciones de registro	AURS3	Estadísticos básicos (registro en RS)	30
Hg2	Actividad - Publicación	AURS9, AURS10	“ (info personal en RS)	36, 37
Hg3	Publicación información sensible	AURS11	“ (info “muy personal”)	38

Fuente: Elaboración Propia (EP)

4.5 Selección de la muestra objeto del estudio

El muestreo es una herramienta usada en la investigación científica. Su función básica es determinar qué parte de una población debe examinarse con la finalidad de hacer inferencias sobre dicha población. El error que se comete debido al hecho de que se obtienen conclusiones sobre cierta realidad a partir de la observación de sólo una parte de ella, es lo que se denomina error de muestreo. Obtener una muestra adecuada significa lograr una versión simplificada de la población, que permita reproducir, de algún modo, sus rasgos básicos.

En nuestro caso, se ha tomado como muestra para la realización del presente estudio a alumnos de 2º curso de la ETSINF y alumnos de 1º, 4º y 5º de la ETSIT en el campus de Vera de la UPV en Valencia.

Las razones por las que se ha elegido precisamente esa población han sido las siguientes:

- Alumnos de diversas procedencias con formación y hábitos variados pero con una vocación hacia las TIC que, se supone, deben ser más conocedores de sus ventajas y saber reducir los riesgos que toda actividad conlleva, y con este caso concreto más aún.
- Accesibilidad a esos alumnos debido a ser alumnos de los directores y del autor de la presente tesis.
- Conjuntos diferentes de madurez (alumnos de 1º-2º versus 4º-5º)
- Tamaño manejable de la información suficiente como para adquirir la experiencia necesaria, tanto a nivel cuestionario como por su análisis posterior, para acceder a un mayor número de alumnos de diferentes titulaciones que sea totalmente representativa de la población universitaria de la UPV

4.5.1 Cálculo del error muestral

Para determinar en términos estadísticos el error introducido en el muestreo se define el concepto de error muestral como la desviación típica de la distribución muestral de las medias, que se representa a modo de una campana de Gauss. Por tanto, nunca es posible abarcar estadísticamente toda el área de la curva, ya que tiende asintóticamente a infinito. Este error indica el porcentaje de incertidumbre, es decir, el riesgo que se corre que la muestra elegida no sea representativa.

A su vez, para evaluar la validez del muestreo, se maneja el concepto de nivel de confianza, establecido como el porcentaje del área de la curva que se contempla en el estudio (por ejemplo, el 90%, el 95%, etc.). En definitiva, es la probabilidad de que la media de la distribución muestral y la media de la población difieran en una cantidad menor que el error máximo admisible en el muestreo. La confianza, o el porcentaje de confianza, indican el porcentaje de seguridad que existe para generalizar los resultados obtenidos. Esto quiere decir que un porcentaje del 100% equivale a decir que no existe ninguna duda para generalizar los resultados, pero implica estudiar a la totalidad de los casos de la población.

Para evitar un costo muy alto para el estudio, o debido a que en ocasiones llega a ser prácticamente imposible el estudio de todos los casos, entonces se busca un porcentaje de confianza menor. Comúnmente en las investigaciones sociales se busca un 95%.

En nuestro caso, para calcular el error muestral, partimos de que la población sobre la que se dirige el estudio es “finita”, formada por una totalidad de 990 alumnos matriculados en los respectivos cursos.

El número de cuestionarios respondidos de que disponemos es de 499 (válidos 396).

Introduciendo ambos valores en la siguiente fórmula:

$$\text{Error muestral} = K * (\text{RAIZ}(((P*(1-P))/n)*((N-n)/(N-1))))$$

donde: n es el tamaño de la muestra, N el de la población, y

K = coeficiente que indica la confianza (1,96 para el 95%, 2,17 para el 97%)

Se obtienen los siguientes resultados para nuestro caso, en el que hemos considerado la situación más adversa en la que la prevalencia (P) esperada del parámetro es 0,5 que es la más desfavorable y exige el mayor tamaño muestral, quedando: $P = 1 - P = Q = 0,5$

Error muestral para un 95% de confianza: 3,1 %

Error muestral para un 97% de confianza: 3,4 %

Error muestral para un 99% de confianza: 4,1 %

La población encuestada estaba integrada por el número de alumnos de la tabla 6.

Tabla 6. Población objeto de la muestra

Año	Escuela	Curso	Total alumnos	Total encuestados	Total válidos
11-12	Informática	2º	380	235	204
12-13	“	2º	410	153	105
“	Telecomunicación	1º	54	38	28
“	“	4º	65	49	39
“	“	5º	81	24	20
2 años	TOTAL	1º - 5º	990	499	396

Fuente: EP

5.- RESULTADOS

5.1 Estadísticos básicos: análisis de fiabilidad

Podemos decir que, aunque sea con carácter preliminar, los resultados nos ofrecen información suficiente como para adecuar el proceso de aprendizaje y sensibilización con las medidas de precaución aconsejables para alcanzar una mejoría en el riesgo asumible de los estudiantes cuando utilizan sus ordenadores y navegan por internet, en general, o por las redes sociales, en particular.

Los encuestados de 2º curso de Informática del curso 2011-2012 tienen una edad de 24 años o menos en el 85% de los casos, siendo las mujeres un 12%. El 57% va a curso por año, sin tener asignaturas pendientes. En el Anexo A3.1 aparecen estos datos.

Con respecto a **contraseñas** (variables AUPx):

- El 36% de los encuestados reconoce tener una única password común, para la mayoría de los accesos.
- Más del 72% las mantiene fijas a lo largo del tiempo y otro 22% las cambia con una frecuencia anual, aproximadamente.
- El 27% deja que se las grabe el propio navegador y otro 8% usa nombres sencillos.
- Analizando conjuntamente las variables observadas, encontramos que un 4,5% de los alumnos establece contraseñas complejas, diferentes para cada acceso y que actualiza cada pocos meses. El 33% declara no proteger el acceso a su ordenador (variable A1).

En referencia a las **copias de seguridad** de los datos (variables ABUx):

- El 15% no ha hecho nunca una copia y otro 33% solo las hace cuando cambia de PC. Un 21% adicional suele hacerlas con frecuencia anual y un 18% cada semestre. El 13% tiene un sistema automático de actualización

- Un 5% guarda las copias en el mismo disco del PC y un 57% en un disco externo
- La frecuencia en hacer copias de seguridad está correlacionada (0,554 con significatividad al 1%) con la garantía del soporte en el que se guardan, pudiendo establecer un factor común de comportamiento que explicaría el 77,7% de la varianza con un Alfa de Cronbach de 0,711.
- El 24% abre los correos de remitentes desconocidos por curiosidad
- Un 16% reconoce no preocuparse por las vulnerabilidades de seguridad y un 26% se enteran de esos problemas a través de amigos.

A la hora de **navegar por las redes sociales** (variables AURSx):

- Un 45 % sube habitualmente información personal de viajes, fotos, fiestas y composiciones propias
- Un 45% se expresa libremente manifestando sus puntos de vista sobre cualquier tema
- Algo más de la cuarta parte (26%) de los alumnos coinciden en las actividades anteriores. De hecho, existe una correlación de 0,369 significativa al nivel del 1%
- Casi dos terceras partes (62%) de los alumnos coinciden en que se dan de alta sin leerse las condiciones de registro aceptándolas al asumir que son estándar.
- También se infiere un factor común de comportamiento en el uso global que hacen al navegar por redes sociales, que explica el 63,5% de la varianza, con un coeficiente KMO⁴³ (Kaiser-Meyer-Olkin) de 0,649 y Alfa de 0,7.

⁴³ Indica el grado de interrelación entre los datos

Hay correlaciones significativas entre las siguientes variables con cinco alternativas de respuesta:

- ABU1 con ABU2 (copias de seguridad)
- AW1 con AW2 y AW3 (tipo de actividad en internet)

Con respecto a la **actividad en internet** (webs 1.0, 2.0, 3.0), se ve que hay una Concentración en la Tabla de Contingencia entre las dos variables, en las mayores frecuencias de uso, indicando que los mayores usuarios de la web 2.0 también lo son de la 1.0.

- URS1, con AURS9, con AURS10 y AURS11 (tipo de actividad en redes sociales)
- A3, 4, 5, 6, 7, 8, 9 (diversas actuaciones de seguridad)

Se forman dos factores, agrupándose A6 con A7 (**protección** vía antivirus y firewall) y A8 con A9 (**privacidad** de rastro de navegación), explicando el 85% de la varianza

Quedan, pues, correlacionadas actuaciones sobre:

- a) copias de seguridad
- b) actividad en redes sociales
- c) disponibilidad de protecciones (antivirus-firewall)
- d) “rastros” de actividad en el PC (archivos temporales, cookies, histórico) que definen el constructo “actividad” real que llevan a cabo los encuestados, incorporando cuatro nuevas variables (fac1, 2, 3 y 4) en la hoja excel que son el resumen de las otras 9 variables que fueron su origen. El valor que cada individuo, o sujeto de la muestra, toma en cada uno de los factores que representan a las variables originales, es la puntuación factorial, puesto que, en regresión trabajo con todas las variables o con los factores que las representan.

La correlación entre los que tienen activos antivirus y firewall es del 0,64 y entre los que eliminan archivos temporales e histórico de páginas visitadas es del 0,75, ambos con significatividad del 1% (lo deseable es que las correlaciones sean superiores a 0,3). Nos determinan dos factores, **autoprotección y privacidad**, que explican el 85% de la varianza, con KMO de 0,6 y alfa de 0,77.

El resumen de los parámetros estadísticos al tratar los cuestionarios de las encuestas, que puede verse en el Anexo C.1, es el de la siguiente tabla:

Tabla 7. Parámetros encuesta curso 2011-2012

Factor / variables	KMO	Varianza	Alfa Cronbach	Significatividad
(valores deseables)	>0,5	>60%	>0,6	<5%
F1/ At1, At2, At3, At4, At5	0,87	71%	0,897	<1%
F2/ E2, E3, E5	0,656	64%	0,714	<1%
F3/ U1, U2, U4, U5, C4, E1	0,847	62%	0,853	<1%
Conjunta (todas las variables)	0,89	67%	0,891	<1%

Fuente: EP

Al factorizar las veinte variables nos aparecen tres factores claramente diferenciados, con una alta correlación entre las variables que conforman cada uno de ellos.

Uno está definido por las cinco variables que propusimos en ese sentido (atracción).

Otro (estrés) queda representado por tres de las cinco variables previstas.

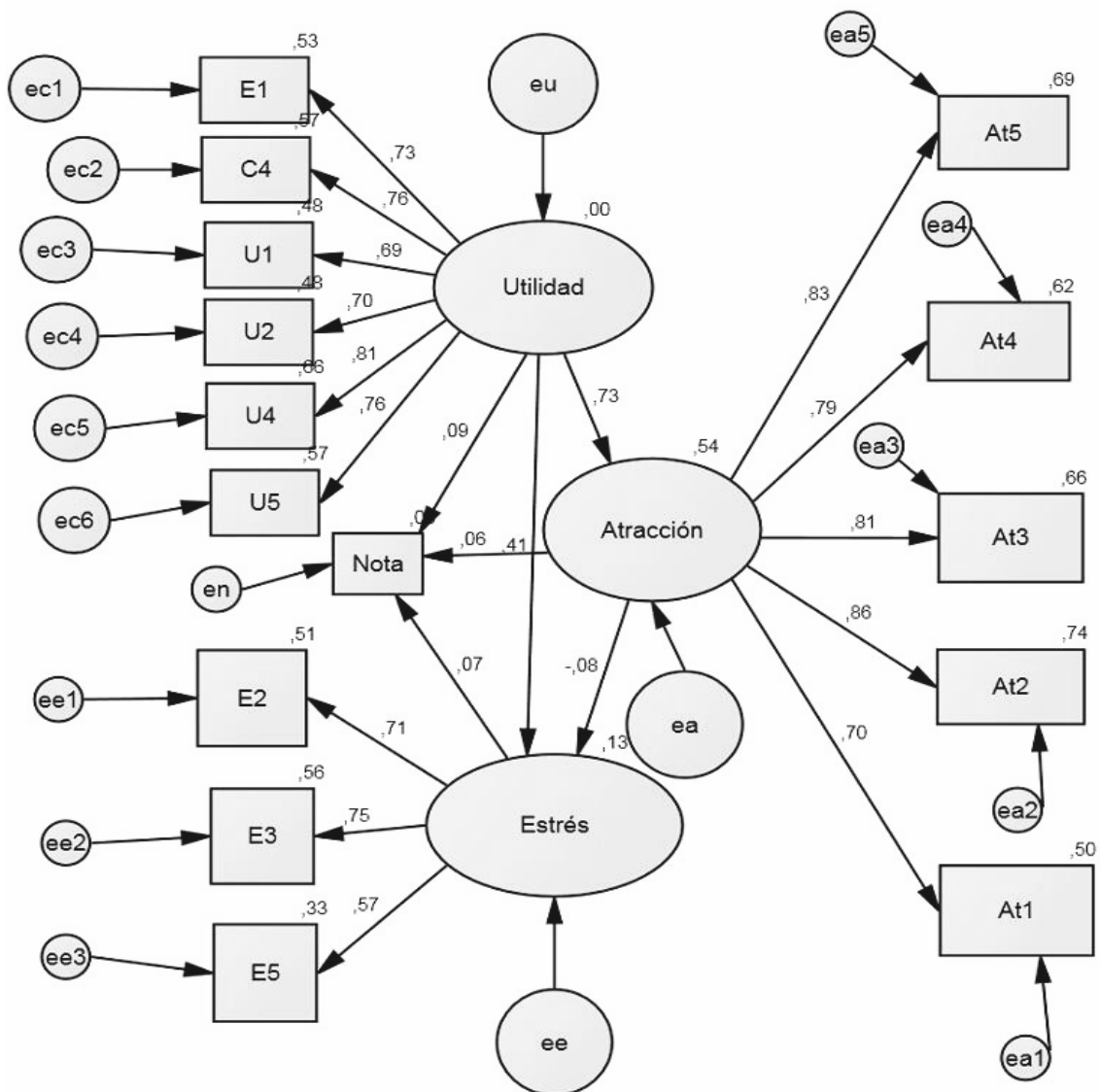
Y el último (utilidad) lo conforman cuatro de las cinco variables supuestas más una de estrés y otra de confianza.

Los resultados estadísticos referentes a calidad, explicación de las varianzas e indicadores de correlación son muy altos, lo que indica la coherencia de las respuestas.

Y, ¿por qué no decirlo?, la idoneidad del planteamiento.

5.2 Estadísticos estructurales previos

Inicialmente, con los datos obtenidos de los alumnos del curso 2011-2012 a nivel de formación de constructos, y los grafos y la orientación de causalidades en el sentido marcado por otros autores (anexo 1), elaboramos nuestro modelo en el que indicamos las variables observables, las latentes y la dependiente “Nota”.



Grafo 2. Modelo más simple propuesto del curso 2011-2012 (EP)

Se logró un ajuste con $\chi^2 = 198,6$, con 85 grados de libertad y un nivel de probabilidad $p = .000 (<1\%)$.

El índice de bondad de ajuste del modelo se mide mediante varios parámetros:

- a) $\chi^2 / \text{grados de libertad} = 2,33$ (siendo lo correcto estar entre 1 y 3)
- b) Los residuos RMSEA están entre 0,066 y 0,096 (no deben superar 0,1), y
- c) el CFI (comparative fit index), que debe ser $>0,9$, en nuestro modelo tiene un valor de 0,923.

Tabla 8. Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
Atracción	<---	Utilidad	,902	,100	8,990	***	par_14
Estrés	<---	Utilidad	,364	,130	2,799	,005	par_16
Estrés	<---	Atracción	-,055	,097	-,560	,575	par_17
U5	<---	Utilidad	1,000				
U4	<---	Utilidad	1,034	,089	11,615	***	par_1
U2	<---	Utilidad	1,137	,116	9,837	***	par_2
U1	<---	Utilidad	1,072	,110	9,770	***	par_3
C4	<---	Utilidad	,984	,091	10,783	***	par_4
E1	<---	Utilidad	1,091	,106	10,315	***	par_5
E5	<---	Estrés	1,000				
E3	<---	Estrés	1,375	,219	6,268	***	par_6
E2	<---	Estrés	1,359	,215	6,308	***	par_7
At5	<---	Atracción	1,000				
At4	<---	Atracción	1,017	,079	12,857	***	par_8
At3	<---	Atracción	,926	,069	13,440	***	par_9
At2	<---	Atracción	1,048	,072	14,605	***	par_10
At1	<---	Atracción	,874	,079	11,051	***	par_11
Nota	<---	Atracción	,156	,333	,467	,641	par_12
Nota	<---	Estrés	,268	,346	,775	,438	par_13
Nota	<---	Utilidad	,314	,440	,714	,475	par_15

Fuente: AMOS (EP)

Observando la columna de significatividad (P) en la tabla 8, comprobamos la confianza que demuestran los índices ($< 1\%$) que informan de la correspondencia entre cada variable observable y su latente, así como entre las latentes Utilidad \rightarrow Atracción y también entre Utilidad \rightarrow Estrés. Sin embargo, llama la atención la escasa significatividad de la variable Nota con los tres factores de Atracción, Estrés y Utilidad.

Tabla 9. Standardized Regression Weights: (Group number 1 - Default model)

			Estimate
Atracción	<---	Utilidad	,732
Estrés	<---	Utilidad	,411
Estrés	<---	Atracción	-,076
U5	<---	Utilidad	,756
U4	<---	Utilidad	,811
U2	<---	Utilidad	,696
U1	<---	Utilidad	,692
C4	<---	Utilidad	,757
E1	<---	Utilidad	,727
E5	<---	Estrés	,572
E3	<---	Estrés	,750
E2	<---	Estrés	,714
At5	<---	Atracción	,828
At4	<---	Atracción	,788
At3	<---	Atracción	,813
At2	<---	Atracción	,861
At1	<---	Atracción	,705
Nota	<---	Atracción	,056
Nota	<---	Estrés	,069
Nota	<---	Utilidad	,091

Fuente: AMOS (EP)

Viendo los índices de regresión en la tabla 9, comprobamos la alta correlación existente entre Utilidad → Atracción y, en menor medida pero también significativa como hemos visto en la tabla anterior, entre Utilidad → Estrés. La escasa significatividad y valor de correlación de Nota con los factores de Atracción, Estrés y Utilidad, nos indican la escasa relevancia de los conocimientos a la hora de determinar la forma de actuar.

Por otra parte, la variable latente Utilidad tiene el indicador más válido en la pregunta U4 (debo saber utilizar los recursos de protección al navegar por internet). El constructo Atracción está mejor representado por la pregunta At2 (si tuviera oportunidad me inscribiría en cursos de seguridad), y el de Estrés por la E3 (me siento incapaz de comprender algunas cuestiones sobre seguridad).

Tabla 10. Efectos entre las variables latentes (EP)

	Utilidad	Atracción	Estrés	Nota
Utilidad		+++	++	0
Atracción				0
Estrés				0

Fuente: Elaboración Propia (EP)

Vemos en la tabla 10 que el efecto del concepto Utilidad influye fuertemente en el de Atracción y bastante en el Estrés, y que ninguna se correlaciona significativamente, ni en valor, con el rendimiento (Nota). Es decir, los estudiantes que consideran que la seguridad informática es útil se sienten más atraídos por la misma, aunque les genere cierto grado de estrés. Ninguna de las variables tiene incidencia con el rendimiento.

Es importante hacer notar que los modelos de ecuaciones estructurales permiten probar hipótesis de forma estadística mucho más compleja que con otros métodos, estableciendo relaciones causales desde las meras relaciones entre las variables de los diferentes datos.

La relación entre variables actitudinales y el propio aprendizaje constituye una información básica para la construcción y/o modificación de planes de estudio en las diversas competencias educativas.

Aprovechando la facilidad de segmentación de la población encuestada gracias a las variables identificativas incluidas en el cuestionario, analizamos repetidamente el mismo modelo estructural utilizando esas variables de control para diferenciar los diversos conjuntos de sub-poblaciones obtenidas y comprobar el comportamiento y fiabilidad de nuestro modelo, obteniendo los resultados del anexo C.2 que mostramos resumidos en la tabla 11.

Tabla 11. Parámetros modelos estructurales curso 2011-2012 (EP)

	<u>CFI</u>	<u>Chi cuadrado</u>	<u>RMSEA</u>
General	0,923	198,6	0,066-0,096
Usuarios con antivirus actualizado (A6 es 4 ó 5)	0,931	150,9	0,051-0,088
chicos	0,933	174,8	0,061-0,093
Passwords AUP3 es 3 (compleja)	0,933	138,2	0,047-0,090
Borran histórico de págs. visitadas (A9 es 4 ó 5)	0,939	132,1	0,044-0,089
Hacen backups	0,947	121,1	0,036-0,091
Protección con password en inicio sesión en PC (A5 es 4 ó 5)	0,952	114,7	0,023-0,074
Privacidad (eliminan archivos temporales y cookies, con A8 es 4 ó 5)	0,953	121,2	0,032-0,080

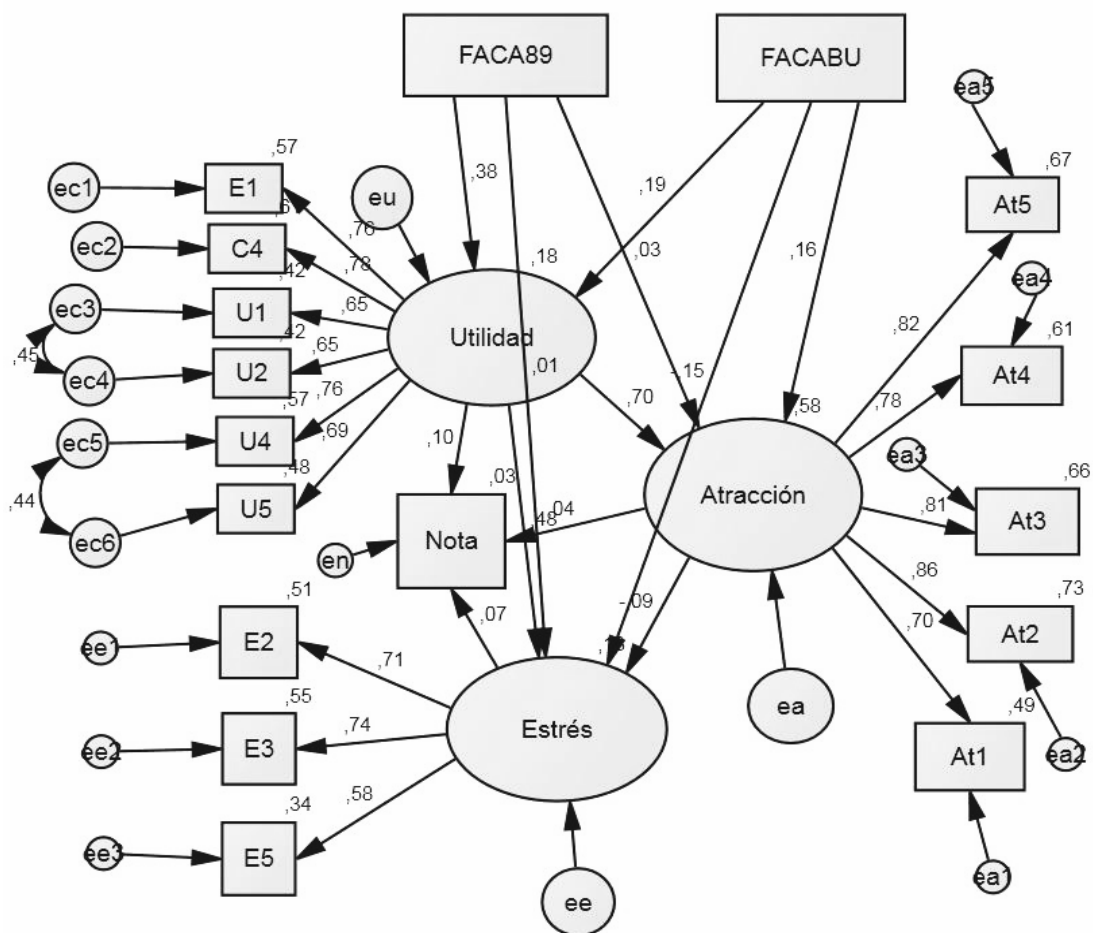
Fuente: Elaboración Propia (EP)

El resultado no puede ser más obvio. El modelo se ajusta mejor a los estudiantes que se preocupan en tener antivirus actualizado. Curiosamente también con los chicos exclusivamente más que con el conjunto. Al igual que con los que usan contraseñas más complicadas. Aún se ajusta más a los cuidadosos con dejar rastro de las páginas que visitan y con los que mantienen un procedimiento adecuado para salvaguardar su información vía backups.

El modelo es bastante irreprochable en el caso de los alumnos que abren su sesión con contraseña y los que “limpian” su ordenador de archivos temporales descargados durante la navegación, que evitan pequeñas incomodidades en procesos posteriores.

Es decir, el modelo se cumple con más fuerza en los alumnos que ponen en práctica un mínimo de medidas de autoprotección para que su intimidad no se vea alterada.

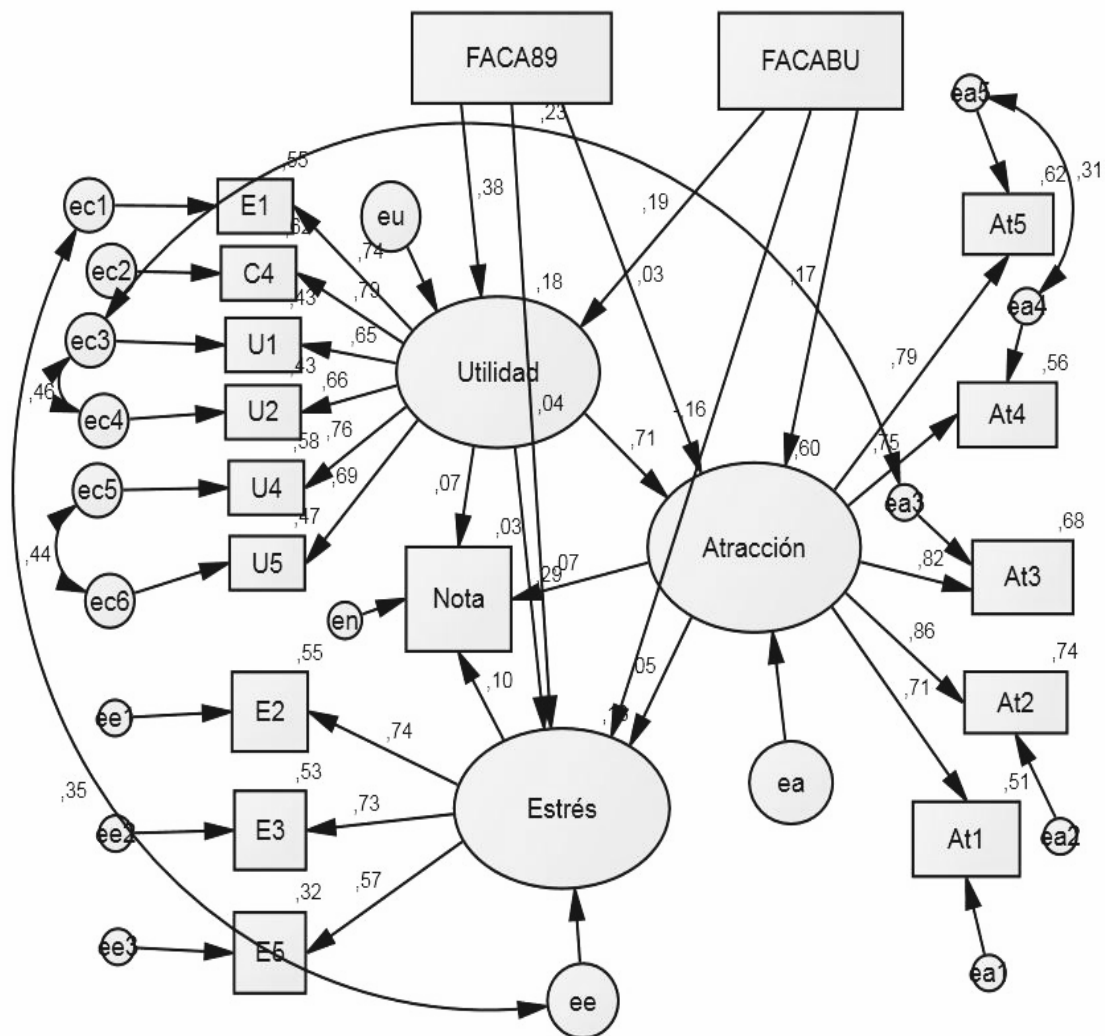
Tras las diversas experimentaciones para optimizar el modelo, introdujimos los factores comunes que nos indicaban el nivel de actuación sobre copias de seguridad (FACABU) y de cuidado sobre la privacidad (FACA89) al ser cuidadosos con los rastros de actividad en el PC (histórico, cookies, archivos temporales). Covariando dos parejas de variables observables del constructo Utilidad (U1-U2 y U5-U4), obtuvimos unos resultados que indican el alto grado de confianza en el mismo, con unos indicadores CFI, TLI, RMSEA excelentes (0,963 / 0,954 / 0,034 – 0,066). Con χ^2 164,5 y 108 grados de libertad.



Grafo 3. Modelo simple con variables de control del curso 2011-2012 (EP)

Los resultados ratifican la idea de que las variables latentes están bien configuradas, covariando de forma positiva las variables indicadoras de las actitudes hacia cada latente. Si una persona da una respuesta alta en una de las variables, tiende también a darla en las otras variables que definen el constructo, aunque sus medias sean diferentes.

No obstante, siguiendo las propias indicaciones del programa en base a las recomendaciones de Modificación de Índices, correlacionando las variables sugeridas por AMOS para la optimización de nuestros datos del modelo llegamos a los resultados siguientes:



Grafo 4. Modelo sugerido, con variables de control, del curso 2011-2012 (EP)

Siendo 125,4 el valor obtenido para Chi-square y 105 los grados de libertad

Tabla 12. Resultados proceso grafo 4

Baseline Comparisons

Model	NFI Delta1	RFI rho 1	IFI Delta2	TLI rho2	CFI
Default model	,925	,903	,987	,983	,987
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,031	,000	,050	,953
Independence model	,236	,226	,247	,000

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
Utilidad	<---	FACABU	,111	,043	2,618	,009	par_15
Utilidad	<---	FACA89	,226	,045	5,012	***	par_19
Atracción	<---	Utilidad	,912	,122	7,472	***	par_12
Atracción	<---	FACABU	,129	,043	2,974	,003	par_17
Atracción	<---	FACA89	,027	,046	,576	,564	par_20
Estrés	<---	Utilidad	,287	,157	1,830	,067	par_13
Estrés	<---	Atracción	,040	,112	,355	,723	par_14
Estrés	<---	FACABU	-,091	,047	-1,928	,054	par_16
Estrés	<---	FACA89	,022	,048	,457	,647	par_18
U5	<---	Utilidad	1,000				
U4	<---	Utilidad	1,063	,084	12,623	***	par_1
U2	<---	Utilidad	1,179	,143	8,238	***	par_2
U1	<---	Utilidad	1,122	,136	8,226	***	par_3
C4	<---	Utilidad	1,125	,117	9,630	***	par_4
E1	<---	Utilidad	1,218	,133	9,143	***	par_5
E5	<---	Estrés	1,000				
E3	<---	Estrés	1,340	,207	6,468	***	par_6
E2	<---	Estrés	1,414	,218	6,474	***	par_7
At5	<---	Atracción	1,000				
At4	<---	Atracción	1,015	,075	13,562	***	par_8
At3	<---	Atracción	,983	,078	12,552	***	par_9
At2	<---	Atracción	1,094	,083	13,144	***	par_10
At1	<---	Atracción	,929	,088	10,537	***	par_11
Nota	<---	Utilidad	,253	,523	,483	,629	par_21
Nota	<---	Atracción	,208	,383	,544	,586	par_22
Nota	<---	Estrés	,370	,340	1,086	,277	par_23

Standardized Regression Weights: (Group number 1 - Default model)

			Estimate
Utilidad	<---	FACABU	,188
Utilidad	<---	FACA89	,380
Atracción	<---	Utilidad	,710
Atracción	<---	FACABU	,169
Atracción	<---	FACA89	,035
Estrés	<---	Utilidad	,294
Estrés	<---	Atracción	,052
Estrés	<---	FACABU	-,157
Estrés	<---	FACA89	,038
U5	<---	Utilidad	,687
U4	<---	Utilidad	,759
U2	<---	Utilidad	,656
U1	<---	Utilidad	,653
C4	<---	Utilidad	,789
E1	<---	Utilidad	,739
E5	<---	Estrés	,570
E3	<---	Estrés	,727
E2	<---	Estrés	,739
At5	<---	Atracción	,789
At4	<---	Atracción	,748
At3	<---	Atracción	,822
At2	<---	Atracción	,858
At1	<---	Atracción	,712
Nota	<---	Utilidad	,066
Nota	<---	Atracción	,070
Nota	<---	Estrés	,095

Fuente: AMOS (EP)

La significatividad es excelente (<1%) y directa en:

- Utilidad → Atracción (regr. 0,71),
- FACA89 → Utilidad (regr. 0,38) , y
- entre las relaciones de las latentes y sus observables, y algo menor entre
- FACABU → Utilidad (regr. =,188)
- FACABU → Atracción (0,169),

debiendo tener presente las relaciones con significatividad $< 7\%$ entre:

FACABU \rightarrow Estrés (negativa, con valor -0,157), y

Utilidad \rightarrow Estrés (0,294)

Las “Notas” no son significativas y de escaso valor. Es decir, respecto estos parámetros, los mejores estudiantes actúan de forma paralela a los no tan buenos. Falta información adecuada a todos los niveles. Ni siquiera los mejores, por el simple hecho de serlo, actúan con la debida seguridad.

Existe un valor de regresión muy alto entre Utilidad y Atracción (0,71) que nos indica que cuando un alumno entiende algo como útil, o práctico, se siente fuertemente atraído por ello y ahí es donde hay que acentuar la formación, con información y ejemplos sobre seguridad que les resulten motivadores y sobre los que se haga hincapié de forma transversal en la mayoría de las asignaturas, no sólo en las específicas que traten los temas de forma general, asumiendo unos conocimientos y unas actitudes que parece que no han asimilado.

También tenemos un valor bastante alto de regresión total (0,38) entre FACA89 \rightarrow Utilidad con un 1% de significatividad, lo que implica que los alumnos que son más cuidadosos con su privacidad consideran más útil adoptar medidas de seguridad.

Así mismo, hay un valor alto directo entre Utilidad \rightarrow Estrés (0,294) que, aunque no sea significativo desde el punto de vista más estricto (6%), nos da idea de que lo que consideran útil les produce cierta ansiedad, quizá por saber que debieran conocerlo mejor no sintiéndose seguros de sus propias capacidades.

5.3 Evolución del análisis

A la vista de los resultados anteriores, creímos conveniente extender la encuesta a una muestra mayor de alumnos de forma que pudiésemos definir una población compuesta por el conjunto de alumnos tanto de la Facultad de Informática como de la Escuela Superior de Ingenieros de Telecomunicación, para obtener unos resultados fiables del conjunto de esa población que, de acuerdo con sus programas de estudio, debe de ser la más cualificada de toda la UPV sobre la materia que nos ocupa.

Resultaba muy preocupante que alumnos de la carrera de Informática pudieran ser tan descuidados con la protección de sus accesos, datos y actividades. Uno de cada tres alumnos reconoce tener una única contraseña para todos sus accesos y la misma proporción no tiene contraseña para iniciar la sesión de su ordenador, con el riesgo para su privacidad que ello comporta.

Algo parecido ocurre con las garantías para proteger la disponibilidad de los datos. Es inadmisibles que una séptima parte de este tipo de estudiante no haya hecho nunca una copia de seguridad y una tercera parte lo haga, por obligación, cuando cambia de ordenador.

En la navegación por redes sociales vimos que no tienen conciencia del escaparate en el que están y que un 45% hable libremente de sus intimidades personales, sexuales, políticas, religiosas es comprometer su futuro profesional, y puede que personal, sin ser conscientes de ello y pretendiendo ser profesionales. Todo un contrasentido.

Con el análisis estructural descubrimos un valor de regresión muy alto entre Utilidad y Atracción que nos informa de la necesidad de hacer ver a nuestros alumnos la importancia práctica de los conocimientos que están adquiriendo con los que está fuertemente vinculada su propia seguridad. Cuando entiendan su utilidad se sentirán más atraídos y ahí deberemos acentuar la formación, con información y ejemplos constantes sobre seguridad que les resulten aleccionadores y susciten su interés y sobre los que se estudien las especificaciones propias de cada asignatura.

También hemos visto que hay un valor alto de correlación entre Utilidad→Estrés que nos dice hasta qué punto lo que consideran útil les produce un nivel de ansiedad, quizá por ser conscientes de que debieran conocerlo mejor no sintiéndose seguros de sí mismos.

Tampoco debemos ignorar la importancia de que la “Nota”; es decir, el nivel de sus conocimientos, no ofrezca mayores sensibilidades, al menos, a los mejores estudiantes. O sea, respecto este parámetro, unos y otros actúan de forma parecida. Falta información que les motive suficientemente a todos los niveles ya que, ni siquiera los mejores, actúan favoreciendo su seguridad.

A la vista de tan preocupantes datos se decidió comprobar si podía haber algún tipo de problema, falta de oportunidad o enfoque en la encuesta. Por lo que se repitió con un grupo de similar perfil académico (1º, 4º y 5º de Teleco y 2º de Informática) un curso más tarde. Con criterios similares al curso anterior, en total fueron válidas 192 encuestas (87 de Teleco y 105 de Informática).

5.3.1 Estadísticos básicos

Los resultados obtenidos a partir de los datos observados en los alumnos del curso 2012-2013 fueron los siguientes (Anexos A 3.2, D y D.1):

Con respecto a **contraseñas** (variables AUPx, en Anexo A3.2):

- El 41% de los encuestados reconoce tener una única password común, para la mayoría de los accesos.
- El 70% las mantiene fijas a lo largo del tiempo y otro 25% las cambia con una frecuencia anual, aproximadamente.
- El 22% deja que se las grave el propio navegador y otro 10% usa nombres sencillos.
- El 34% declara no proteger el acceso a su ordenador (variable A1).
- Analizando conjuntamente las variables observadas, encontramos que un 4,2% de los alumnos establece contraseñas complejas, diferentes para cada acceso y que actualiza cada pocos meses.

Con referencia a las **copias de seguridad** de los datos (variables ABUx):

- El 13% no ha hecho nunca una copia y otro 32% solo las hace cuando cambia de PC. Un 18% adicional suele hacerlas con frecuencia anual y un 20% cada semestre.
- Un 4% guarda las copias en el mismo disco del PC y un 56% en un disco externo
- El 17% tiene un sistema automático de actualización.
- La frecuencia en hacer copias de seguridad está correlacionada (0,581 con significatividad al 1%) con la garantía del soporte en el que se guardan, pudiendo establecer un factor común de comportamiento que explicaría el 79% de la varianza con un Alfa de Cronbach de 0,734.

- El 30% abre los correos de remitentes desconocidos para averiguar lo que pretenden (variable A2)
- Un 15% reconoce no preocuparse por las vulnerabilidades de seguridad y un 31% se enteran de esos problemas a través de amigos (variable A3).

A la hora de **navegar por las redes sociales** (variables AURSx):

- Un 34% sube habitualmente información personal de viajes, fotos, fiestas y composiciones propias
- Un 41% se expresa libremente manifestando sus puntos de vista sobre cualquier tema
- Casi dos terceras partes (61%) de los alumnos coinciden en que se dan de alta sin leerse las condiciones de registro aceptándolas al asumir que son estándar.

La correlación entre los que tienen activos antivirus y firewall es del 0,741 y entre los que eliminan archivos temporales e histórico de páginas visitadas es del 0,809, ambos con significatividad del 1%. Nos determinan dos factores, **autoprotección** y **privacidad**, que explican el 89% de la varianza, con KMO de 0,553 y alfa de 0,746.

Resumiendo, en cuadros comparativos (tablas 13 a 17):

Tabla 13: Frecuencias de alumnos que realizan funciones sobre uso de contraseñas (EP)

Contraseñas	Password única	Siempre fijas	Cambio anual	Grabación por navegador	Nombres sencillos	No protección acceso a PC	Seguros
Curso 2011-2012	36%	72%	22%	27%	8%	33%	4,5%
Curso 2012-2013	41%	70%	25%	22%	10%	34%	4,2%

Donde:

Password única implica una única contraseña para la mayoría de accesos

Siempre fijas se refiere a no cambiarlas a lo largo del tiempo

En *grabación por navegador*, que el propio sistema las genera de forma automática

Nombres sencillos son contraseñas fáciles de adivinar

La *no protección de acceso al PC* significa que es libre, sin contraseña para la sesión
Seguros son los que utilizan nombres complejos, diferentes, y cambian con frecuencia

Tabla 14: Frecuencias de alumnos que realizan funciones sobre uso de backups (EP)

Copias de seguridad	Nunca hizo	Al cambiar PC	Anual	Semestral	En PC	Disco externo	Actualización automática
Curso 2011-2012	15%	33%	21%	18%	5%	57%	13%
Curso 2012-2013	13%	32%	18%	20%	4%	56%	17%

Interpretando lo siguiente:

Nunca hizo significa que no hacen copias de seguridad en ningún caso

Al cambiar de PC es el porcentaje que hace copia en ese caso

En PC indica el alojamiento en el que guardan las copias

Disco externo es el alojamiento de las copias

Actualización automática implica disponer de un sistema que se encarga de hacerlo

Tabla 15: Correlación entre funciones de defensa que realizan los alumnos y Estadísticos básicos (EP)

	antivirus y firewall (*)	Archivos temp./ histórico pgs. (*)	significatividad	Explicación de varianza	Alfa de Cronbach	KMO
Curso 2011-2012	0,64	0,75	1%	85%	0,77	0,6
Curso 2012-2013	0,741	0,809	1%	89%	0,746	0,553

(*) La correlación entre los que tienen activos antivirus y firewall, contribuyen a la **autoprotección**

(*) La correlación entre los que eliminan archivos temporales e histórico de páginas visitadas, conforman la idea de **privacidad**

Uno de los parámetros utilizados para conocer el porcentaje de alumnos que protegen su privacidad fue saber si se preocupan por la eliminación periódica de las cookies que se almacenan en el PC tras navegar por internet (variable A8).

El resultado obtenido fue que el 38,6% del total de alumnos de los dos cursos (Anexo E) no se preocupan por hacerlo (37,3% del curso 11-12, y 40,1% del 12-13).

Tabla 16: Frecuencias de alumnos que realizan funciones sobre normas básicas de seguridad (EP)

	Abren mails desconocidos	Despreocupación por vulnerabilidades	Info x amigos
Curso 2011-2012	24%	16%	26%
Curso 2012-2013	30%	15%	31%

Significando lo siguiente:

Abren mails de desconocidos, para averiguar lo que pretenden

No tienen preocupaciones por vulnerabilidades, de seguridad

La *información*, sobre vulnerabilidades de seguridad la conocen a través de los amigos

Tabla 17: Frecuencias de alumnos que expresan contenidos a través de Redes Sociales (EP)

Navegar x SNS	Info amistosa	Expresión libre	Aceptan sin leer conds.
Curso 2011-2012	45%	45%	62%
Curso 2012-2013	34%	41%	61%

En esta última tabla:

La *información amistosa*, se refiere a la personal (viajes, fotos, fiestas, composiciones propias....).

La *expresión libre*, implica manifestarse a través de Redes Sociales con opiniones políticas, religiosas, sexuales....

Aceptan sin leer condiciones, de registro, dando por suficientes las ofertadas por defecto.

Así pues, lamentablemente se confirma el acierto por la preocupación de los resultados previos obtenidos con los alumnos del curso 2011-2012 al constatar la similitud, en el

orden de magnitud, con los datos conseguidos al procesar las respuestas de los alumnos del curso siguiente. Lo que demuestra su coherencia.

A su vez, a través del diseño factorial que nos permite confirmar, o variar, los grafos estructurales del curso anterior al procesar las respuestas contenidas en los cuestionarios de las encuestas del curso 2012-2013 que pueden consultarse en el Anexo D.1, encontramos los resultados que, resumidos, pueden verse en la tabla 18:

Tabla 18. Parámetros encuesta curso 2012-2013

Factor / variables	KMO	Varianza	Alfa Cronbach	Significatividad
(valores deseables)	>0,5	>60%	>0,6	<5%
F1/ At1, At2, At3, At4, At5	0,835	71%	0,897	<1%
F2/ E2, E3, E5	0,637	57%	0,616	<1%
F3/ U1, U2, U4, U5, C4, E1	0,674	68%	0,782	<1%
Conjunta (todas las variables)	0,781	60%	0,828	<1%

Fuente: EP

Al agrupar las variables nos aparecen tres factores claramente diferenciados y definidos como en el curso anterior, con una alta correlación entre las variables que conforman cada uno de ellos.

Uno está definido por las cinco variables que propusimos en ese sentido (atracción). Otro (estrés) queda representado por tres de las cinco variables previstas. Y el último (utilidad) lo conforman cuatro de las cinco variables supuestas más una de estrés y otra de confianza.

Nuevamente los resultados estadísticos referentes a calidad, explicación de las varianzas e indicadores de correlación nos informan de la coherencia de respuestas y planteamiento.

No obstante, disponiendo de los datos de los dos cursos realizamos un análisis factorial exploratorio con el conjunto de todos los alumnos (anexo E) y nos encontramos con un cuarto factor (confianza) que completaba los tres existentes (atracción, estrés y utilidad)

tal y como se identifica en los modelos basados en la teoría referenciados en el Anexo 1. El resumen de los valores estadísticos obtenidos se presenta en la tabla 19.

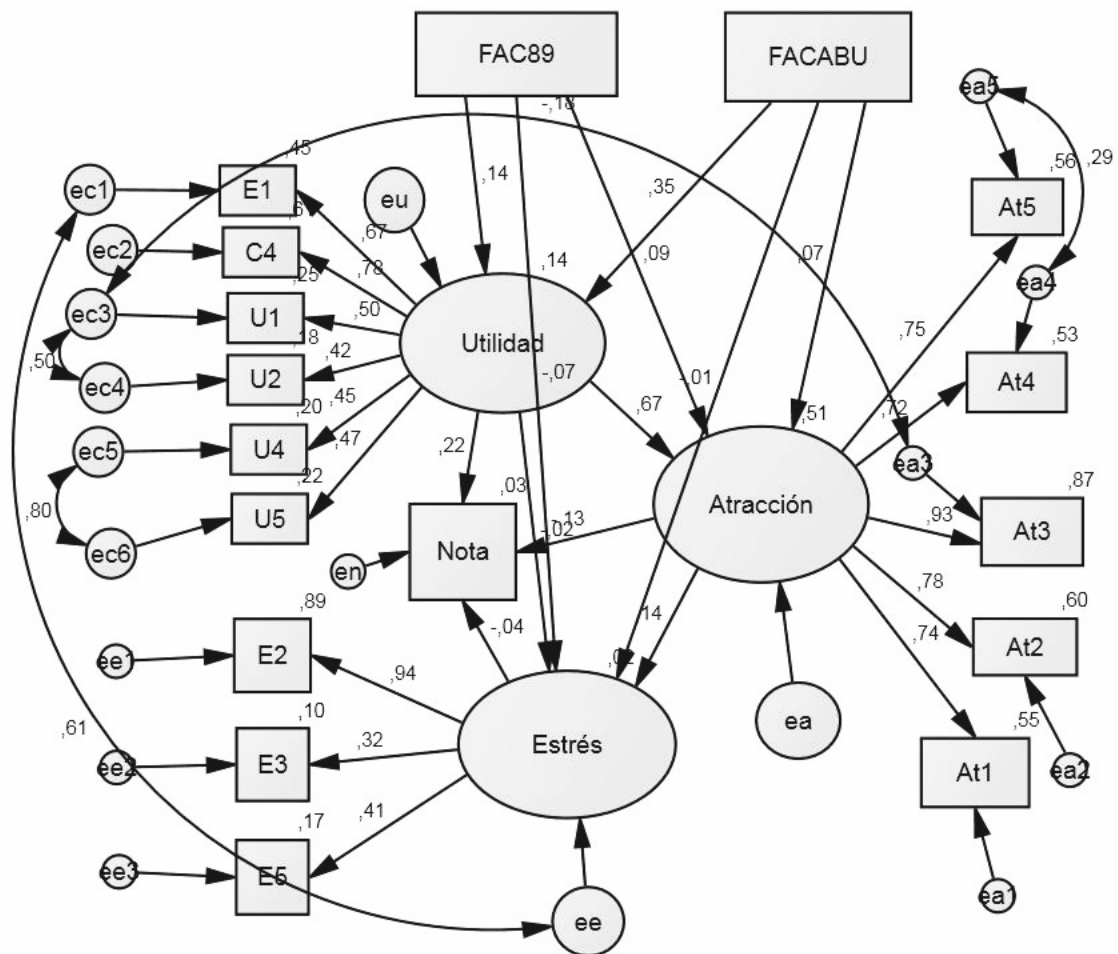
Tabla 19. Parámetros encuesta ambos cursos

Factor / variables (valores deseables)	KMO	Varianza	Alfa Cronbach	Significatividad
	>0,5	>60%	>0,6	<5%
Atracción/ At1, At2, At3, At4, At5	0,860	71%	0,898	<1%
Estrés/ E2, E3, E5	0,661	60%	0,669	<1%
Utilidad/ U3, U4, U5	0,657	74%	0,805	<1%
Confianza/ C1, C2, C4	0,669	62%	0,696	<1%
Conjunta (todas las variables)	0,872	69%	0,853	<1%

Fuente: EP

5.3.2 Estadísticos estructurales

Ensayando el modelo estructural visto en el grafo 4 correspondiente a los alumnos del curso 2011-2012, pero aplicándolo a los datos obtenidos de los alumnos del curso 2012-2013 conseguimos el siguiente ajuste:



Grafo 4bis. Modelo sugerido, con variables de control, del curso 2012-2013 (EP)

Siendo 196,7 el valor obtenido para Chi-square, 105 los grados de libertad y 0,93 el CFI, la bondad de ajuste del modelo no es tan perfecto como en el caso del curso anterior pero sigue siendo aceptable reflejando los siguientes parámetros

Tabla 20. Resultados proceso grafo 4bis

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,068	,053	,082	,026

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
Utilidad	<---	FACABU	,123	,033	3,681	***	par_15
Utilidad	<---	FAC89	,049	,029	1,710	,087	par_19
Atracción	<---	Utilidad	1,362	,274	4,968	***	par_12
Atracción	<---	FACABU	,051	,049	1,027	,305	par_17
Atracción	<---	FAC89	,063	,045	1,386	,166	par_20
Estrés	<---	Utilidad	-,024	,182	-,134	,893	par_13
Estrés	<---	Atracción	,083	,079	1,047	,295	par_14
Estrés	<---	FACABU	-,005	,032	-,145	,885	par_16
Estrés	<---	FAC89	-,030	,030	-,994	,320	par_18
U5	<---	Utilidad	1,000				
U4	<---	Utilidad	1,027	,102	10,044	***	par_1
U2	<---	Utilidad	1,120	,260	4,312	***	par_2
U1	<---	Utilidad	1,303	,273	4,776	***	par_3
C4	<---	Utilidad	2,020	,345	5,848	***	par_4
E1	<---	Utilidad	1,784	,323	5,531	***	par_5
E5	<---	Estrés	1,000				
E3	<---	Estrés	,828	,234	3,540	***	par_6
E2	<---	Estrés	2,407	,588	4,094	***	par_7
At5	<---	Atracción	1,000				
At4	<---	Atracción	1,083	,090	12,018	***	par_8
At3	<---	Atracción	1,271	,098	12,936	***	par_9
At2	<---	Atracción	1,126	,103	10,919	***	par_10
At1	<---	Atracción	1,027	,099	10,384	***	par_11
Nota	<---	Utilidad	1,345	,834	1,614	,107	par_21
Nota	<---	Atracción	-,402	,377	-1,065	,287	par_22
Nota	<---	Estrés	-,213	,385	-,553	,580	par_23

Standardized Regression Weights: (Group number 1 - Default model)

			Estimate
Utilidad	<---	FACABU	,346
Utilidad	<---	FAC89	,139
Atracción	<---	Utilidad	,672
Atracción	<---	FACABU	,070
Atracción	<---	FAC89	,087
Estrés	<---	Utilidad	-,020
Estrés	<---	Atracción	,137
Estrés	<---	FACABU	-,011
Estrés	<---	FAC89	-,070
U5	<---	Utilidad	,466
U4	<---	Utilidad	,451
U2	<---	Utilidad	,424
U1	<---	Utilidad	,499
C4	<---	Utilidad	,778
E1	<---	Utilidad	,674
E5	<---	Estrés	,408
E3	<---	Estrés	,322
E2	<---	Estrés	,943
At5	<---	Atracción	,747
At4	<---	Atracción	,725
At3	<---	Atracción	,932
At2	<---	Atracción	,778
At1	<---	Atracción	,743
Nota	<---	Utilidad	,220
Nota	<---	Atracción	-,133
Nota	<---	Estrés	-,043

Fuente: AMOS (EP)

La significatividad es excelente (<1%) y directa entre:

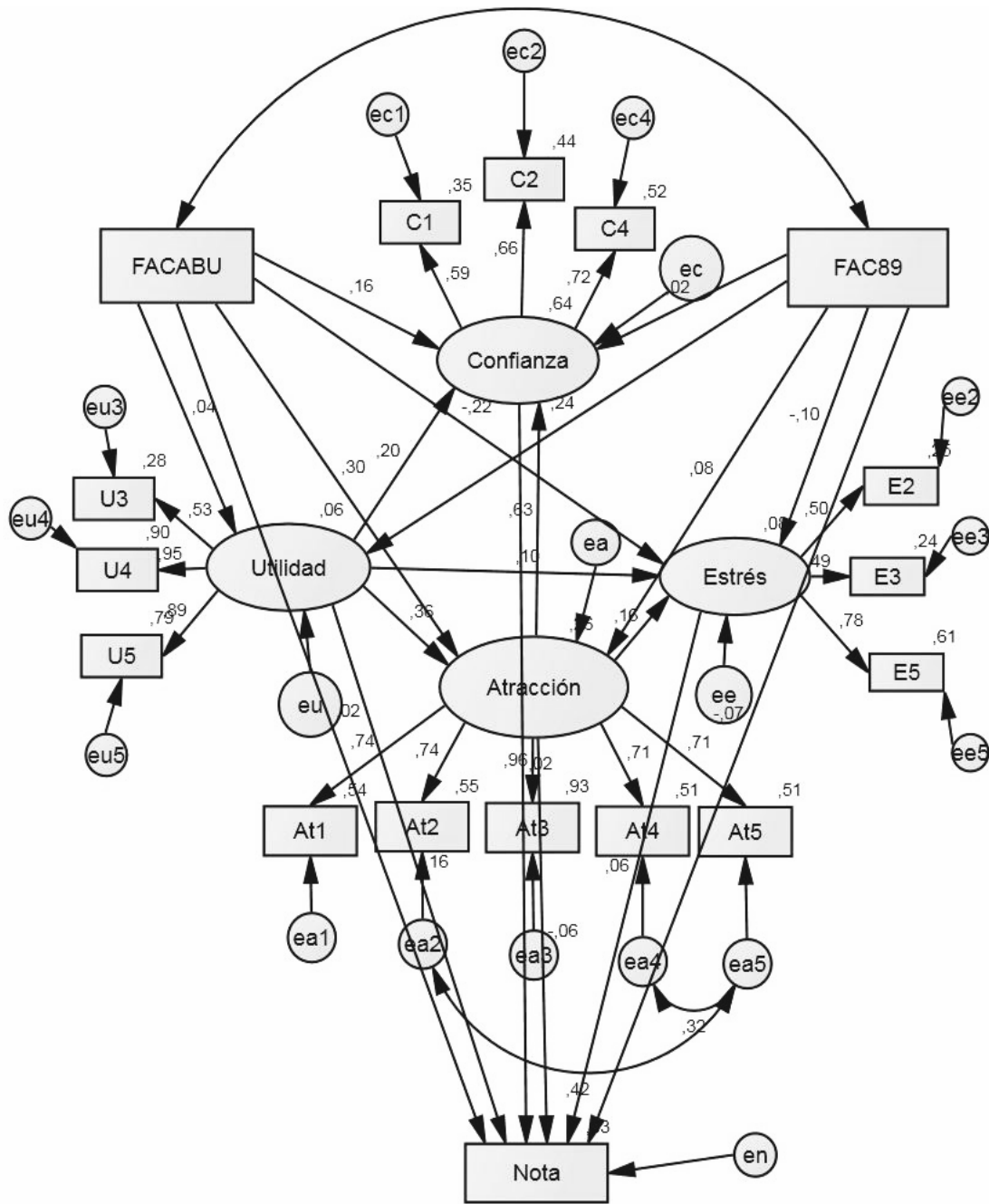
- Utilidad → Atracción (regr. 0,672),
- FACABU → Utilidad (regr. 0,346) , y
- entre las relaciones de las latentes y sus observables

Las “Notas” siguen siendo no significativas y de bajo valor. Es decir, respecto estos parámetros, los mejores estudiantes de este curso tampoco se diferencian de los no tan buenos. Continua faltando información adecuada a todos los niveles pues ni siquiera los mejores actúan con suficiente seguridad.

Existe un valor de regresión muy alto entre Utilidad y Atracción (0,672) que mantiene que cuando los alumnos entienden que algo es útil se sienten más atraídos.

También tenemos un valor bastante alto de regresión total (0,346) entre FACABU → Utilidad con un 1% de significatividad, lo que implica que los alumnos que son más cuidadosos con la protección de sus datos consideran más útil adoptar medidas de seguridad.

Adicionalmente, analizamos la modelización correspondiente a la totalidad de las variables latentes definidas en la tabla 19 aplicándola sobre los datos obtenidos con los alumnos del curso 2012-2013. Manteniendo las trayectorias de causalidad de estudios similares referenciados con esas latentes (Anexo 1), obtuvimos los siguientes resultados



Grafo 5. Modelo de cuatro constructos con los alumnos del curso 2012-13 (EP)

Los resultados del modelo con los cuatro constructos previstos en el modelo inicial, con los alumnos del curso 2012-2013, dan unos parámetros de bondad de ajuste muy satisfactorios, con un Comparative fit index (CFI) de 0,96 y unos residuos (RMSEA) entre 0,034 y 0,068, como puede verse a continuación.

Tabla 21. Resultados proceso global con alumnos 2012-2013

Result (Default model)

Minimum was achieved
 Chi-square = 150,567
 Degrees of freedom = 100
 Probability level = ,001

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,892	,852	,961	,945	,960
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,051	,034	,068	,427
Independence model	,220	,209	,230	,000

Covariances: (Group number 1 - Default model)

	Estimate	S.E.	C.R.	P	Label
FAC89 <--> FACABU	,147	,073	2,021	,043	par_29
ea5 <--> ea4	,163	,038	4,278	***	par_31
ea5 <--> ea2	,196	,039	5,081	***	par_32

Correlations: (Group number 1 - Default model)

	Estimate
FAC89 <--> FACABU	,148
ea5 <--> ea4	,318
ea5 <--> ea2	,416

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
Utilidad	<---	FACABU	,030	,050	,592	,554	par_12
Utilidad	<---	FAC89	,161	,051	3,180	,001	par_27
Atracción	<---	FACABU	,203	,048	4,245	***	par_13
Atracción	<---	Utilidad	,364	,077	4,722	***	par_15
Atracción	<---	FAC89	,054	,047	1,147	,252	par_26
Confianza	<---	FAC89	,011	,042	,271	,786	par_11
Estrés	<---	FAC89	-,056	,050	-1,114	,265	par_14
Estrés	<---	Utilidad	,084	,083	1,008	,314	par_16
Estrés	<---	Atracción	,126	,088	1,436	,151	par_17
Confianza	<---	FACABU	,098	,044	2,202	,028	par_18
Confianza	<---	Utilidad	,185	,073	2,546	,011	par_19
Confianza	<---	Atracción	,571	,101	5,676	***	par_28
Estrés	<---	FACABU	-,122	,056	-2,184	,029	par_30
C1	<---	Confianza	1,000				
C2	<---	Confianza	,898	,134	6,692	***	par_1
C4	<---	Confianza	1,077	,153	7,042	***	par_2
U5	<---	Utilidad	1,000				
U4	<---	Utilidad	1,131	,079	14,392	***	par_3
U3	<---	Utilidad	,807	,104	7,791	***	par_4
E2	<---	Estrés	1,000				
E3	<---	Estrés	,996	,228	4,374	***	par_5
E5	<---	Estrés	1,504	,380	3,959	***	par_6
At5	<---	Atracción	1,000				
At4	<---	Atracción	1,121	,097	11,588	***	par_7
At3	<---	Atracción	1,391	,113	12,261	***	par_8
At2	<---	Atracción	1,139	,087	13,101	***	par_9
At1	<---	Atracción	1,074	,108	9,906	***	par_10
Nota	<---	Confianza	,081	,625	,130	,897	par_20
Nota	<---	Atracción	-,184	,463	-,398	,691	par_21
Nota	<---	Estrés	,248	,360	,690	,490	par_22
Nota	<---	Utilidad	,528	,295	1,792	,073	par_23
Nota	<---	FACABU	,049	,182	,269	,788	par_24
Nota	<---	FAC89	-,160	,164	-,973	,330	par_25

Standardized Total Effects (Group number 1 - Default model)

	FACABU	FAC89	Utilidad	Atracción	Estrés	Confianza
Utilidad	,044	,237	,000	,000	,000	,000
Atracción	,311	,164	,360	,000	,000	,000
Estrés	-,168	-,052	,159	,156	,000	,000
Confianza	,362	,169	,428	,629	,000	,000
Nota	,009	-,043	,164	-,034	,063	,023
At1	,229	,121	,265	,736	,000	,000
At2	,232	,122	,268	,745	,000	,000
At3	,299	,158	,346	,962	,000	,000
At4	,221	,116	,256	,711	,000	,000
At5	,221	,117	,256	,712	,000	,000
E5	-,130	-,040	,124	,121	,778	,000
E3	-,083	-,025	,078	,077	,492	,000
E2	-,083	-,026	,079	,078	,497	,000
U3	,023	,125	,528	,000	,000	,000
U4	,041	,225	,947	,000	,000	,000
U5	,039	,211	,888	,000	,000	,000
C4	,262	,122	,309	,455	,000	,723
C2	,239	,112	,283	,415	,000	,660
C1	,215	,101	,255	,374	,000	,595

Fuente: AMOS (EP)

La significatividad es excelente (<1%) y directa entre:

- FACA89 → Utilidad,
- FACABU → Atracción,
- Utilidad → Atracción,
- Atracción → Confianza, y
- entre las relaciones de las latentes y sus observables,

Algo menor (<5%) entre:

- FACABU → Confianza
- Utilidad → Confianza y FACABU → Estrés

Las “Notas” no son significativas y de escaso valor. Tan solo existe cierto grado de significatividad (<8%) entre Utilidad y Nota pero de valor muy bajo (0,164), con lo que se mantienen las afirmaciones descritas anteriormente respecto esta variable.

Existe correspondencia entre FACA89 y Utilidad (0,237), más alta entre FACABU y Atracción (0,311), y entre FACABU y Confianza (0,362) y lógicamente de signo contrario entre FACABU y Estrés (los alumnos que más protegen sus datos se preocupan menos).

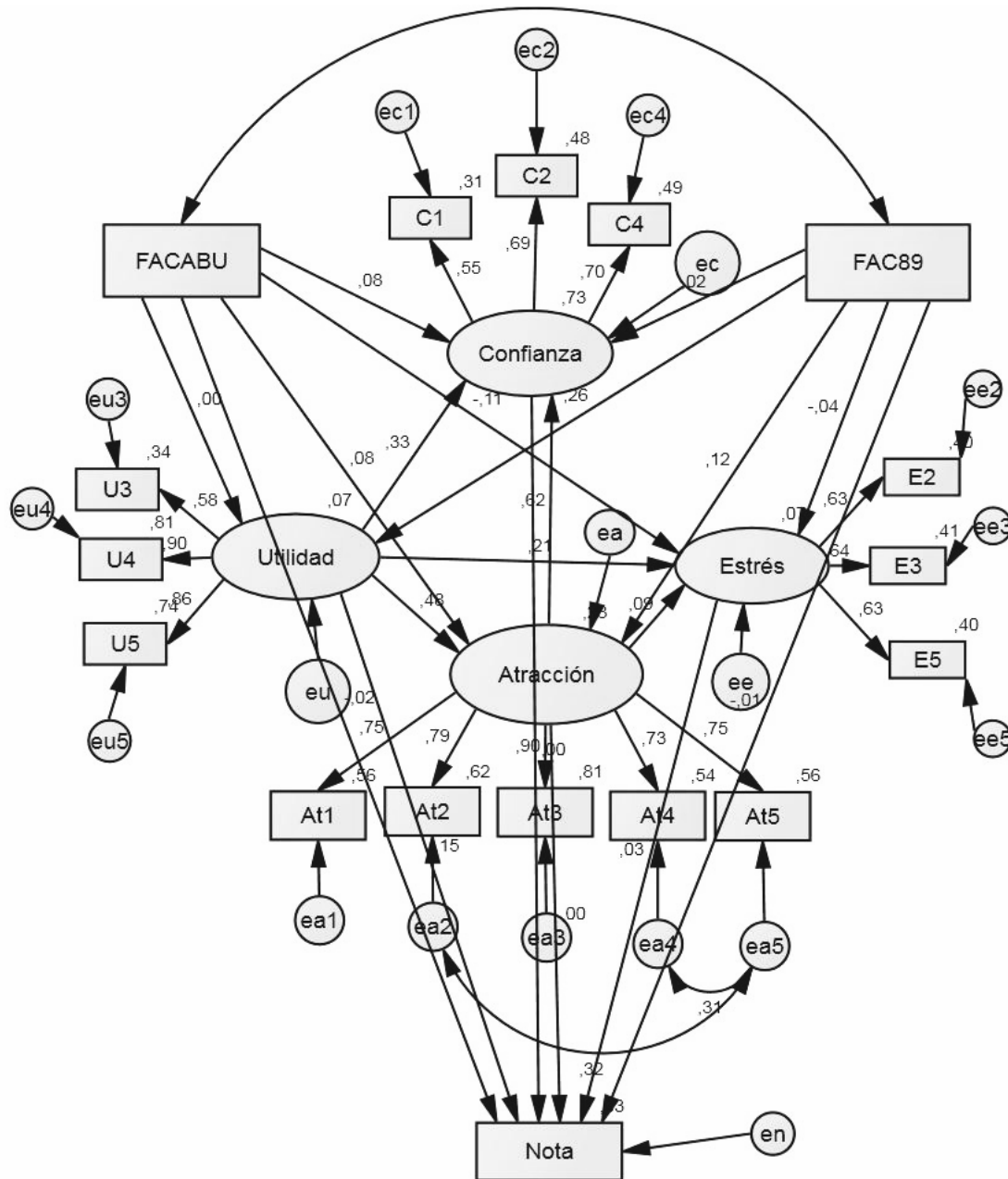
Hay un valor de regresión alto entre Utilidad y Atracción (0,36) que confirma que lo considerado útil genera atracción.

Sobre la variable latente Confianza influyen de forma decisiva las variables latentes Utilidad (0,428) y Atracción (0,629). Cuando estas últimas crecen una unidad, la Confianza crece en la medida indicada por cada una de ellas.

En definitiva, si algo es útil nos atrae y nos genera confianza. Y a mayor atracción, mucha mayor confianza.

5.4 Modelos estructurales completos

Probando el mismo modelo presentado en el grafo 5, pero aplicado a la totalidad de alumnos de los dos cursos, obtenemos los siguientes resultados con un excelente ajuste:



Grafo 6. Modelo de cuatro constructos con todos los alumnos de los dos cursos (EP)

Tabla 22. Resultados proceso global con alumnos ambos cursos

Result (Default model)

Minimum was achieved
 Chi-square = 150,162
 Degrees of freedom = 100
 Probability level = ,001

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,943	,922	,980	,973	,980
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,036	,023	,047	,983
Independence model	,216	,208	,223	,000

Covariances: (Group number 1 - Default model)

	Estimate	S.E.	C.R.	P	Label
FAC89 <--> FACABU	,083	,050	1,645	,100	par_29
ea5 <--> ea4	,144	,027	5,359	***	par_31
ea5 <--> ea2	,127	,025	5,164	***	par_32

Correlations: (Group number 1 - Default model)

	Estimate
FAC89 <--> FACABU	,083
ea5 <--> ea4	,311
ea5 <--> ea2	,317

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
Utilidad	<---	FACABU	,002	,037	,055	,956	par_12
Utilidad	<---	FAC89	,187	,037	5,013	***	par_27
Atracción	<---	FACABU	,058	,034	1,679	,093	par_13
Atracción	<---	Utilidad	,493	,060	8,285	***	par_15
Atracción	<---	FAC89	,084	,036	2,345	,019	par_26
Confianza	<---	FAC89	,013	,026	,507	,612	par_11
Estrés	<---	FAC89	-,028	,044	-,625	,532	par_14
Estrés	<---	Utilidad	,203	,079	2,570	,010	par_16
Estrés	<---	Atracción	,083	,075	1,113	,266	par_17
Confianza	<---	FACABU	,047	,026	1,833	,067	par_18
Confianza	<---	Utilidad	,267	,051	5,229	***	par_19
Confianza	<---	Atracción	,484	,062	7,768	***	par_28
Estrés	<---	FACABU	-,076	,043	-1,785	,074	par_30
C1	<---	Confianza	1,000				
C2	<---	Confianza	1,073	,113	9,471	***	par_1
C4	<---	Confianza	1,093	,115	9,535	***	par_2
U5	<---	Utilidad	1,000				
U4	<---	Utilidad	1,050	,055	19,025	***	par_3
U3	<---	Utilidad	,821	,068	12,042	***	par_4
E2	<---	Estrés	1,000				
E3	<---	Estrés	1,001	,132	7,557	***	par_5
E5	<---	Estrés	,948	,125	7,559	***	par_6
At5	<---	Atracción	1,000				
At4	<---	Atracción	1,075	,062	17,473	***	par_7
At3	<---	Atracción	1,184	,067	17,562	***	par_8
At2	<---	Atracción	1,104	,058	18,989	***	par_9
At1	<---	Atracción	1,028	,070	14,716	***	par_10
Nota	<---	Confianza	-,009	,623	-,014	,989	par_20
Nota	<---	Atracción	,012	,371	,032	,974	par_21
Nota	<---	Estrés	,104	,204	,510	,610	par_22
Nota	<---	Utilidad	,474	,269	1,764	,078	par_23
Nota	<---	FACABU	-,039	,116	-,339	,735	par_24
Nota	<---	FAC89	-,021	,117	-,178	,858	par_25

Standardized Total Effects (Group number 1 - Default model)

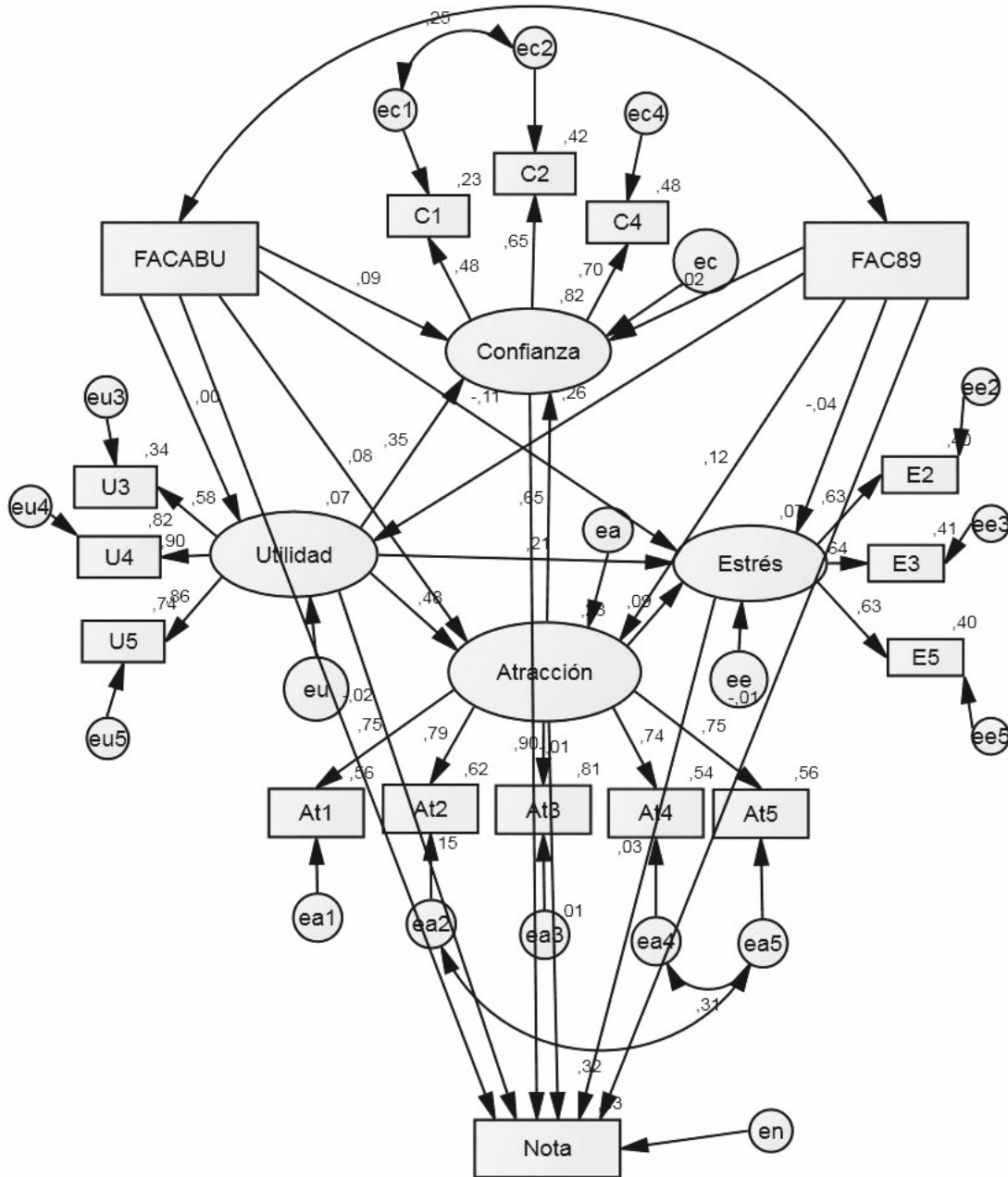
	FACABU	FAC89	Utilidad	Atracción	Estrés	Confianza
Utilidad	,003	,264	,000	,000	,000	,000
Atracción	,080	,242	,480	,000	,000	,000
Estrés	-,102	,036	,248	,087	,000	,000
Confianza	,132	,260	,628	,617	,000	,000
Nota	-,021	,032	,160	,005	,033	-,002
At1	,060	,181	,358	,746	,000	,000
At2	,063	,191	,379	,789	,000	,000
At3	,072	,217	,431	,899	,000	,000
At4	,059	,178	,353	,735	,000	,000
At5	,060	,182	,360	,750	,000	,000
E5	-,065	,023	,157	,055	,635	,000
E3	-,065	,023	,158	,056	,639	,000
E2	-,064	,023	,156	,055	,631	,000
U3	,002	,153	,580	,000	,000	,000
U4	,003	,238	,902	,000	,000	,000
U5	,002	,227	,862	,000	,000	,000
C4	,093	,183	,441	,433	,000	,702
C2	,092	,180	,435	,428	,000	,693
C1	,073	,144	,347	,341	,000	,553

Modification Indices (Group number 1 – Default model). Covariances:

			M.I.	Par Change
ec	<-->	ee	5,115	,047
ea2	<-->	ec	6,154	-,038
ea4	<-->	ee	5,141	-,067
ea4	<-->	ec	4,585	-,038
ea5	<-->	FACABU	4,801	-,064
ea5	<-->	ee	10,738	,080
ee5	<-->	ea5	8,264	,076
ee3	<-->	eu	4,383	-,073
eu3	<-->	ee5	7,061	-,102
eu4	<-->	ee5	4,112	,045
eu4	<-->	ee3	4,800	-,051
ec4	<-->	ea1	6,317	,063
ec2	<-->	ea5	5,286	,047
ec2	<-->	ec4	9,582	-,074
ec1	<-->	ec	10,183	,067
ec1	<-->	ea2	7,520	-,077
ec1	<-->	ea4	5,255	-,073
ec1	<-->	ea5	5,166	,059
ec1	<-->	ec2	12,310	,110

Fuente: AMOS (EP)

Siguiendo la recomendación de modificación de índices, covariando ec1 con ec2, llegamos a los siguientes valores:



Grafo 6bis. Modelo optimizado de cuatro constructos con los alumnos de ambos cursos (EP)

Tabla 23. Resultados optimizados del proceso global con alumnos ambos cursos

Result (Default model)

Minimum was achieved
 Chi-square = 133,814
 Degrees of freedom = 99
 Probability level = ,011

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,949	,930	,986	,981	,986
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,030	,015	,042	,998
Independence model	,216	,208	,223	,000

Covariances: (Group number 1 - Default model)

	Estimate	S.E.	C.R.	P	Label
FAC89 <--> FACABU	,083	,050	1,645	,100	par_29
ea5 <--> ea4	,145	,027	5,387	***	par_31
ea5 <--> ea2	,128	,025	5,200	***	par_32
ec1 <--> ec2	,149	,038	3,927	***	par_33

Correlations: (Group number 1 - Default model)

	Estimate
FAC89 <--> FACABU	,083
ea5 <--> ea4	,312
ea5 <--> ea2	,318
ec1 <--> ec2	,246

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
Utilidad	<---	FACABU	,002	,037	,054	,957	par_12
Utilidad	<---	FAC89	,187	,037	5,017	***	par_27
Atracción	<---	FACABU	,058	,034	1,682	,092	par_13
Atracción	<---	Utilidad	,493	,060	8,282	***	par_15
Atracción	<---	FAC89	,084	,036	2,346	,019	par_26
Confianza	<---	FAC89	,009	,024	,369	,712	par_11
Estrés	<---	FAC89	-,027	,044	-,620	,536	par_14
Estrés	<---	Utilidad	,203	,079	2,565	,010	par_16
Estrés	<---	Atracción	,083	,075	1,100	,272	par_17
Confianza	<---	FACABU	,047	,023	2,037	,042	par_18
Confianza	<---	Utilidad	,250	,048	5,187	***	par_19
Confianza	<---	Atracción	,447	,061	7,287	***	par_28
Estrés	<---	FACABU	-,076	,043	-1,783	,075	par_30
C1	<---	Confianza	1,000				
C2	<---	Confianza	1,151	,123	9,366	***	par_1
C4	<---	Confianza	1,240	,147	8,413	***	par_2
U5	<---	Utilidad	1,000				
U4	<---	Utilidad	1,052	,055	19,079	***	par_3
U3	<---	Utilidad	,823	,068	12,052	***	par_4
E2	<---	Estrés	1,000				
E3	<---	Estrés	1,001	,132	7,556	***	par_5
E5	<---	Estrés	,948	,125	7,558	***	par_6
At5	<---	Atracción	1,000				
At4	<---	Atracción	1,077	,062	17,461	***	par_7
At3	<---	Atracción	1,185	,068	17,518	***	par_8
At2	<---	Atracción	1,106	,058	18,972	***	par_9
At1	<---	Atracción	1,032	,070	14,719	***	par_10
Nota	<---	Confianza	-,048	1,113	-,043	,966	par_20
Nota	<---	Atracción	,029	,547	,054	,957	par_21
Nota	<---	Estrés	,105	,204	,516	,606	par_22
Nota	<---	Utilidad	,483	,350	1,381	,167	par_23
Nota	<---	FACABU	-,037	,124	-,302	,763	par_24
Nota	<---	FAC89	-,020	,117	-,176	,861	par_25

Standardized Total Effects (Group number 1 - Default model)

	FACABU	FAC89	Utilidad	Atracción	Estrés	Confianza
Utilidad	,003	,264	,000	,000	,000	,000
Atracción	,081	,242	,480	,000	,000	,000
Estrés	-,102	,036	,247	,086	,000	,000
Confianza	,148	,269	,668	,652	,000	,000
Nota	-,021	,032	,160	,005	,033	-,011
At1	,060	,181	,359	,748	,000	,000
At2	,064	,191	,379	,789	,000	,000
At3	,072	,217	,431	,898	,000	,000
At4	,059	,178	,353	,735	,000	,000
At5	,060	,181	,359	,749	,000	,000
E5	-,065	,023	,157	,055	,635	,000
E3	-,065	,023	,158	,055	,639	,000
E2	-,064	,023	,156	,054	,630	,000
U3	,002	,153	,581	,000	,000	,000
U4	,003	,238	,903	,000	,000	,000
U5	,002	,227	,861	,000	,000	,000
C4	,103	,187	,464	,454	,000	,695
C2	,096	,175	,433	,423	,000	,649
C1	,071	,130	,322	,315	,000	,483

Standardized Direct Effects (Group number 1 - Default model)

	FACABU	FAC89	Utilidad	Atracción	Estrés	Confianza
Utilidad	,003	,264	,000	,000	,000	,000
Atracción	,079	,115	,480	,000	,000	,000
Estrés	-,109	-,039	,206	,086	,000	,000
Confianza	,095	,018	,355	,652	,000	,000
Nota	-,017	-,009	,154	,010	,033	-,011
At1	,000	,000	,000	,748	,000	,000
At2	,000	,000	,000	,789	,000	,000
At3	,000	,000	,000	,898	,000	,000
At4	,000	,000	,000	,735	,000	,000
At5	,000	,000	,000	,749	,000	,000
E5	,000	,000	,000	,000	,635	,000
E3	,000	,000	,000	,000	,639	,000
E2	,000	,000	,000	,000	,630	,000
U3	,000	,000	,581	,000	,000	,000
U4	,000	,000	,903	,000	,000	,000
U5	,000	,000	,861	,000	,000	,000
C4	,000	,000	,000	,000	,000	,695
C2	,000	,000	,000	,000	,000	,649
C1	,000	,000	,000	,000	,000	,483

Variances: (Group number 1 - Default model)

	Estimate	S.E.	C.R.	P	Label
FAC89	,995	,071	14,053	***	par_51
FACABU	,995	,071	14,053	***	par_52
eu	,465	,047	9,911	***	par_53
ea	,379	,047	8,070	***	par_54
ec	,044	,019	2,312	,021	par_55
ee	,452	,086	5,239	***	par_56
ec1	,815	,063	12,907	***	par_57
ec2	,452	,040	11,220	***	par_58
ec4	,407	,040	10,308	***	par_59
eu5	,174	,023	7,577	***	par_60
eu4	,125	,023	5,423	***	par_61
eu3	,666	,051	13,170	***	par_62
ee2	,738	,080	9,248	***	par_63
ee3	,706	,078	9,012	***	par_64
ee5	,649	,071	9,134	***	par_65
ea5	,413	,034	12,038	***	par_66
ea4	,521	,043	12,174	***	par_67
ea3	,178	,024	7,526	***	par_68
ea2	,391	,034	11,354	***	par_69
ea1	,443	,037	12,064	***	par_70
en	4,784	,342	14,001	***	par_71

Fuente: AMOS (EP)

A la vista de los resultados del modelo podemos asegurar que la bondad (calidad) del mismo es excelente, con un CFI de 0,986 y unos residuos entre 0,015 y 0,042 para la totalidad de la población con encuesta válida (alumnos de los dos cursos) y una relación $\text{Chi}^2 / \text{grados de libertad}$ de 1,35.

Hemos conseguido obtener un ajuste que se corresponde con el modelo teórico de cuatro constructos y las interpretaciones que podemos derivar son las siguientes:

Son significativas (<2%) las relaciones entre

- FAC89 y Utilidad,
- entre FAC89 y Atracción,
- entre Utilidad y Atracción,

- entre Utilidad y Estrés,
- entre Utilidad y Confianza,
- entre Atracción y Confianza, y lógicamente ...
- entre los constructos y las variables que los definen.

En menor medida (<5%) entre

- entre FACABU y Confianza, y

a tener en cuenta (<10%) entre

- FACABU y Estrés, y
- FACABU y Atracción

Cuando observamos el peso de los efectos totales considerados, nos damos cuenta que:

- Utilidad es importante sobre Estrés (0,247),
- así como FAC89 sobre Utilidad (0,264) y Atracción (0,242), aunque esta última se reparte entre directa e indirectamente (a través de Utilidad).
- Utilidad sobre Atracción tiene mucha influencia (0,48), y sobre todo
- Utilidad sobre Confianza tiene muchísima influencia (0,668), también repartido entre directa e indirectamente (a través de Atracción).
- También influye muchísimo Atracción sobre Confianza (0,652).

Tienen menos relación y significatividad

- FACABU sobre Estrés (en dirección contraria), y FACABU sobre Confianza, y
- Sin importancia de FACABU sobre Atracción.

Observamos que los alumnos que más se preocupan por proteger su privacidad (FAC89) son los que consideran más útiles (Utilidad) los sistemas de protección en su navegación y se sienten más atraídos (Atracción) por su implementación.

Utilidad es un constructo que influye mucho en la Atracción y en la Confianza y, en menor medida, sobre el Estrés. Lo que significa que los que ven útil poner en práctica medidas de seguridad, se sienten más atraídos por conocerlas y tienen más confianza aunque hay un porcentaje significativo que no se siente suficientemente seguro (con mayor estrés).

La Confianza recibe la influencia de Atracción y también de Utilidad, tanto directamente como incrementando su influencia a través de Atracción.

La covarianza entre FACABU y FAC89 es escasa y poco significativa (10%).

Ni hay significatividad ni los parámetros tienen relevancia en lo que cada constructo se correlaciona con la Nota. Tampoco hay correlación significativa con Nota por parte de los alumnos que son más o menos cuidadosos con la protección de su privacidad o de sus datos (FAC89 y FACABU). Lo que nos viene a decir que el comportamiento de los alumnos en su vida “real” no tiene nada que ver con el grado de aprovechamiento en sus estudios. No deja de sorprendernos pues parece que estudian para aprobar, pero no aprenden y no incorporan en su vida las enseñanzas que, supuestamente, han recibido pero no asimilado.

Algo parecido sucede con el nivel de protección de sus datos generando procedimientos de backup. Correlaciones significativas con Confianza (>5 %) y a tener en cuenta (<10%), con Atracción y Estrés (en negativo) pero siempre de bajo valor. Parece como si les diese igual, que no les importa.

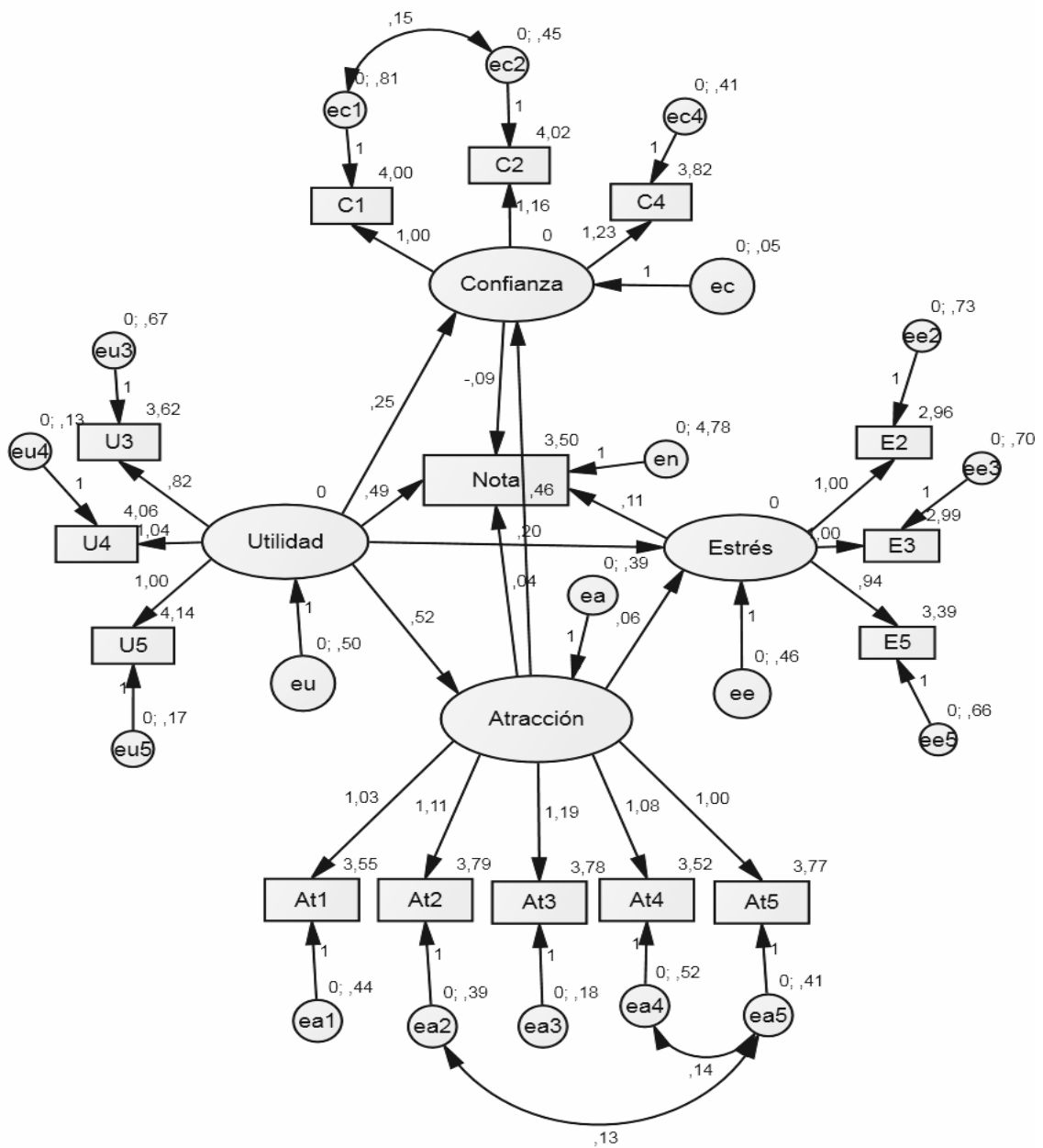
En resumen, si hacemos comprender a nuestros alumnos la ventaja de entender la utilidad de la navegación segura, conseguiremos incrementar su atracción hacia ese tipo de medidas e incrementar su confianza y seguridad.

Estamos utilizando habitualmente la forma de representación gráfica de los modelos causales que estamos planteando, por ser la más sencilla de observación y obtención de conclusiones. Pero también es posible representarlos mediante la notación algebraica. Ambas formas son equivalentes, aunque una utiliza los diagramas de caminos y la otra la formulación matemática mediante ecuaciones.

Para la representación algebraica (grafo 6tris) de los resultados obtenidos con el modelo básico (con independencia de variables independientes exógenas, de control) del grafo 6bis tendríamos en cuenta los siguientes factores:

Indicadores correspondientes a las variables latentes endógenas, incluida la dependiente (Nota): At5, At4, At3, At2, At1, E2, E3, E5, C1, C2, C4, U5, U4, U3, Nota

Variables latentes endógenas: Atracción, Estrés, Confianza, Utilidad



Grafo 6tris. Modelo básico de cuatro constructos optimizado con los alumnos de ambos cursos (EP)

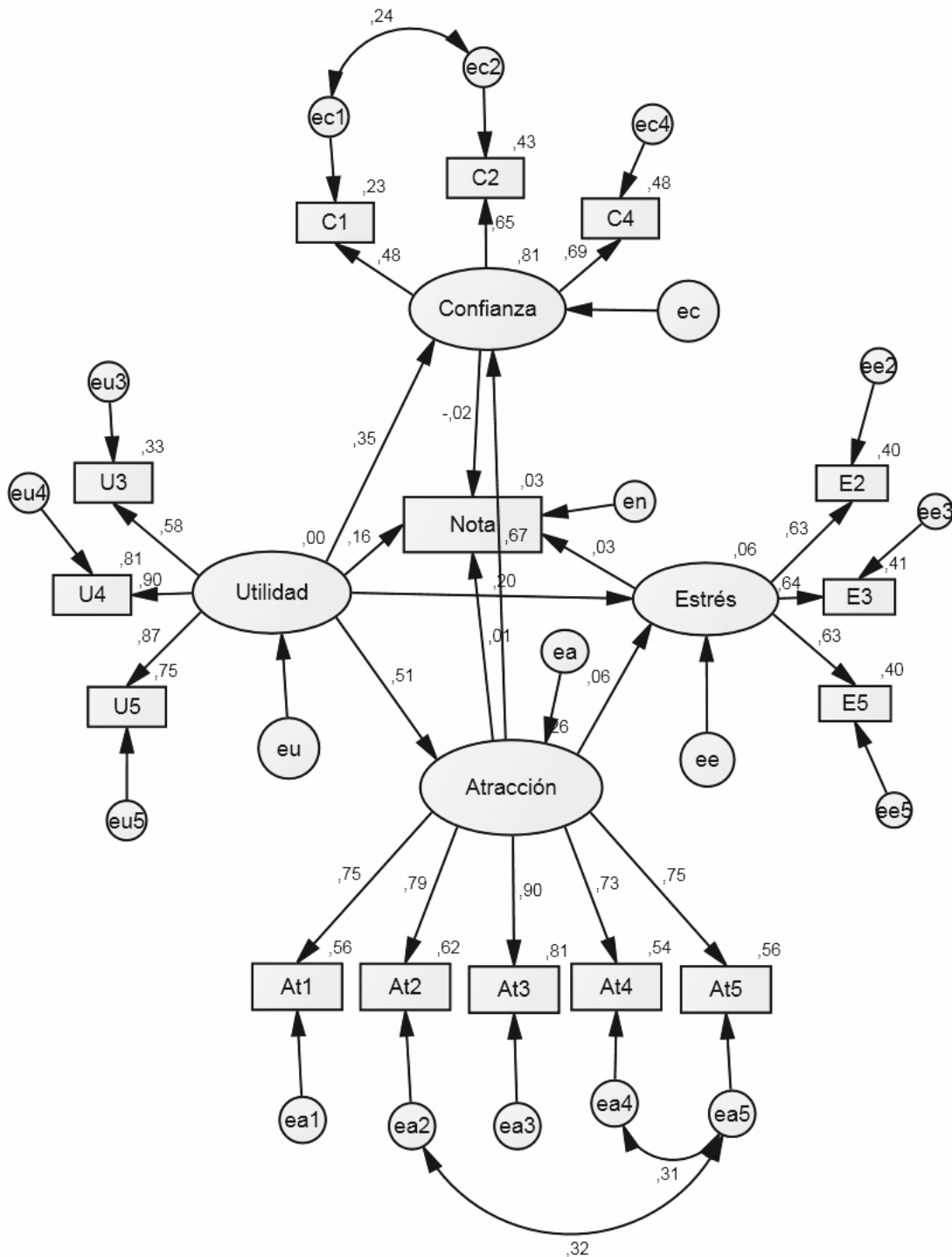
Sus respectivas matrices de impactos y errores asociados, nos dejan las siguientes ecuaciones:

$$\begin{pmatrix} \text{At5} \\ \text{At4} \\ \text{At3} \\ \text{At2} \\ \text{At1} \\ \text{E2} \\ \text{E3} \\ \text{E5} \\ \text{C1} \\ \text{C2} \\ \text{C4} \\ \text{U5} \\ \text{U4} \\ \text{U3} \\ \text{Nota} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1,08 & 0 & 0 & 0 \\ 1,19 & 0 & 0 & 0 \\ 1,11 & 0 & 0 & 0 \\ 1,03 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0,94 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1,16 & 0 \\ 0 & 0 & 1,23 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1,04 \\ 0 & 0 & 0 & 0,82 \\ 0,04 & 0,11 & -0,09 & 0,49 \end{pmatrix} \times \begin{pmatrix} \text{Atracción} \\ \text{Estrés} \\ \text{Confianza} \\ \text{Utilidad} \end{pmatrix} + \begin{pmatrix} 0,41 \\ 0,52 \\ 0,18 \\ 0,39 \\ 0,44 \\ 0,73 \\ 0,7 \\ 0,66 \\ 0,81 \\ 0,45 \\ 0,41 \\ 0,17 \\ 0,13 \\ 0,67 \\ 4,78 \end{pmatrix}$$

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
Atracción	<---	Utilidad	,524	,059	8,903	***	par_11
Estrés	<---	Utilidad	,200	,078	2,556	,011	par_12
Estrés	<---	Atracción	,062	,075	,834	,404	par_13
Confianza	<---	Utilidad	,249	,048	5,212	***	par_14
Confianza	<---	Atracción	,458	,062	7,374	***	par_19
C1	<---	Confianza	1,000				
C2	<---	Confianza	1,156	,124	9,353	***	par_1
C4	<---	Confianza	1,229	,147	8,355	***	par_2
U5	<---	Utilidad	1,000				
U4	<---	Utilidad	1,042	,055	18,920	***	par_3
U3	<---	Utilidad	,816	,068	11,999	***	par_4
E2	<---	Estrés	1,000				
E3	<---	Estrés	1,002	,133	7,511	***	par_5
E5	<---	Estrés	,937	,125	7,519	***	par_6
At5	<---	Atracción	1,000				
At4	<---	Atracción	1,076	,062	17,453	***	par_7
At3	<---	Atracción	1,187	,068	17,536	***	par_8
At2	<---	Atracción	1,106	,058	18,971	***	par_9
At1	<---	Atracción	1,031	,070	14,705	***	par_10
Nota	<---	Confianza	-,091	1,070	-,085	,933	par_15
Nota	<---	Atracción	,038	,539	,070	,945	par_16
Nota	<---	Estrés	,111	,201	,551	,582	par_17
Nota	<---	Utilidad	,489	,338	1,447	,148	par_18

A su vez, los valores estandarizados de las variables latentes se construyen desde sus respectivas variables observables, con los siguientes niveles de influencia que se muestran en el grafo 6-tetrakis:



Grafo 6-tetrakis. Modelo básico de cuatro constructos optimizado con los alumnos de ambos cursos – valores estandarizados (EP)

$$\text{Confianza} = 0,484 C1 + 0,653 C2 + 0,69 C4$$

$$\text{Utilidad} = 0,579 U3 + 0,899 U4 + 0,866 U5$$

$$\text{Estrés} = 0,633 E2 + 0,642 E3 + 0,63 E5$$

$$\text{Atracción} = 0,747 At1 + 0,789 At2 + 0,899 At3 + 0,734 At4 + 0,749 At5$$

Standardized Regression Weights: (Group number 1 - Default model)

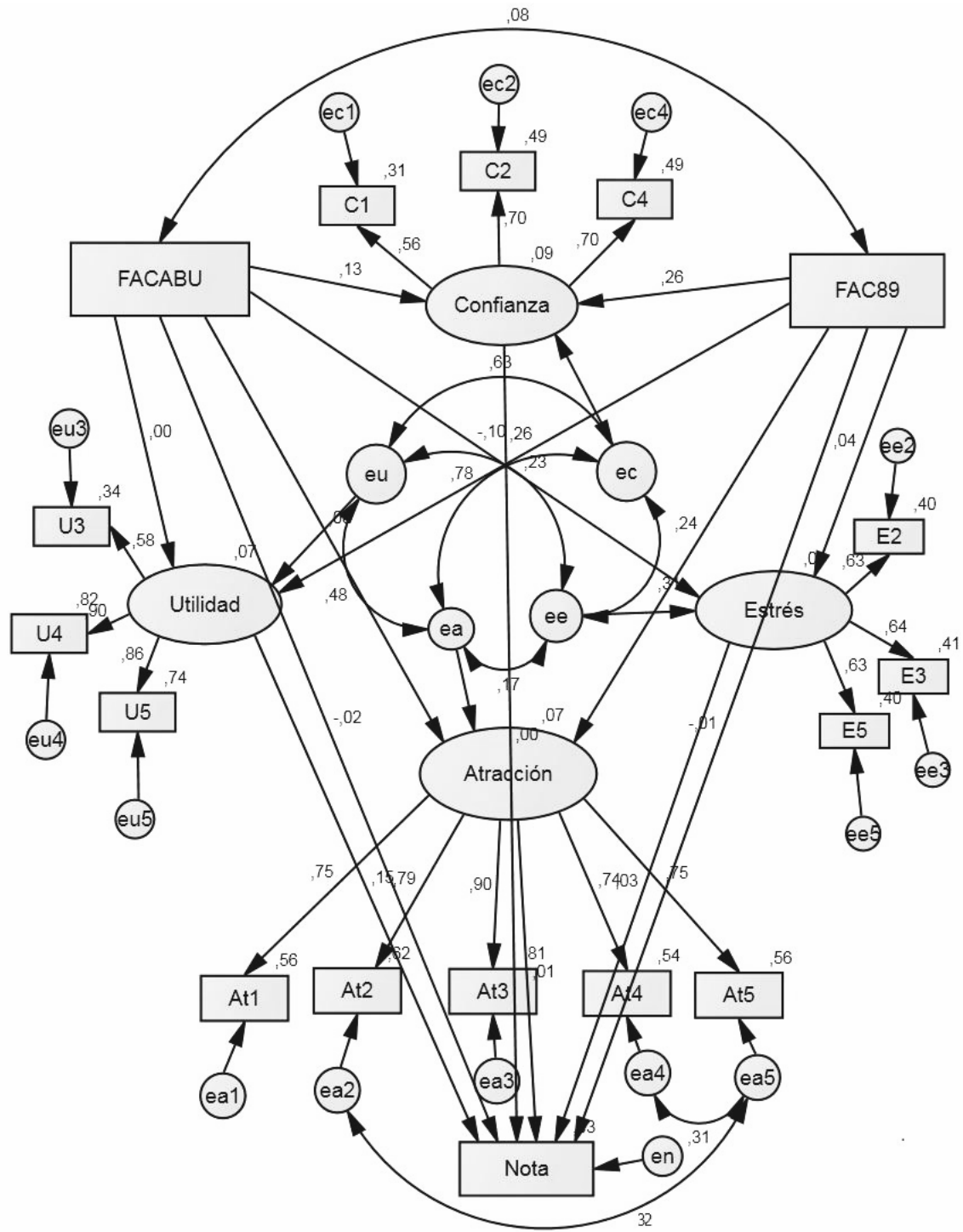
		Estimate
Atracción	<--- Utilidad	,512
Estrés	<--- Utilidad	,203
Estrés	<--- Atracción	,064
Confianza	<--- Utilidad	,355
Confianza	<--- Atracción	,667
C1	<--- Confianza	,484
C2	<--- Confianza	,653
C4	<--- Confianza	,690
U5	<--- Utilidad	,866
U4	<--- Utilidad	,899
U3	<--- Utilidad	,579
E2	<--- Estrés	,633
E3	<--- Estrés	,642
E5	<--- Estrés	,630
At5	<--- Atracción	,749
At4	<--- Atracción	,734
At3	<--- Atracción	,899
At2	<--- Atracción	,789
At1	<--- Atracción	,747
Nota	<--- Confianza	-,020
Nota	<--- Atracción	,012
Nota	<--- Estrés	,035
Nota	<--- Utilidad	,157

5.4.1 Modelo estructural alternativo

Observamos que, cambiando el sentido de algunas de las supuestas causalidades, en algunos casos los valores obtenidos por los parámetros expuestos eran muy similares, aunque en otros diferían sustancialmente. Concretamente, pese a haber visto relaciones causales entre las percepciones de Confianza y Atracción en ejercicios similares, comprobamos que los coeficientes de ajuste en nuestro caso eran prácticamente los mismos cambiando causa por efecto, por lo que decidimos mantener la correlación entre todos los constructos sin afirmar que uno fuese causa de otro.

Así que probamos este otro modelo en el que, sin establecer causalidad, correlacionamos libremente todos los constructos tal y como recomiendan Anderson y Gerbin (1988), a través de los errores de covarianza, generando un modelo en el que lo que obtendremos será la influencia de las variables de control sobre las latentes y de todas ellas sobre la dependiente que clusteriza a los alumnos por sus conocimientos, medidos a través del test que origina la variable Nota.

Los resultados obtenidos del modelo representado por el grafo 7 pueden observarse en la tabla 24 y confirman su calidad a través de unos indicadores que, para la relación Chi cuadrado sobre los grados de libertad dan un cociente de 1,46, con un CFI de 0,982 y unos residuos entre 0,021 y 0,046.



Grafo 7. Modelo correlacional con los 396 alumnos de los dos cursos (EP)

Tabla 24. Resultados optimizados del modelo correlacional con alumnos ambos cursos

Result (Default model)

Minimum was achieved
 Chi-square = 144,908
 Degrees of freedom = 99
 Probability level = ,002

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,945	,924	,982	,975	,982
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,034	,021	,046	,989
Independence model	,216	,208	,223	,000

Covariances: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
FACABU	<-->	FAC89	,083	,050	1,645	,100	par_21
ee	<-->	eu	,111	,033	3,348	***	par_22
eu	<-->	ea	,229	,032	7,122	***	par_23
ec	<-->	eu	,236	,033	7,054	***	par_24
ec	<-->	ea	,301	,040	7,608	***	par_25
ec	<-->	ee	,118	,032	3,708	***	par_26
ee	<-->	ea	,082	,033	2,478	,013	par_27
ea5	<-->	ea2	,128	,025	5,202	***	par_32
ea5	<-->	ea4	,145	,027	5,386	***	par_33

Correlations: (Group number 1 - Default model)

			Estimate
FACABU	<-->	FAC89	,083
ee	<-->	eu	,232
eu	<-->	ea	,479
ec	<-->	eu	,631
ec	<-->	ea	,783
ec	<-->	ee	,309
ee	<-->	ea	,167
ea5	<-->	ea2	,319
ea5	<-->	ea4	,312

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
Utilidad	<---	FACABU	,002	,037	,054	,957	par_11
Atracción	<---	FACABU	,059	,038	1,554	,120	par_13
Estrés	<---	FACABU	-,071	,044	-1,639	,101	par_14
Confianza	<---	FACABU	,076	,034	2,216	,027	par_15
Confianza	<---	FAC89	,150	,036	4,214	***	par_16
Utilidad	<---	FAC89	,187	,037	5,016	***	par_17
Atracción	<---	FAC89	,176	,038	4,575	***	par_18
Estrés	<---	FAC89	,025	,043	,588	,557	par_19
C1	<---	Confianza	1,000				
C2	<---	Confianza	1,073	,112	9,593	***	par_1
C4	<---	Confianza	1,077	,112	9,584	***	par_2
U5	<---	Utilidad	1,000				
U4	<---	Utilidad	1,052	,056	18,954	***	par_3
U3	<---	Utilidad	,823	,068	12,042	***	par_4
E2	<---	Estrés	1,000				
E3	<---	Estrés	,996	,131	7,623	***	par_5
E5	<---	Estrés	,936	,123	7,622	***	par_6
At5	<---	Atracción	1,000				
At4	<---	Atracción	1,078	,062	17,465	***	par_7
At3	<---	Atracción	1,187	,068	17,530	***	par_8
At2	<---	Atracción	1,106	,058	18,974	***	par_9
At1	<---	Atracción	1,029	,070	14,679	***	par_10
Nota	<---	FACABU	-,039	,118	-,328	,743	par_12
Nota	<---	FAC89	-,021	,117	-,177	,859	par_20
Nota	<---	Atracción	,017	,376	,044	,965	par_28
Nota	<---	Estrés	,107	,216	,493	,622	par_29
Nota	<---	Confianza	-,017	,642	-,026	,979	par_30
Nota	<---	Utilidad	,475	,261	1,824	,068	par_31

Standardized Regression Weights: (Group number 1 - Default model)

			Estimate
Utilidad	<---	FACABU	,003
Atracción	<---	FACABU	,081
Estrés	<---	FACABU	-,102
Confianza	<---	FACABU	,131
Confianza	<---	FAC89	,260
Utilidad	<---	FAC89	,264
Atracción	<---	FAC89	,242
Estrés	<---	FAC89	,036
C1	<---	Confianza	,557
C2	<---	Confianza	,698
C4	<---	Confianza	,696
U5	<---	Utilidad	,861
U4	<---	Utilidad	,904
U3	<---	Utilidad	,580
E2	<---	Estrés	,634
E3	<---	Estrés	,640
E5	<---	Estrés	,631
At5	<---	Atracción	,749
At4	<---	Atracción	,735
At3	<---	Atracción	,900
At2	<---	Atracción	,789
At1	<---	Atracción	,746
Nota	<---	FACABU	-,017
Nota	<---	FAC89	-,009
Nota	<---	Atracción	,005
Nota	<---	Estrés	,034
Nota	<---	Confianza	-,004
Nota	<---	Utilidad	,152

Standardized Total Effects (Group number 1 - Default model)

	FAC89	FACABU	Atracción	Estrés	Utilidad	Confianza
Atracción	,242	,081	,000	,000	,000	,000
Estrés	,036	-,102	,000	,000	,000	,000
Utilidad	,264	,003	,000	,000	,000	,000
Confianza	,260	,131	,000	,000	,000	,000
Nota	,032	-,021	,005	,034	,152	-,004
At1	,180	,060	,746	,000	,000	,000
At2	,191	,064	,789	,000	,000	,000
At3	,218	,073	,900	,000	,000	,000
At4	,178	,059	,735	,000	,000	,000
At5	,181	,060	,749	,000	,000	,000
E5	,023	-,064	,000	,631	,000	,000
E3	,023	-,065	,000	,640	,000	,000
E2	,023	-,064	,000	,634	,000	,000
U3	,153	,002	,000	,000	,580	,000
U4	,238	,003	,000	,000	,904	,000
U5	,227	,002	,000	,000	,861	,000
C4	,181	,091	,000	,000	,000	,696
C2	,181	,092	,000	,000	,000	,698
C1	,145	,073	,000	,000	,000	,557

Fuente: AMOS (EP)

Encontramos valores de ajuste del modelo muy próximos, incluyendo o no causalidad, pero aunque algunos resultados sugieren postulados distintos hay total convergencia en afirmar extremos tales como:

Nuevamente, tenemos un modelo con una bondad de ajuste (calidad) excelente, con el mismo orden de magnitud de los indicadores como los obtenidos en el de relaciones causales. En este caso son CFI con valor 0,982, residuos entre 0,021 y 0,046 y una relación $\text{Chi}^2 / \text{grados de libertad}$ de 1,46.

Hemos resaltado en rojo las relaciones significativas (<3%) entre:

- FACABU y Confianza,
- entre FAC89 y Confianza
- entre FAC89 y Utilidad,
- entre FAC89 y Atracción, y entre los constructos y las variables que los definen.

En menor medida (<7%) entre

- entre Utilidad y Nota.

Cuando observamos el peso de los efectos totales considerados, nos damos cuenta que:

- FAC89 es importante sobre Confianza (0,26), sobre Utilidad (0,264) y sobre Atracción (0,242)

La covarianza entre FACABU y FAC89 es igual de escasa y poco significativa (10%) como en el modelo anterior, aunque si hay significatividad en las covarianzas entre los constructos. Sobre todo hay una gran correlación entre Confianza y Atracción (0,783) y entre Confianza y Utilidad (0,631). También es fuerte entre Atracción y Utilidad (0,479).

Continuamos interpretando que los alumnos que más se preocupan por proteger su privacidad (FAC89) son los que consideran más útiles (Utilidad) los sistemas de protección en su navegación, se sienten más atraídos (Atracción) por su implementación y se sienten más confiados.

Seguimos concluyendo que ni hay significatividad ni los parámetros tienen relevancia en lo que cada constructo se correlaciona con la Nota. Tan solo hay que tener en cuenta, parcialmente, que los conocimientos se incrementan con los que consideran la Utilidad como una ventaja.

Tampoco hay una influencia significativa con Nota por parte de los alumnos que son más o menos cuidadosos con la protección de su privacidad o de sus datos (FAC89 y FACABU). Lo que nos vuelve a decir que el comportamiento de los alumnos en su vida diaria indica el nulo grado de asimilación de su aprendizaje. Parece que estudian solo para aprobar, sin estímulo por aprender, no incorporando en su vida las enseñanzas que supuestamente han recibido pero no interiorizado. En definitiva, al menos sobre estos aspectos, los resultados nos demuestran que no han sido capaces de transformar la información, aunque la hayan recibido por distintos medios, en conocimiento. No se sienten suficientemente atraídos por el contenido de las asignaturas.

Algo parecido sucede con el nivel de protección de sus datos generando procedimientos de backup. Ninguna correlación válidamente significativa ($>10\%$) con cualquiera de los constructos, excepto con Confianza. Parece que les da igual, que no les importa. Tan solo con Confianza, y de escaso efecto (0,131) de forma que a mayor preocupación por salvaguardar sus datos más tranquilidad.

5.4.2 Modelo estructural “multiobservado”

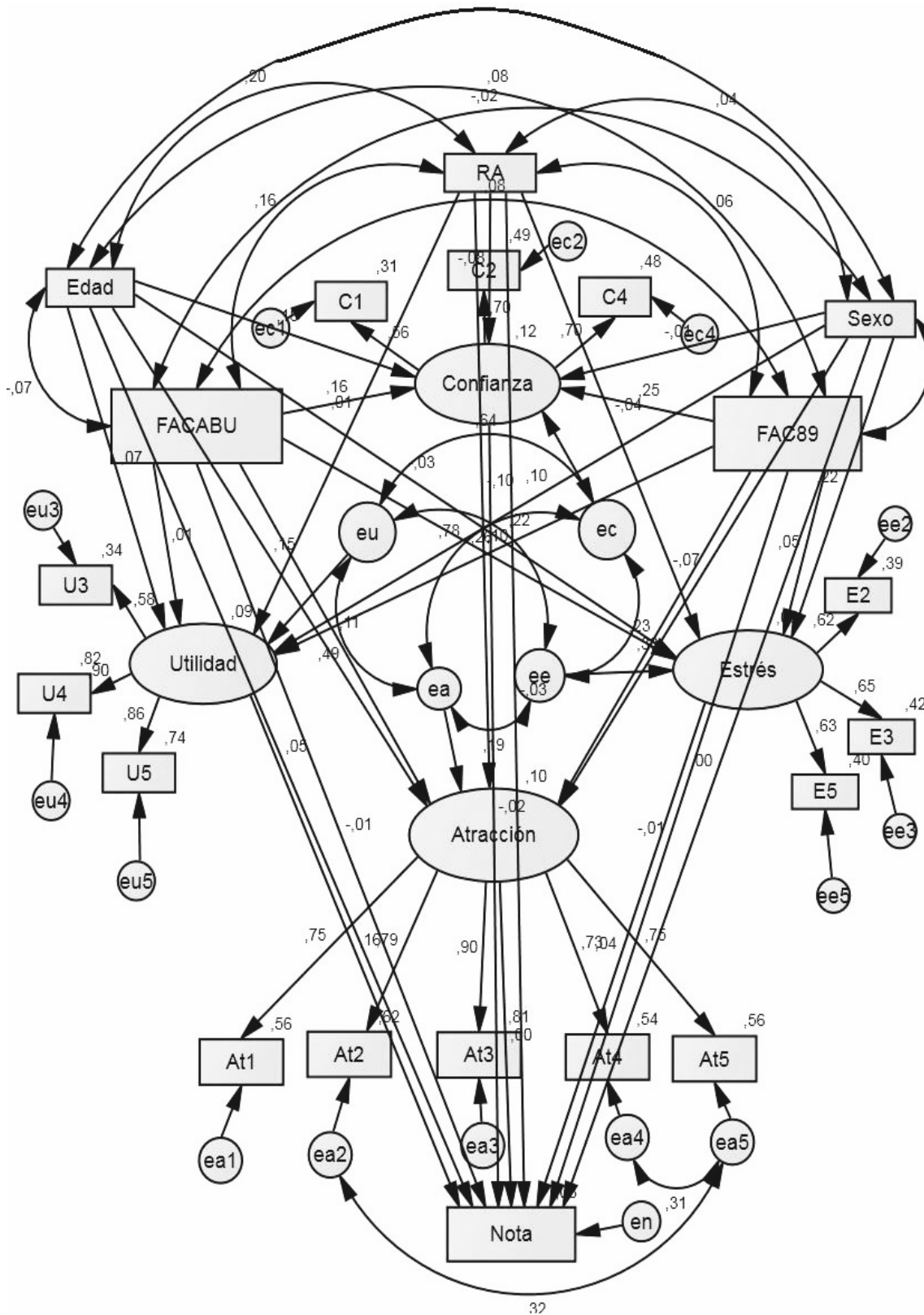
Excediendo el objetivo de la investigación, pero teniendo en cuenta el compromiso recogido en el apartado 3.4 sobre “Hipótesis” cuando decíamos que los propios resultados nos podrían llevar a plantear nuevas hipótesis, vamos a incluir un rápido estudio adicional sobre este último modelo estructural.

Nos servirá para comprobar y demostrar su ajuste, así como la facilidad de obtener respuestas a las múltiples preguntas que, bajo diferentes visiones, deseemos formularnos sobre este caso.

También nos servirá para justificar una de las características que describíamos sobre la utilización de ecuaciones estructurales en el apartado 4.5 de la presente tesis cuando afirmábamos que permitían analizar datos de distintas poblaciones simultáneamente, lo que diferencia esta metodología de otras técnicas de análisis multivariante al estudiar relaciones para cada subconjunto de poblaciones integradas en la muestra, dando una visión global del fenómeno en cuestión.

El nuevo grafo (7bis) nos muestra el mismo modelo presentado en el grafo 7 en el que correlacionábamos las variables latentes vistas bajo la influencia de dos variables de control y con una variable dependiente, pero añadiendo ahora otras tres variables de control (sexo, edad y rendimiento académico) simultáneas a las anteriores.

Nos queda lo siguiente:



Grafo 7bis. Modelo correlacional con cinco variables de control para los dos cursos - EP

Obtenemos un χ^2 de 174,2 y 129 grados de libertad (ratio: 1,35)

Tabla 25. Resultados del modelo con 5 variables de control para ambos cursos

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
Utilidad	<---	FACABU	,006	,037	,149	,882	par_10
Atracción	<---	FACABU	,078	,038	2,055	,040	par_12
Atracción	<---	FAC89	,168	,038	4,426	***	par_13
Estrés	<---	FAC89	,032	,042	,760	,447	par_14
Confianza	<---	FAC89	,143	,035	4,066	***	par_22
Confianza	<---	FACABU	,090	,034	2,623	,009	par_23
Estrés	<---	FACABU	-,066	,043	-1,536	,124	par_24
Utilidad	<---	FAC89	,184	,037	4,964	***	par_30
Confianza	<---	Edad	,022	,007	2,926	,003	par_40
Estrés	<---	Edad	-,004	,009	-,425	,671	par_41
Atracción	<---	Edad	,024	,008	2,911	,004	par_42
Utilidad	<---	Edad	,011	,008	1,371	,170	par_44
Confianza	<---	RA	-,064	,045	-1,412	,158	par_45
Estrés	<---	RA	-,032	,057	-,566	,572	par_46
Atracción	<---	RA	-,098	,051	-1,934	,053	par_47
Utilidad	<---	RA	,011	,050	,220	,826	par_48
Confianza	<---	Sexo	-,026	,099	-,258	,796	par_50
Estrés	<---	Sexo	,449	,130	3,456	***	par_51
Utilidad	<---	Sexo	,220	,110	2,011	,044	par_53
Atracción	<---	Sexo	-,154	,111	-1,388	,165	par_54
C1	<---	Confianza	1,000				
C2	<---	Confianza	1,077	,112	9,621	***	par_1
C4	<---	Confianza	1,076	,112	9,587	***	par_2
U5	<---	Utilidad	1,000				
U4	<---	Utilidad	1,056	,055	19,107	***	par_3
U3	<---	Utilidad	,825	,068	12,062	***	par_4
E2	<---	Estrés	1,000				
E3	<---	Estrés	1,028	,132	7,781	***	par_5
E5	<---	Estrés	,959	,123	7,769	***	par_6
At5	<---	Atracción	1,000				
At4	<---	Atracción	1,076	,062	17,457	***	par_7
At3	<---	Atracción	1,190	,068	17,598	***	par_8
At1	<---	Atracción	1,029	,070	14,691	***	par_9
Nota	<---	FACABU	-,014	,122	-,118	,906	par_11
Nota	<---	Atracción	,008	,375	,021	,983	par_15
Nota	<---	Estrés	,121	,229	,528	,597	par_16
Nota	<---	Confianza	-,062	,652	-,095	,924	par_17
Nota	<---	Utilidad	,491	,266	1,843	,065	par_18
Nota	<---	FAC89	-,021	,117	-,181	,856	par_31
At2	<---	Atracción	1,105	,058	18,975	***	par_33
Nota	<---	Edad	,023	,025	,916	,360	par_43
Nota	<---	RA	-,096	,152	-,633	,527	par_49
Nota	<---	Sexo	,015	,354	,044	,965	par_52

Standardized Regression Weights: (Group number 1 - Default model)

			Estimate
Utilidad	<---	FACABU	,008
Atracción	<---	FACABU	,107
Atracción	<---	FAC89	,231
Estrés	<---	FAC89	,046
Confianza	<---	FAC89	,248
Confianza	<---	FACABU	,157
Estrés	<---	FACABU	-,095
Utilidad	<---	FAC89	,260
Confianza	<---	Edad	,178
Estrés	<---	Edad	-,026
Atracción	<---	Edad	,153
Utilidad	<---	Edad	,073
Confianza	<---	RA	-,085
Estrés	<---	RA	-,035
Atracción	<---	RA	-,102
Utilidad	<---	RA	,012
Confianza	<---	Sexo	-,015
Estrés	<---	Sexo	,216
Utilidad	<---	Sexo	,104
Atracción	<---	Sexo	-,071
C1	<---	Confianza	,557
C2	<---	Confianza	,700
C4	<---	Confianza	,695
U5	<---	Utilidad	,860
U4	<---	Utilidad	,905
U3	<---	Utilidad	,581
E2	<---	Estrés	,623
E3	<---	Estrés	,648
E5	<---	Estrés	,634
At5	<---	Atracción	,749
At4	<---	Atracción	,734
At3	<---	Atracción	,901
At1	<---	Atracción	,745
Nota	<---	FACABU	-,006
Nota	<---	Atracción	,003
Nota	<---	Estrés	,038
Nota	<---	Confianza	-,016
Nota	<---	Utilidad	,156
Nota	<---	FAC89	-,010
At2	<---	Atracción	,788
Nota	<---	Edad	,049
Nota	<---	RA	-,033
Nota	<---	Sexo	,002

Covariances: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
FACABU	<-->	FAC89	,083	,050	1,645	,100	par_21
FACABU	<-->	Edad	-,316	,235	-1,342	,180	par_34
FACABU	<-->	RA	,121	,039	3,118	,002	par_35
FAC89	<-->	Sexo	-,010	,017	-,618	,536	par_36
FAC89	<-->	RA	,047	,038	1,240	,215	par_37
FAC89	<-->	Edad	,381	,236	1,617	,106	par_38
FACABU	<-->	Sexo	-,005	,017	-,324	,746	par_39
RA	<-->	Sexo	,010	,013	,782	,434	par_55
Edad	<-->	Sexo	-,034	,078	-,440	,660	par_56
Edad	<-->	RA	,727	,183	3,976	***	par_57
ee	<-->	ea	,089	,032	2,795	,005	par_25
eu	<-->	ea	,228	,032	7,233	***	par_26
ec	<-->	eu	,231	,033	7,069	***	par_27
ee	<-->	eu	,098	,031	3,135	,002	par_28
ec	<-->	ea	,288	,038	7,565	***	par_29
ec	<-->	ee	,118	,031	3,853	***	par_32
ea5	<-->	ea2	,128	,025	5,222	***	par_19
ea5	<-->	ea4	,145	,027	5,407	***	par_20

Correlations: (Group number 1 - Default model)

			Estimate
FACABU	<-->	FAC89	,083
FACABU	<-->	Edad	-,068
FACABU	<-->	RA	,159
FAC89	<-->	Sexo	-,031
FAC89	<-->	RA	,062
FAC89	<-->	Edad	,082
FACABU	<-->	Sexo	-,016
RA	<-->	Sexo	,039
Edad	<-->	Sexo	-,022
Edad	<-->	RA	,204
ee	<-->	ea	,193
eu	<-->	ea	,491
ec	<-->	eu	,637
ee	<-->	eu	,218
ec	<-->	ea	,778
ec	<-->	ee	,329
ea5	<-->	ea2	,319
ea5	<-->	ea4	,312

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,936	,906	,983	,974	,982
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,030	,017	,041	,999
Independence model	,184	,178	,190	,000

Standardized Total Effects (Group number 1 - Default model)

	Sexo	RA	Edad	FAC89	FACABU	Atracción	Estrés	Utilidad	Confianza
Atracción	-,071	-,102	,153	,231	,107	,000	,000	,000	,000
Estrés	,216	-,035	-,026	,046	-,095	,000	,000	,000	,000
Utilidad	,104	,012	,073	,260	,008	,000	,000	,000	,000
Confianza	-,015	-,085	,178	,248	,157	,000	,000	,000	,000
Nota	,027	-,032	,057	,029	-,011	,003	,038	,156	-,016
At1	-,053	-,076	,114	,172	,080	,745	,000	,000	,000
At2	-,056	-,081	,121	,182	,084	,788	,000	,000	,000
At3	-,064	-,092	,138	,208	,096	,901	,000	,000	,000
At4	-,052	-,075	,113	,169	,078	,734	,000	,000	,000
At5	-,053	-,077	,115	,173	,080	,749	,000	,000	,000
E5	,137	-,022	-,017	,029	-,060	,000	,634	,000	,000
E3	,140	-,023	-,017	,030	-,062	,000	,648	,000	,000
E2	,135	-,022	-,016	,029	-,059	,000	,623	,000	,000
U3	,060	,007	,042	,151	,005	,000	,000	,581	,000
U4	,094	,011	,066	,236	,007	,000	,000	,905	,000
U5	,089	,010	,062	,224	,007	,000	,000	,860	,000
C4	-,010	-,059	,124	,172	,109	,000	,000	,000	,695
C2	-,010	-,059	,124	,173	,110	,000	,000	,000	,700
C1	-,008	-,047	,099	,138	,088	,000	,000	,000	,557

Fuente: AMOS (EP)

Con unos indicadores de bondad de ajuste similares al caso anterior (CFI = 0,982, y con mejores residuos) obtenemos una información similar en cuanto a niveles de correlación entre las variables definidas. Pero, adicionalmente, vemos las diferencias existentes en nuestro modelo bajo la observación de la variable edad de los estudiantes, su sexo y su rendimiento académico (si van a curso por año, o llevan más o menos asignaturas pendientes de cursos anteriores).

Existe covarianza significativa entre el rendimiento en los estudios y la edad, con una correlación de 0,204. Normalmente alumnos más jóvenes son de primeros cursos o están yendo a curso por año y los de más edad son repetidores o personas que van cursando asignaturas más que cursos.

La edad también es significativa con las latentes de *Confianza* y *Atracción* (a mayor “experiencia” más seguridad en lo que hacen y por qué lo hacen)

El rendimiento académico es significativo, pero en sentido contrario, con la *Atracción* (contra peor van menos se sienten atraídos)

Las chicas se sienten más estresadas que los chicos en la adopción de medidas de seguridad. Hay alta significatividad (<1%) con una influencia de 0,216. Analizar las razones exige un estudio más profundo.

Y así sucesivamente. De esta manera puede abordarse el estudio de los diferentes subconjuntos de población que decidamos investigar.

6.- CONCLUSIONES

6.1 Limitaciones

Pese a tratarse de las conclusiones de los análisis realizados con una muestra muy numerosa y representativa de estudiantes de las Ingenierías más afines al tema que nos ocupa, no podemos obviar que se trata de una muestra no probabilística, de conveniencia, con la que hemos trabajado.

Extrapolar esos resultados a la totalidad de la población, no ya de la propia Universitat Politècnica de València, sino siquiera al conjunto de las Escuelas de Ingeniería de Informática y Telecomunicación no sería válido, en pura semántica Estadística. No obstante, como estudio de caso, nos proporciona suficiente información fiable como para intuir que algo está pasando con los planes de enseñanza que no consiguen su asimilación y aprendizaje por parte del público objetivo que constituye, en definitiva, la población de nuestro universo.

Lo demás no es cuestionable. Los “factores / variables latentes / constructos” que otros autores utilizan en el estudio de “afecciones / aprendizajes / motivaciones / reacciones” han sido validados por las herramientas estadísticas que justifican su validez y fiabilidad.

Hemos seguido al pie de la letra todas las recomendaciones pertinentes que indican los expertos en la cuestión a la hora de tomar determinadas decisiones, como considerar o rechazar determinadas variables.

Hemos medido lo que queríamos medir y utilizado los ítems que lo miden, con herramientas adecuadas, potentes y reconocidas.

Hemos comprobado, en una y otra dirección, las relaciones, correlaciones, factorización, regresiones, etc. de unas variables sobre otras.

Hemos convergido en el orden de magnitud de ciertos resultados parciales obtenidos por otros investigadores en estudios diferentes.

Y, finalmente, hemos sido cautos a la hora de afirmar lo que los datos nos dicen pues, precisamente por eso, son los datos obtenidos los que nos lo afirman.

Estas etapas confirman que se han cubierto las especificaciones formuladas por Asimov (2010) en el punto 2.1.1 respecto el método de investigación científica que se representa en el siguiente cuadro:

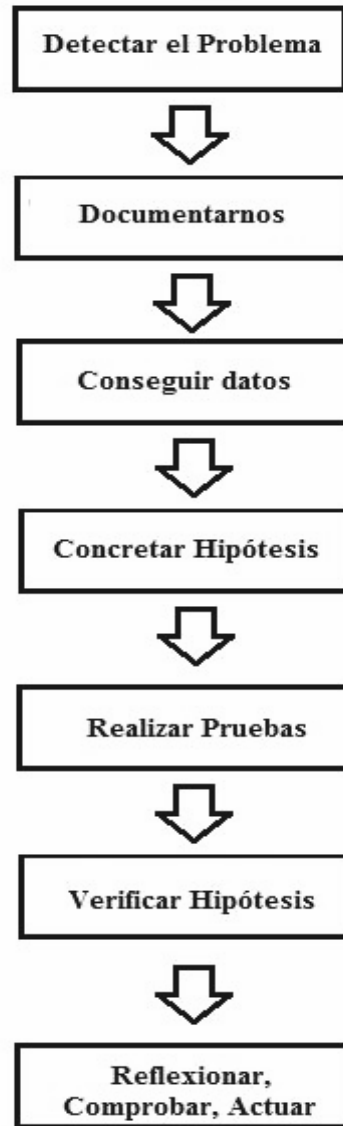


Fig .37: Ejecución de la investigación (EP)

Obtenemos una información que es más que suficiente para nuestro objetivo y no es necesario, en el ámbito de esta tesis, incidir más en diagnosticar causalidades (Martínez, J.A. y Martínez, L., 2009). Podíamos superar, poco pero algo, los parámetros de bondad de ajuste con otras alternativas de los modelos estructurales pero estaríamos optimizando el modelo de nuestros datos, no el teórico.

6.2 Discusión de los resultados

Con respecto a los parámetros estadísticos básicos, donde analizamos los parámetros de factorización (KMO, % de varianza explicada, significatividad, y Alfa de Cronbach) de los dos cursos por separado, observamos que tienen órdenes de magnitud similares y, tanto individualmente como en conjunto, son suficientemente satisfactorios.

El resumen contenido en las tablas 13 a 17, incluidas en el capítulo de Resultados, demuestra una consistencia que no deja lugar a dudas sobre la imprudencia, temeridad o falta de conciencia o conocimientos prácticos sobre los riesgos que asumen nuestros alumnos tanto con respecto al cuidado de sus soportes informáticos, a nivel de la permisividad de acceso a sus recursos, como cuando navegan por internet en general o interactúan con las redes sociales en particular.

Llaman preocupantemente la atención los siguientes valores:

- Tan solo algo más del 4% de los encuestados utilizan contraseñas complejas, diferentes para cada acceso y renovadas con frecuencia.
- Alrededor del 40% tienen una password única para todos los accesos, el 70% las mantiene fijas en el tiempo y una cuarta parte deja que las genere el propio sistema
- Una tercera parte no protege el acceso a su propio PC
- Una séptima parte de encuestados nunca ha hecho una copia de seguridad de sus datos y tan solo otra séptima parte tiene un sistema automático de actualización
- Algo más del 25% abren mails de desconocidos, y una sexta parte no tienen inquietud por conocer las vulnerabilidades que se producen
- Con respecto a las redes sociales, más del 60% se dan de alta sin leerse las condiciones de registro y casi la mitad (entre el 40 y el 45%) manifiestan libremente sus opiniones personales sobre temas sensibles

Todos estos resultados, ya patentes en la primera encuesta en el curso 2011-2012, justificaron la conveniencia de investigar a los alumnos del curso siguiente que, lamentablemente, confirmaron nuestros temores.

Resultados que indican por si solos la necesidad de preguntarnos sobre lo que estamos haciendo a nivel de planes de estudio y exigencias curriculares, pues promociones con esas actitudes tendrán muy difícil el desempeño de una actividad profesional productiva, de confianza y competitiva.

Al comparar nuestros resultados con los de investigaciones referenciadas, encontramos las siguientes coincidencias:

- En el estudio titulado “Youth, Privacy and Reputation”, de Marwick, Murgia y Palfrey (2010) se informa que un 47% de jóvenes incluyen información privada (actividad sexual, consumo de alcohol y droga) a través de las redes sociales y que un 64% de esa población mantiene la configuración que, por defecto, proporciona la plataforma al registrarse. En nuestra investigación los porcentajes obtenidos para esos mismos comportamientos son del 41 al 45% en el primer caso y entre el 61-62% en el segundo.
- En la investigación llevada a cabo por Hoofnagle y otros (2010) en la Universidad de Berkeley utilizan un parámetro para conocer el porcentaje de usuarios que protegen su privacidad consistente en saber si se preocupan por la eliminación periódica de las cookies que se almacenan en el PC tras navegar por internet, tal y como también hacemos nosotros (variable A8). En su caso llegan a la conclusión de que el 38% no se preocupan o ignoran esa posibilidad, frente al resultado obtenido en nuestro caso que fue del 38,6% del total de alumnos de los dos cursos (Anexo E). El 37,3% del curso 2011-12, y el 40,1% en el 2012-13.
- En el caso de “Los efectos de la motivación, la confianza y la preocupación por la privacidad en las redes sociales”, de Shi-Woei Lin y Yu-Cheng Liu (2012), vimos que también hicieron dos pilotos con treinta encuestados y finalmente la encuesta definitiva con 207 personas; es decir, muestras de tamaños similares a la nuestra. Utilizaron las mismas herramientas estadísticas básicas que nosotros (correlaciones, índices de fiabilidad, regresión, constructos, etc.), haciendo referencias a razones extrínsecas e intrínsecas (interés, estrés) para estudiar los riesgos de privacidad en redes sociales y teniendo en cuenta la confianza y sus motivaciones.

Es decir, comprobamos que prácticamente nuestros antípodas tienen unas inquietudes similares a las nuestras, se han dado cuenta también del riesgo, las están trabajando y utilizan teoría similar de apoyo a la que usamos nosotros. Aún teniendo en cuenta la distancia en todos los órdenes (física, cultural, perfil de encuestados por edad y por selección...), llegamos a converger en aspectos tales como la intensa correlación entre la frecuencia de navegación por las redes sociales y la revelación de información (0,499 en su caso versus 0,441 en el nuestro, en ambos casos con significatividad⁴⁴ <1%).

También coincidimos en la afirmación vertida por la investigación de Shi-Woei Lin (2012) cuando dice: “*nuestros resultados indican que la confianza puede efectivamente mitigar la preocupación de un usuario por su privacidad*” pues encontramos una correlación suficiente entre los parámetros con los que nosotros definimos ambos conceptos (0,26, con significatividad <1%).

- Los trabajos de Jiang, Z. *et al* (2013) sobre privacidad en redes sociales indican que en USA entre el 43 y el 51% de los encuestados dan información personal (domicilio, correo electrónico, fotos, vídeos, opiniones, creaciones, etc.). Nosotros encontramos esa misma actuación en el 45% de nuestros alumnos.

Al introducir los modelos estructurales también consignados en el capítulo de Resultados, hemos hecho un recorrido desde el modelo inicial propuesto, basado en la teoría existente en el que representábamos el grafo con cuatro variables latentes, llegando a otro modelo más simple, con solo tres constructos, fruto del análisis factorial exploratorio de nuestros datos con los alumnos encuestados en el primer curso, analizando su comportamiento bajo la observación de diferentes variables de control (tabla 11) para llegar a definir las más características, **protección y privacidad**, con las que hemos ajustado los modelos. Con los alumnos del siguiente curso, y con el conjunto de ambos cursos, ya surgía la cuarta variable latente que nos había indicado la teoría.

Siempre hemos obtenido unos buenos indicadores de calidad de ajuste que ambiciosamente hemos mejorado a veces haciendo uso de las recomendaciones del propio programa haciendo covariar determinadas variables, sin ser necesario.

⁴⁴ La significatividad mide el grado de error

Desde un principio observamos que la variable latente *Utilidad* se convertía en impulsora de la motivación principal que se detectaba en el análisis, siendo básica para incrementar la *Atracción* y la *Confianza* de los alumnos hacia los conceptos de seguridad. Ella misma aparecía bastante influenciada por los estudiantes más proclives a preservar su privacidad, lo que implica que los alumnos que son más cuidadosos con esa característica de salvaguarda de su seguridad son los que consideran más útil la adopción de medidas al respecto.

En definitiva, cuando un alumno entiende algo como útil, o práctico, se siente fuertemente atraído por ello y le genera confianza. Y a mayor atracción, mucha mayor confianza por lo que ahí es donde hay que acentuar la formación, con información y ejemplos sobre seguridad que les resulten motivadores y sobre los que se haga hincapié de forma transversal en la mayoría de las asignaturas, no sólo en las específicas que traten los temas de forma general, asumiendo unos conocimientos y unas actitudes que parece que no han asimilado.

También vimos repetidamente en cada modelo, con independencia del grado de ajuste, que la variable dependiente *Nota* no se correlacionaba con ninguna de las variables latentes ni con las de control, ni en significación ni en valor. Es decir, en cada curso los mejores estudiantes no se diferencian de los no tan buenos a la hora de haberse concienciado de la necesidad de proteger su propia información e imagen pública, y actuar en consecuencia. Continúa faltando información adecuada a todos los niveles pues ni siquiera los mejores actúan con suficiente seguridad.

Al analizar la muestra con la totalidad de alumnos de los dos cursos ya hemos comentado que obtuvimos el cuarto constructo que nos señala la teoría estudiada, consiguiendo los mejores índices de ajuste de nuestra investigación, con CFIs de 0,98, y donde se manifestaba claramente la influencia de *Utilidad* sobre *Atracción*, *Confianza* y *Estrés*

Seguimos estudiando los modelos a los que habíamos ido llegando en esta última fase observando que, en algunos de los casos, obteníamos ajustes con unos valores análogos con independencia del sentido que diésemos a las flechas que indican causalidad, por lo que decidimos ser conservadores y comparar las diversas influencias en uno y otro caso;

es decir, con causalidad y sin ella, correlacionando las latentes y proponiendo un modelo alternativo.

La bondad de ajuste de ambos modelos no es fácilmente mejorable, tal como podemos comprobar en la tabla 26:

Tabla 26. Comparación parámetros de ajuste modelo final y alternativo (EP)

Modelos	χ^2	° libertad	$\chi^2 / \text{° libertad}$	CFI	RMSEA
Completo (causal)	150,2	100	1,5	0,980	0,023 – 0,047
Optimizado (causal)	133,8	99	1,35	0,986	0,015 – 0,042
Alternativo (no causal)	144,9	99	1,46	0,982	0,021 – 0,046

En ambos modelos converge el que los alumnos que más se preocupan por proteger su privacidad (*FAC89*) son los que consideran más útiles (*Utilidad*) los sistemas de protección en su navegación y se sienten más atraídos (*Atracción*) por su implementación. También ambos modelos coinciden en decirnos que los alumnos que más se preocupan por su autoprotección (*FACABU*) son los que tienen más *Confianza* en los sistemas implementados.

La covarianza entre *FACABU* y *FAC89* es escasa y poco significativa (10%) tanto en el modelo causal como en el correlacionado aunque, en este último, si hay significatividad en las covarianzas entre los constructos. Sobre todo hay una gran correlación entre *Confianza* y *Atracción*, entre *Confianza* y *Utilidad* y entre *Atracción* y *Utilidad*.

Se mantiene, en todos los casos, la afirmación anterior sobre la variable dependiente *Nota*, que aunque se haya visto en todos los casos, no deja de ser una triste sorpresa.

Debemos hacer comprender a nuestros alumnos la ventaja de entender la utilidad de la navegación segura y conseguiremos incrementar su atracción hacia ese tipo de medidas así como su confianza y seguridad.

Todas estas conclusiones quedan reflejadas en la tabla siguiente en la que se reproducen las hipótesis iniciales con las que partía nuestra investigación y en donde hemos incluido una columna adicional, a la derecha, con el grado de cumplimiento de cada una de ellas. Los “0” reflejan la nula incidencia que tiene el test de conocimientos con los

que pensábamos que se dejaría entrever un comportamiento distinto entre los encuestados mejor o peor preparados. Las cruces indican el nivel de certeza comprobado ante cada afirmación de forma que, en el caso de las tres cruces es máxima, las dos cruces implican un grado satisfactorio y una significa cumplimiento escaso. El signo menos niega la afirmación vertida en la hipótesis correspondiente, con la misma gradación.

Tabla 27. Resultados de las Hipótesis

Hipótesis	descripción	variables observables	Constructos o de control	pregunta encuesta	Grado de acuerdo
He1	Protección accesos	AUP1, AUP2, AUP3, A1, A2, A4, A5	“ (passwords)	5, 6, 7, 11, 12, 59, 60	---
He2	Backups	ABU1, ABU2, ABU3	“ (copias)	8, 9, 10	--
He3	Antivirus, firewall	A6, A7	“ (autoprotección)	61, 62	++
He4	Información vulnerabilidades	A3	“ (inquietud x info)	13	--
He5	Privacidad de actividad	A8, A9 (FACA89)	“ (privacidad)	63, 64	+
H1	Covarianza entre latentes	Atx-Cx-Ex- Ux	Atracción, Confianza, Estrés, Utilidad	39 - 58	+++
H2	Utilidad implica mayor atracción	Ux - Atx	Utilidad, Atracción	39-43, 54-58	+++
H3	Confianza \leftrightarrow privacidad	Cx - A8, A9	Confianza, Privacidad	44-48, 63-64	++
H4	Confianza \leftrightarrow protección	Cx - A6, A7	Confianza, Protección	44-48, 61-62	++
H5	Privacidad \leftrightarrow protección	A6 – A9	Privacidad, Protección	61 - 64	+
H6	A mayor nota más atracción	P1-P11-Atx	Nota, Atracción	17-27, 39-43	0

H7	A mayor nota mayor utilidad	P1-P11-Ux	Nota, Utilidad	17-27, 54-58	0
H8	A mayor nota más privacidad	P1-P11, A8-A9	Nota, Privacidad	17-27, 63-64	0
H9	A mayor nota más protección	P1-P11, A6-A7	Nota, Protección	17-27, 61-62	0
H10	A menor nota más Estrés	P1-P11-Ex	Nota, Estrés	17-27, 49-53	0
H11	A peor nota menos confianza	P1-P11, Cx	Nota, Confianza	17-27, 44-48	0
H12	Buen ajuste de latentes	Atx-Cx-Ux- Ex	Atracción, Confianza, Estrés, Utilidad	39-58	+++
H13	Más privacidad → más ajuste	A8-A9, Atx - Cx-Ux-Ex	Atracción, Confianza, Estrés, Utilidad, Privacidad	39-58, 63-64	+++
H14	Más protección → más ajuste	A8-A9, Atx - Cx-Ux-Ex	Atracción, Confianza, Estrés, Utilidad, Protección	39-58, 61-62	+++
Hg1	Condiciones de registro	AURS3	Estadísticos básicos (registro en RS)	30	---
Hg2	Actividad - Publicación	AURS9, AURS10	“ (info personal en RS)	36, 37	---
Hg3	Publicación información sensible	AURS11	“ (info “muy personal”)	38	---

Fuente: EP

6.3 Resumen de aportaciones

La popularización del uso de la informática, la navegación por internet y la gran penetración de las redes sociales, no son garantía de su correcto uso, ni siquiera por parte de nuestros alumnos universitarios que se forman en esas tecnologías. Tampoco los de mejores conocimientos han sido capaces de asimilarlos y ponerlos en práctica, diferenciándose de sus compañeros.

El hecho de utilizar esos recursos muy frecuentemente no es razón suficiente para asumir la motivación de un uso seguro. Como si se tratase de otro tipo de aprendizajes, menos incorporados a la vida diaria, no podemos dejar de atraer su atención hacia casos reales, prácticos, con ejemplos y experiencias que fomenten su inquietud con el objetivo de sensibilizarlos adecuadamente.

Repasando sucintamente las fases que nos llevaron a una preocupación creciente por la forma en que nuestros estudiantes navegan y se protegen al acceder a la red recordaremos que todo empezó en una investigación inicial sobre los conocimientos, sensibilidad y actuación de los alumnos de primer curso de la Licenciatura de Comunicación Audiovisual.

A la vista de su escasa sensibilización con los posibles riesgos que entrañan esas prácticas consideré conveniente profundizar más en estos comportamientos, accediendo a los futuros profesionales que serán desarrolladores de herramientas para estas actividades. Así que decidimos comprobar esos mismos comportamientos por parte de alumnos de las Escuelas de Ingeniería Informática y Telecomunicación.

Indagamos sobre la forma en la que se realiza el aprendizaje y se genera conocimiento, partiendo de las premisas motivacionales que los facilitan. Relacionamos las actitudes respecto su comportamiento habitual cuando utilizan las TIC, con sus propias aptitudes. Utilizamos Ecuaciones Estructurales para profundizar en las relaciones entre las variables que definieron los conceptos emocionales, analizando los factores críticos que se dan tanto en su aprendizaje como en su vida laboral y/o social.

Obtuvimos una información, a través de las dos pruebas piloto del cuestionario, que vaticinaba unos resultados que parecían confirmar que nuestra preocupación estaba sustentada por los datos de los análisis que estábamos haciendo, siendo muy similares a los que ya disponíamos de los alumnos de Comunicación Audiovisual. Desafección hacia el uso de contraseñas, escasa garantía en preservar la información mediante copias de seguridad, falta de protección en la navegación inalámbrica en sitios públicos, asunción de compromisos con los proveedores de aplicaciones de Redes Sociales, etc. son características comunes que igualaban el comportamiento de unos y otros estudiantes.

Todos estos comportamientos quedaron refrendados cuando se procesaron y analizaron los datos obtenidos con los alumnos de Informática del curso 2011-2012.

No queríamos aceptar esa situación pensando que podíamos haber cometido algún error en alguna de las fases del proceso, por lo que decidimos extender el estudio con alumnos del curso siguiente.

Los resultados del análisis de los datos obtenidos con los nuevos alumnos, coherentes con los anteriores, confirmaron la necesidad de darnos cuenta de que hay que asegurar la puesta en práctica de la formación recibida revisando los programas docentes para generar un conocimiento que, lamentablemente, no asimilan nuestros alumnos.

Si ya los valores de las tablas de frecuencias indicaban el alto grado de temeridad de la población encuestada a la hora de proteger sus datos, no siendo conscientes del significado de la pérdida de sus trabajos, de sus archivos y, en consecuencia, de la necesidad de adoptar medidas de protección de los mismos, así como para su privacidad y capacidad de navegación segura por internet, salvaguardando su identidad digital y siendo prudentes en el escaparate que se han convertido las redes sociales, el estudio estructural nos demuestra la correlación entre factores motivacionales (Confianza-Utilidad-Estrés-Atracción), donde comprobamos que los estudiantes con más inquietudes sobre su privacidad son los que reconocen como más útiles las herramientas que protegen su navegación y se sienten más atraídos por su puesta en funcionamiento, a la vez que se sienten con más confianza.

Pero lo que es sorprendente y muy preocupante es la nula incidencia del aprovechamiento académico en la adopción de una determinada actitud a la hora de actuar en el ámbito privado. Esa arriesgada forma de actuar iguala a los estudiantes, no habiendo diferencias significativas entre los que tienen mayores o menores conocimientos.

Todas estas conclusiones dan respuesta a las preguntas que, como objetivos de la presente tesis, nos planteamos en la tabla 1 y que justifican la recomendación de revisar los planes de estudio, teniendo en cuenta las motivaciones de los alumnos.

Paralelamente, encontramos información de investigaciones similares a la nuestra en sitios tan distintos y distantes, tanto cultural como geográficamente, como la Universidad de Harvard, o las Nacionales de Taiwán o de Singapur que confirmaban muchos de nuestros resultados. (Marwick, A., Murgía Díaz, D., Palfrey, J. (2010); Lin, S-W.; Liu, Y-C. (2012); Jiang, Z.; Suang, C., Choi, B. (2013)).

Tal como afirmaban Pintrich y de Groot (1990), para obtener buenos resultados en la formación de los estudiantes hay que ayudarlos a desarrollar tanto las habilidades (skills) como la voluntad (will). Siendo el aprendizaje auto regulado uno de los principales retos de la futura práctica docente. (Miñano, P.; Castejón, J.L., 1997)

6.4 Acciones futuras, recomendadas

Es aconsejable crear un plan de formación específico sobre uso y riesgo de las herramientas informáticas más habituales que se estudie en cada asignatura desde su propia óptica, de forma que se consiga concienciar al alumnado en el sentido de que por mucho que se trabaje, si no se protege ese trabajo, puede perderse en su totalidad.

Sabiendo que la mayor motivación de los estudiantes con más inquietudes sobre su privacidad reside en el reconocimiento de la utilidad de las herramientas que protegen su navegación, lo que les hace sentir una mayor atracción por su puesta en funcionamiento a la vez que se sienten con más confianza, debemos estimular esa faceta demostrándoles con casos prácticos lo que puede acarrearles el ignorar esas enseñanzas.

Formación transversal sobre seguridad en una asignatura específica, o coordinada entre varias asignaturas en los primeros cursos de carrera, con muchos ejemplos prácticos de incidencias, abusos, experiencias, contratiempos y perjuicios, que desgraciadamente no faltan, deberían facilitar el interés de las medidas a adoptar para no perder información, arriesgar su privacidad, o poder ser víctimas de fraudes, haciéndoselo más atractivo y útil. Como primer paso ante una formación más completa, adaptada a la realidad y sensibilizada con la protección de la información, los datos y la propia imagen, que genere suficiente nivel de seguridad a la hora de incorporarse a un entorno profesional.

Un ejemplo de esta estrategia nos lo da la Universitat Oberta de Catalunya, en la que todos los grados contemplan en su plan de estudios una asignatura obligatoria de primer semestre de seis créditos denominada “Uso y aplicación de las TIC en el ámbito académico y profesional” que consta de una introducción o iniciación a las competencias TIC, que comprende el uso racional y crítico de las TIC para trabajar y estudiar un conjunto de habilidades consideradas básicas en la Sociedad de la Información, con las que se posibilita el desarrollo de la competencia (Guitert, M. *et al*, 2008).

Dicha asignatura dota a los alumnos de todas las titulaciones de una base de conocimientos y competencias en TIC en donde se trabajan la búsqueda de información en la red, la elaboración de la información digital, su presentación y difusión, la comunicación, las funciones básicas de tecnología digital, la adquisición de una actitud cívica, el trabajo colaborativo en red y la planificación y gestión de un proyecto virtual.

El papel del docente es clave como guía, animador, dinamizador del proceso colaborativo y como evaluador de proceso y de resultados. Durante la acción docente facilita las estrategias docentes para la adquisición de las competencias y evalúa las competencias digitales. Al finalizar, favorece escenarios para la reflexión y el análisis compartido del proceso realizado. (Guitert, Romeu, 2011).

Algunas de las recomendaciones vertidas en cursos de Seguridad en internet, organizados en la UPV por el CFP⁴⁵ ya iban en el sentido de que, antes de iniciar el uso de cualquier aplicación de comunicación, se configure el perfil paso a paso para evitar que, por defecto, se asuma que permitimos limitar nuestra privacidad a los parámetros de interés del proveedor.

Conferencias como las organizadas por el Instituto de Ingeniería de España en septiembre de 2013 de “Seguridad en la red: la protección de la sociedad frente a las amenazas del Siglo XXI”, con ponentes tan próximos para los jóvenes, deberían potenciarse con frecuencia a nivel de toda la UPV.

Deberían transmitirse mensajes vía radio / tv de la UPV, trípticos, mails.... y cualquier otro medio de difusión al alcance de la Universidad con contenidos referidos a temas de seguridad para concienciar a toda la población universitaria (alumnos, PAS, profesores...).

Estos mensajes deberían hacer saber los perjuicios generados por ignorar los riesgos asumidos, incluyendo eslóganes para facilitar el tomar medidas tales como:

- 1) Impida la entrada de virus
- 2) Bloquee a los hackers con un firewall

⁴⁵ Centro de Formación Permanente. Curso: Internet seguro–Como proteger a los hijos, impartido por Ismael Lengua.

- 3) Sea cuidadoso con los mensajes de correo y selectivo con las descargas
- 4) Seleccione contraseñas “auténticas”, utilícelas asiduamente y no permita que su navegador las “recuerde”.
- 5) Mantenga privada su vida privada. Compártala solo con los que desee.
- 6) Haga frecuentes copias de respaldo de sus trabajos para evitarse mayores pérdidas.
- 7) Actualice sus programas de seguridad, etc.

Siendo la finalidad básica de nuestra investigación mejorar el conocimiento y comprensión del fenómeno que nos ocupa (el uso masivo e indiscriminado de comunicación a través de las redes sociales), para lo que hemos recogido la información descrita de cara a facilitar la intervención social y, consecuentemente de forma más útil, corregir posibles desviaciones y ayudar a resolver los problemas derivados, debemos tener en cuenta también el momento o periodo de tiempo en el que se realiza la recogida de la información.

Los procedimientos surgidos de esas actuaciones nos recuerdan los principios que inspiraron el desarrollo de los programas de Calidad en los comienzos de la década de los años 90. Concretamente, se trataba de la llamada “Calidad de Servicio al Cliente” (Market Driven Quality-MDQ), que se basaba en:

Respeto a la persona / Servicio al Cliente / Excelencia

y, para lograrlo, se seguían las siguientes iniciativas:

Definición de las necesidades del Cliente / Medición / Eliminación de Defectos / Reducción de ciclo / Participación de todos

En nuestro estudio, el cliente son los alumnos TIC de la UPV. Sus necesidades se basan en la buena convivencia, el desarrollo de sus capacidades, y la seguridad y confianza de que sus derechos no van a ser conculcados utilizando las posibilidades de la red.

La medición de las actuaciones se obtiene a través de las evaluaciones que impulsemos.

La eliminación de defectos se consigue a través de los datos obtenidos y la promulgación de Recomendaciones, Comunicaciones, contenidos en planes de estudio...

La reducción de ciclo consiste, en facilitar la normativa para detectar desviaciones y facilitar su corrección con la frecuencia necesaria.

Y la participación de todos es obvia: autoridades, instituciones, operadores, proveedores de acceso a internet, empresas, profesores, padres, tutores, familia, compañeros... deberán actuar con un objetivo común, minimizar el riesgo de abusos.

La aplicación periódica de esta metodología MDQ, nos acercará a:

- cuantificar el alcance de la trasgresión,
- el daño consiguiente,
- la forma de reducirlo,
- las acciones necesarias para acortar plazos de ejecución de las mejoras propuestas,
- la involucración de distintos estamentos, y
- comprobar eficientemente el resultado de las distintas iniciativas puestas en marcha en cada una de las fases de la investigación.

es decir, nos obligará a realizar mediciones para poder entender mejor lo que estamos haciendo y como mejorarlo.

De forma global, es similar a la metodología más actual conocida como PDCA o círculo de Deming (Plan/Do/Check/Act). Es decir, una vez analizada la situación, deberíamos ser capaces de crear una sensibilización con la formación adecuada que nos permita, en un futuro próximo, medir la evolución para comprobar los efectos y resultados de los objetivos propuestos para, nuevamente, proponer mejoras adicionales.

Una vez completado un ciclo, hay que volver a empezar hasta estar lo bastante seguros de que las precauciones adoptadas son suficientes, pues la tecnología continuará desarrollándose, facilitando determinadas actuaciones de protección, pero también será aprovechada en perjuicio de nuestros legítimos intereses personales.

De esa forma, podremos cuantificar los riesgos y el grado de sensibilidad de las nuevas muestras de universitarios, así como los posibles daños asociados, las medidas a impulsar desde la propia UPV para reducirlos, las acciones necesarias para acortar plazos de ejecución de las mejoras propuestas, involucrar a todos los estamentos y, tras comprobar la asimilación de las diferentes iniciativas puestas en marcha en cada fase, volver a estudiar la nueva situación y seguir proponiendo medidas de mejora para incrementar la navegación segura de las futuras generaciones que salgan de sus aulas.

7.- BIBLIOGRAFÍA

ACED, C. *et al* (2009). "Las redes sociales". En: *Visibilidad: Cómo gestionar la reputación en Internet*. Barcelona: Gestión 2000, pp. 65–81.

ADE (2010). *Agenda Digital Europea*. <<http://ec.europa.eu/digital-agenda>> [Consulta: 19-03-2015].

AEPD (Agencia Española de Protección de Datos) (2000). *Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre*.

<http://www.agpd.es/portaIwebAGPD/canaIdocumentacion/sentencias/tribunaI_constitucional/common/pdfs/Sentencia292.pdf> [Consulta: 19-03-2015].

AEPD (Agencia Española de Protección de Datos) (2009). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*.

< <http://www.inteco.es/file/vuiNP2GNuMinSjvyZnPW2w> > [Consulta: 19-03-2015].

AEMI (2014). *Anuario Estadístico de 2013*. Ministerio del Interior.

ALABAU, A. (2001). *La Unión Europea y su Política para el Desarrollo de la Sociedad de la Información*. Madrid: Fundación Airtel Vodafone.

ALABAU, A. (2006). *La Unión Europea y su Política para las Comunicaciones Electrónicas*. Madrid: Fundación Vodafone España.

ALAMINOS, A. (2005). *El análisis de la realidad social. Modelos estructurales de covarianzas*. Alicante: Observatorio Europeo de tendencias Sociales.

<<http://www.obets.ua.es/obets/libros/modelos.pdf>> [Consulta: 29-03-2015].

ALBERT GÓMEZ, M^a. J. (2007). *La investigación Educativa: Claves teóricas*. Madrid, España: Mc Graw Hill. Primera Edición.

ALLPORT, G. (1935). *Attitudes*. In *Handbook of Social Psychology*. Worcester, MA: Clarck University Press.

ALONSO TAPIA, J. (2005). *Motivaciones, expectativas y valores-intereses relacionados con el aprendizaje: el cuestionario MEVA*. Madrid: Universidad Autónoma. <<http://www.psicothema.com/psicothema.asp?id=3120>> [Consulta: 19-03-2015].

ALSAJJAN, B., DENNIS, C. (2006). “The impact of trust on acceptance of online banking”, en: *European Association of Education and Research in Commercial Distribution*. 27-30 June 2006 Brunel University - West London, Reino Unido. <<http://bura.brunel.ac.uk/handle/2438/738> > [Consulta: 29-03-2015].

ANDERSON, J. C.; GERBIN, D. W. (1988). “Structural equation modelling in practice: a review and recommended two-step approach”. *Psychological Bulletin*, 103, pp. 411-423.

ANDRADE, J.; COBA, M. (2006). *Modelización de Ecuaciones Estructurales*. La Habana: Escuela Politécnica Nacional.

AREA, M. *et al* (2008). *Alfabetizaciones y tecnologías de la información y la comunicación*. Madrid: Síntesis.

ASIMOV, I. (2010). *Cien preguntas básicas sobre la Ciencia*. Madrid: Alianza.

BACA LOBERA, G. (2005). “La modelización con ecuaciones estructurales en la investigación operativa”, en: *Producción Económica: Anuario de Investigación 2005*. México: Universidad Autónoma Metropolitana de Xochimilco.
<http://148.206.107.15/biblioteca_digital/estadistica.php?id_host=12&tipo=CAPITULO&id=5211&archivo=375-5211pul.pdf&titulo=La%20modelaci%C3%B3n%20con%20ecuaciones%20estructurales%20en%20la%20investigaci%C3%B3n%20educativa> [Consulta: 29-03-2015].

BAGOZZI, R.P., DHOLAKIA, U.M. (2006). "Open source software user communities: A study of participation in Linux User Groups", *Management Science*. 52, pp. 1099–1115.

<<http://www.jstor.org/discover/10.2307/20110583?uid=3737952&uid=2129&uid=2&uid=70&uid=4&sid=21105057663133>> [Consulta: 19-03-2015].

BARCA LOZANO, A. (1999). *Cuestionario de Evaluación de Procesos de Estudio y Aprendizaje para el alumnado universitario*. Traducción de "The study Process Questionnaire (SPQ)" de Biggs, J. B. (1987). A Coruña: Publicaciones de la Revista Galego-Portuguesa de Psicología e Educación.

BARRÓN, A.; SÁNCHEZ, E. (2001). "Estructura social, apoyo social y salud mental", *Psicothema*, 13(1), pp. 17-23.

BATISTA, J.M.; GALLART, G.C. (2000). *Modelos de Ecuaciones estructurales*. Madrid: Ed. La Muralla.

BATISTA, J.M.; GALLART, G.C. (2005). *Temas avanzados en Modelos de Ecuaciones estructurales*. Madrid: Ed. La Muralla.

BAYOT MESTRE, A. (2008). "Medición de la actitud hacia la Estadística. Influencia de los procesos de estudio". *Revista Electrónica de Investigación Psicoeducativa*. nº 16, vol.6 (3), pp: 729-748.

BBC (2005). *Encuesta de la campaña "Get Safe Online", de la Unidad Nacional del Crimen de Alta Tecnología y el gobierno británico*.

<<http://news.bbc.co.uk/2/hi/technology/4378186.stm>> [Consulta: 19-03-2015]

BECHTEL, R.B.; MARANS, R.W.; MICHELSON, W. (1990). *Methods in environmental and behavioral research*. Malabar, FL: Krieger.

BEER, S. (1985). *Diagnosing the system for organizations*. Chichester: J. Wiley.

BELT IBÉRICA (2009). *Portal de profesionales de seguridad informática*.
<http://www.belt.es/noticiasmdb/HOME2_noticias.asp?id=8358>
<<http://www.reuters.com/article/2009/08/28/crime-internet-idUSSP49844920090828>>
[Consultadas: 19-03- 2015].

BELTRÁN, J. (1993). *Procesos, estrategias y técnicas de aprendizaje*. Madrid: Síntesis.

BELTRÁN, J.; PÉREZ, J.A.; ORTEGA, M.I. (2006). *Cuestionario de Estrategias de Aprendizaje (CEA)*. Madrid: TEA Ediciones.

BENTLER, P. M.; BONETT, D. G. (1980). “Significant tests and goodness of fit in the analysis of covariance structures”, *Psychological Bulletin*, 88, pp. 588-606.

BENTLER, P M. (1990). “Comparative fit indexes in structural models”. *Psychological Bulletin*, 107, pp. 238-246.

BENTLER, P.M. (2006). *EQS 6. Structural Equations Manual*. Los Angeles: Universidad de California. Multivariate Software, Inc.
<<http://www.econ.upf.edu/~satorra/CourseSEMVienna2010/EQSManual.pdf>>
[Consulta: 19-03-2015].

BIGGS, J. B. (1987). *The study Process Questionnaire (SPQ) Manual. Student Approaches to Learning and Studying*. Melbourne: Australian Council for Educational Research.

BIGGS, J. B.; KEMBER, D.; LEUNG, D. (2001). “The revised Two Factor Study Process Questionnaire: R-SPQ-2F”. *British Journal of Educational Psychology*. Vol 71, issue 1, pp. 133-149. < http://www.johnbiggs.com.au/pdf/ex_2factor_spq.pdf >
[Consulta: 19-03-2015].

BIT (2008). “España tercer país del mundo en phishing”. *BIT, Revista del COIT (Colegio Oficial de Ingenieros de Telecomunicación)*, nº 167, de febrero – marzo / 2.008, p. 104.

BLALOCK, H. (1967). *Causal inferences in nonexperimental research*. Chapel Hill: University of North Carolina Press.

BLANCO, A. (2008). “Una revisión crítica de la investigación sobre las actitudes de los estudiantes universitarios hacia la Estadística”, *Revista Complutense de Educación*, Vol.19 nº 2, pp. 311-330. Madrid: Universidad Complutense.

BOCG (2003). *Boletín Oficial de las Cortes Generales*, nº 133-8, de 7 de mayo de 2003, en referencia al Diario de Sesiones del Senado del 9 de diciembre de 1999.

BOUDON, R. (1965). “A Method of Linear Causal Analysis: Dependence Analysis”, *American Sociological Review*, vol. 30, pp. 365-374.

BOYD, D.; CRAWFORD, K. (2011). “Six Provocations for Big Data”. En: *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*. Universidad de Oxford, 21-24 de septiembre.

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431> [Consulta: 3-04-2015].

BRIONES, G. (2002). *Metodología de la investigación cuantitativa en las ciencias sociales*. Bogotá: Instituto Colombiano para el fomento de la Educación Superior.

< <http://ebevidencia.com/wp-content/uploads/2014/02/Metodolog%C3%ADa-de-la-investigaci%C3%B3n-cuantitativa-en-las-ciencias-sociales.pdf> > [Consulta: 19-3-2015].

CA (CA Global Security Advisor) (2008). *Informe de Seguridad en Internet: Principales amenazas online de 2008*.

<<http://inza.wordpress.com/2008/01/17/principales-amenazas-online-de-2008-segun-ca/>> [Consulta: 19-03-2015].

CABALLERO DOMÍNGUEZ, A. J. (2006). “SEM vs. PLS: Un Enfoque basado en la Práctica”, en *IV Congreso de Metodología de Encuestas*. Pamplona, 20-22 de septiembre de 2006.

< http://www.emoinsights.com/downloads/articulos/SEM_vs_PLS.pdf > [Consulta: 29-03-2015].

CÁNOVAS, R. (2014). “Los datos, catalizadores de la sociedad y la economía del mañana”. *Revista Bit*, nº 197, pp. 56-58.

CAROT, J.M.; CONCHADO, A.; JABALOYES, J.M. (2009). *Manual del usuario de SPSS Base 16.0*. Universitat Politècnica de València. <<http://min.webs.upv.es/wp-content/uploads/2011/03/Manual-SPSS16.pdf>> [Consulta: 19-03-2015].

CARROLL, J.B. (1985). “Exploratory factor analysis: A tutorial”, en Detterman, D.K. (Ed.), *Current topics in human intelligence*, Vol. 1 *Research Methodology*. Norwood, NJ: Ablex, pp.25-88.

CASAS, M. (2002). *Los modelos de ecuaciones estructurales y su aplicación en el índice europeo de Satisfacción del cliente*. <<http://www.uv.es/asepuma/X/C29C.pdf>> [Consulta: 19-03-2015].

CEBRIÁN, J.L. (1998). *La Red*, Madrid: Editorial Taurus.

CERVELLÓ, E. *et al* (2002). “Motivación y Ansiedad en jugadores de tenis”. *Motricidad. European Journal of Human Movement*, v. 9, pp. 141-161. <<http://www.revistamotricidad.es/openjs/index.php?journal=motricidad&page=article&op=viewArticle&path%5B%5D=84&path%5B%5D=177>> [Consulta: 4-04-2015].

CERVELLÓ, E. *et al* (2003). “Aplicación de modelos de ecuaciones estructurales al estudio de la motivación de los alumnos en las clases de educación física”. *Revista de Educación*, nº 335. Instituto de Evaluación. Ministerio de Educación.

CHAMORRO, D. J. (2005). *Factores determinantes del estilo de liderazgo del director-a*. Tesis doctoral. Universidad Complutense de Madrid. <<http://es.calameo.com/read/000762552140c48cb5df3>> [Consulta: 19-03-2015].

CHRISTENSEN, R.; KNEZEK, G. (2007). “Cross-Validating Measures of Technology Integration: A First Step Toward Examining Potential Relationships Between Technology Integration and Student Achievement”. *Journal of Computing in Teacher Education*, v. 24, nº 1, pp. 15-21.

CIDEC (2004). *Competencias profesionales: enfoques y modelos a debate*. Donostia-San Sebastián: Centro de Investigación y Documentación sobre problemas de la Economía, el Empleo y las Cualificaciones.

CILIP (Chartered Institute of Library and Information Professionals) (2004). *Information literacy – Definition*. <<http://www.cilip.org.uk/cilip/advocacy-campaigns-awards/advocacy-campaigns/information-literacy/information-literacy>>. Traducido en: <<http://dialnet.unirioja.es/descarga/articulo/1302261.pdf>> [Consultados: 19-03-2015].

CISCO (2014). *Annual Security Report*. Cisco Systems Inc.
<http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf> [Consulta: 19-03-2015].

CMT (Comisión para el Mercado de las Telecomunicaciones) (2013). *Informe CMT sobre Comercio Electrónico en España, primer trimestre de 2013*.
<http://www.cmt.es/c/document_library/get_file?uuid=e995b42a-bd79-4dc2-a7ea-b0e068033da9&groupId=10138> [Consulta: 19-03-2015].

COMEU (1999). *eEurope - Una sociedad de la información para todos*. Comunicación, del 8 de diciembre de 1999, relativa a una iniciativa de la Comisión para el Consejo Europeo extraordinario de Lisboa de 23 y 24 de marzo de 2000: 687.
<http://europa.eu/legislation_summaries/information_society/strategies/124221_es.htm> [Consulta: 19-03-2015].

COMEU (2000a). *Indicadores para el examen de los progresos realizados para la creación de un espacio de libertad, seguridad y justicia en la Unión Europea*. Comunicación de la Comisión, de 24 de marzo de 2.000: 167final.
<http://europa.eu/legislation_summaries/other/133121_es.htm> [Consulta: 19-03-2015].

COMEU (2000b). *Creación de una Sociedad de la Información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos. Plan eEurope 2002*. Comunicación de la Comisión al Consejo, al Parlamento, al Comité Económico y Social y al Comité de las Regiones: 890 final.
<http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/133193b_es.htm> [Consulta: 19-03-2015].

COMEU (2005). *i2010 – Una Sociedad de la Información Europea para el crecimiento y el empleo*. Comunicación de la Comisión, de 1 de junio de 2005: 229 final.
<http://europa.eu/legislation_summaries/information_society/strategies/c11328_es.htm
[Consulta: 19-03-2015].

COMSI (2005). *Propuestas de cara al nuevo Plan para el Desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre nuestras Comunidades Autónomas*. Comisión de la Sociedad de la Información y el Conocimiento – junio/2005
<<http://www.agendadigital.gob.es/agenda-digital/planes-antteriores/DescargasPlan%20Avanza/4.%20Antecedentes/conclusiones-definitivas-14Jun1.pdf>> [Consulta: 19-03-2015].

CONCHADO, A. (2011). *Modelización multivariante de los Procesos de Enseñanza – Aprendizaje basados en Competencias en Educación Superior*. Tesis doctoral. Universitat Politècnica de València.
<<https://riunet.upv.es/bitstream/handle/10251/12099/tesisUPV3654.pdf?sequence=6>>
[Consulta: 19-03-2015].

CORRAL-VERDUGO, V. (1995). “Modelos de variables latentes para la investigación conductual”. *Acta Comportamental*, 3, nº 1, pp.171-190.

CRONBACH, L. (1951). “Coefficient alpha and the internal structure of tests”, *Psychometrika*, v. 16, pp. 297-334.

CUPANI, M. (2008). “Análisis de Ecuaciones Estructurales: conceptos, etapas de desarrollo y un ejemplo de aplicación”, *Revista Tesis Psicología*, 1, pp. 164-176.

D'AGOSTINO, D. (2007). "La seguridad en el mundo de la web 2.0". *TechWeek.es*, de 26 de marzo.

<<http://www.techweek.es/seguridad/informes/1001309004801/seguridad-mundo-web-2.0.1.html>> [Consulta: 19-03-2015].

DANKHE, G.L. (1989). "Investigación y Comunicación", en Fernández-Collado, C. y Danhke, G.L. (Eds.). *La comunicación Humana: ciencia social*. México Mcgraw Hill. pp. 385-454.

DAVARA, M.A. (2000). "El Humanismo Tecnológico", *El Mundo, Diario del Navegante*, 4 de marzo de 2000.

<http://www.elmundo.es/navegante/2000/05/03/davara_humanismo.html>, [Consulta: 19-03-2015].

DAVIS, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Tesis Doctoral. Institute of Technology of Massachusetts. < <http://dspace.mit.edu/handle/1721.1/15192>> [Consulta: 3-04-2015].

DAVIS, F.D. (1989). "Perceived usefulness, perceived ease of use and user acceptance of Information Technology". *MIS Quarterly*, 13, pp. 319–340.

DAVIS, F.D.; BAGOZZI, R.P.; WARSHAW, P.R. (1989). "User acceptance of computer technology: A comparison of two theoretical models". *Management Science* 35, pp. 982–1003.

DAVIS, F.D., BAGOZZI, R.P., WARSHAW, P.R. (1992). "Extrinsic and Intrinsic Motivation to use Computers in The Workplace". *Journal of Applied Social Psychology* 22, pp. 1111–1132.

DE VILLAMOR MORGAN-EVANS, LI. (2008). *Derecho, internet y protección de los consumidores en la Unión Europea*. Tesis doctoral. Universidad de Extremadura. <<https://www.educacion.gob.es/teseo/mostrarRef.do?ref=611163>> [Consulta: 19-03-2015].

DE ZWART, M.; LINDSAY, D. (2011). *Teenagers, Legal Risks and Social Networking Sites*. Melbourne: Monash University.

DÍAZ, J. R. (2008). *Seguridad en Internet*. Trabajo de Investigación para Diploma de Estudios Avanzados. Universitat Politècnica de Valencia.

DÍAZ, J. R. (2009). *Análisis de seguridad de la web 2.0, en alumnos de la UPV*. Tesina de Máster. Valencia. Universitat Politècnica. <<http://riunet.upv.es/handle/10251/14401>> [Consulta: 19-03-2015].

DICCIONARIO Temático de Sinónimos y Antónimos (1983). Madrid: Editorial Everest.

DÍEZ, J. (1992). *Métodos de análisis causal*. Madrid: Cuadernos metodológicos del CIS (Centro de Investigaciones Sociológicas), nº 3.

DIRCE (2001). *Armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la Sociedad de la Información*. Directiva 2001/29/CE del Parlamento Europeo y del Consejo de 22 de Mayo de 2001.

DUNCAN, O. (1966). "Path Analysis: Sociological examples", *The American Journal of Sociology*. v. 72, nº 1. pp. 1-16.

DUPEYRAT, C.; MARINÉ, C. (2005). "Implicit of intelligence, goal orientation, cognitive engagement, and achievement: A test of Dweck's model with returning to school adults", *Contemporary Educational Psychology*, 30, pp. 43-59.

DWECK, C.S. (1986). "Motivational Processes Affecting Learning". *American Psychologist*, v. 41, nº 10, pp. 1040-1048.

<<http://www.nisdtx.org/cms/lib/TX21000351/Centricity/Domain/21/j%20carlisle/Motivational%20Processes.pdf>> [Consulta: 3-04-2015].

ECCLES, J.; WIGFIELD, A. (1995). "In the mind of the actor: The structures of adolescents' achievement task values and expectancy beliefs". *Personality and Social Psychology Bulletin*, v. 21, nº 3, pp. 215-225. < <http://hdl.handle.net/2027.42/69045>> [Consulta: 3-04-2015].

ECCLES, J.; WIGFIELD, A. (2002). "Motivational beliefs, values, and goals". *Annual Review of Psychology*, v. 53, pp. 109-132.
< <http://www.rcgd.isr.umich.edu/garp/articles/eccles02c.pdf>> [Consulta: 3-04-2015].

ELEJABARRIETA, F.J.; IÑIGUEZ, L. (1984). *Construcción de Escalas de actitud tipo Thurst y Likert*. Barcelona: Universidad Autónoma.
<http://www.ict.edu.mx/acervo_bibliotecologia_escalas_escalas%20Likert-Thust.pdf> [Consulta: 19-03-2015].

ELLIOT, A.J. y CHURCH, M.A.(1997). "A hierarchical Model of Approach and Avoidance Achievement Motivation". *Journal of Personality and Social Psychology*, v. 72, nº 1, pp. 218-232.

ESPAÑA (1978). Constitución Española. *Boletín Oficial del Estado*, nº 311, de 29 de diciembre, pp. 29313-29424. < http://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229> [Consulta: 29-03-2015].

ESPAÑA (1999). Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, nº 298, de 14 de diciembre de 1.999, pp. 43088-43099. < http://www.boe.es/diario_boe/txt.php?id=BOE-A-1999-23750> [Consulta: 29-03-2015].

ESPAÑA (2008). Reglamento de Desarrollo de la LOPD. *Boletín Oficial del Estado*, de 21 de diciembre de 2.008, pp. 4103-4136.
< <http://www.boe.es/buscar/doc.php?id=BOE-A-2008-979>> [Consulta: 29-03-2015].

ESPAÑA (2010). Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la LEY ORGÁNICA 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado*, del 23 de junio de 2010, pp. 54811-54883. <http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-9953> [Consulta: 29-03-2015].

EUB (Eurobarómetro) (2007). *Datos de enero 2007*.

<http://ec.europa.eu/public_opinion/archives/ebs/ebs_274_en.pdf> [Consulta: 19-03-2015].

EUB (Eurobarómetro) (2011). *Attitudes on Data Protection and Electronic Identity in the European Union*. European Comisión. Special Eurobarometer 359, de Junio.

<http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> [Consulta: 19-03-2015].

EUB (Eurobarómetro) (2013). *Informe de la CE sobre Ciberseguridad*.

<http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf> [Consulta: 19-03-2015].

FERNÁNDEZ, V. (2004). *Relaciones encontradas entre las dimensiones de las estructuras organizativas y los componentes del constructo "capacidad de absorción": El caso de empresas ubicadas en el territorio español*. Tesis doctoral. Terrassa: Universitat Politècnica de Catalunya.

<<http://dialnet.unirioja.es/servlet/tesis?codigo=6837>> [Consulta: 19-03-2015].

FERNÁNDEZ, V. (2006). *Introducción a la investigación en ciencias sociales*. Terrassa: Universitat Politècnica de Catalunya.

FINK, R.; SAMUELS, S.J. (2007). *Inspiring reading success: Interest and Motivation in Age of High-stakes Testing*. Newark: International Reading Assoc.

FUNDACIÓN CTNE (2013). *Identidad digital: el nuevo usuario en el mundo digital*. Madrid: Fundación Telefónica.

FUNTEL (2005): *La Sociedad de la Información en España - 2005*. Madrid: Fundación Telefónica.

FUNTEL (2007). *La Sociedad de la Información en España – 2007*. Madrid: Fundación Telefónica.

FUNTEL (2008). *La Sociedad de la Información en España – 2008*. Madrid: Fundación Telefónica.

FUNTEL (2009). *La Sociedad de la Información en España – 2009*. Madrid: Fundación Telefónica.

FUNTEL (2011). *La Sociedad de la Información en España – 2010*. Madrid: Fundación Telefónica.

FUNTEL (2012). *La Sociedad de la Información en España – 2011*. Madrid: Fundación Telefónica.

FUNTEL (2013). *La Sociedad de la Información en España – 2012*. Madrid: Fundación Telefónica.

FUNTEL (2014). *La Sociedad de la Información en España – 2013*. Madrid: Fundación Telefónica.

GARCÍA, M^a. A. (2011). *Análisis causal con ecuaciones estructurales de la satisfacción ciudadana con los servicios municipales*. Tesina de Máster. Universidad de Santiago de Compostela.

<http://eio.usc.es/pub/mte/descargas/proyectosfinmaster/proyecto_610.pdf> [Consulta: 19-03-2015].

GARCÍA, T.; PINTRICH, P. (1994). “Regulating motivation and cognition in the classroom: The role of self-schemas and self-regulatory strategies”. En Schunk, Dale H.; Zimmerman, Barry J. (Eds). *Self-regulation of learning and performance: Issues and educational applications*. Hillsdale, NJ: Lawrence Erlbaum Associates Inc.,pp. 127-153.

GARCÍA CLAVEL, J.; ARQUES, A. (2003). *Medida de la satisfacción del alumnado a partir de un modelo de ecuaciones estructurales*. Murcia: Universidad de Murcia.

GARCÍA CLAVEL, J.; BALIBREA, J. (2010). *Motivación y rendimiento académico. Los intangibles de la educación*. Murcia: Universidad de Murcia.

GARCÍA SANZ, R. M. (2004). *El Derecho de autor en internet*. Tesis doctoral. Universidad Complutense de Madrid.

<<https://www.educacion.gob.es/teseo/mostrarRef.do?ref=303753>> [Consulta: 19-03-2015].

GARDNER, R. (2003). *Estadística para Psicología usando SPSS para Windows*. México: Prentice Hall.

GARGALLO, B.; FERRERAS, A.; SUÁREZ-RODRÍGUEZ, J.M. (2007). “Estrategias de aprendizaje y rendimiento académico en estudiantes universitarios”. *Revista de Investigación Educativa*, v. 25, n. 2, pp. 421 – 441.

GARGALLO, B. *et al* (2012). “Estrategias de aprendizaje en estudiantes universitarios excelentes y medios. Su evolución a lo largo del primer año de carrera”. *RELIEVE (Revista Electrónica de Investigación y Evaluación Educativa)*, v. 18, nº. 2.

DOI: 10.7203/relieve.18.2.2000 [Consulta: 3-04-2015].

GIL, H. (2005). *Relaciones del capital intelectual y el aprendizaje interorganizativo en el entorno de un centro de investigación tecnológica: aplicación al sector textil de la Comunidad Valenciana*. Tesis doctoral. Universitat Politècnica de València

<http://www.worldcat.org/title/relaciones-del-capital-intelectual-y-el-aprendizaje-interorganizativo-en-el-entorno-de-un-centro-de-investigacion-tecnologica-aplicacion-al-sector-textil-de-la-comunidad-valenciana-tesis-doctoral/oclc/433537498&referer=brief_results> [Consulta: 19-03-2015].

GIONÉS-VALLS, A.; SERRAT-BRUSTENGA, M. (2010). “La gestión de la identidad digital: una nueva habilidad informacional y digital”. *Bid (textos universitaris de biblioteconomía i documentació)*, nº 24. Universitat de Barcelona. <<http://bid.ub.edu/24/giones2.htm>> [Consulta: 3-04-2015].

GITHUA, B. N.; MWANGI, J. G. (2003). “Students’ mathematics self-concept and motivation to learn mathematics: relationship and gender differences among Kenya’s secondary-school students in Nairobi and Rift Valley provinces”. *International Journal of Educational Development*, 23, pp. 487-499.

GOBUSA (2000). *Safe Harbor, Acuerdo UE y EEUU*. Dptº de Comercio USA. <http://www.export.gov/safeharbor/eu/eg_main_018476.asp> [Consulta: 19-03-2015].

GOLDBERGER, AS.; JÖRESKOG, KG. (1975). “Estimation of a model with multiple indicators and multiple causes of a single latent variable”. *JASA (Journal of the American Statistical Association)*, v.10, nº 351, pp. 631-639. <<http://teaching.ust.hk/~sosc602m/Joreskog,%20Karl%20G.%20and%20Arthur%20S.%20Goldberger.pdf>> [Consulta: 3-04-2015].

GÓMEZ-BORJA, M. A.; LORENZO, C.; ALARCÓN, M. C. (2011). *Redes sociales virtuales, ¿de qué depende su uso en España?*. Albacete: Universidad de Castilla-La Mancha.

GONZÁLEZ, F. (2001). *Caracterización de los procesos de Aprendizaje Organizativo y su relación con las Tecnologías de la Información. Aplicación al Sector Textil Hogar de la Comunidad Valenciana*. Tesis doctoral. Universitat Politècnica de València. <<http://www.itio.upv.es/index.php?a=8>> [Consulta: 19-03-2015].

GONZÁLEZ, R. *et al* (1998). “Variables motivacionales, estrategias de aprendizaje y rendimiento académico en estudiantes universitarios: un modelo de relaciones causales”. *Revista de Orientación y Psicopedagogía*, v. 9, nº 16, pp.217-229.

GONZÁLEZ, R. *et al* (2002). “Un modelo causal sobre los determinantes cognitivo-motivacionales del rendimiento académico”. *Revista de Psicología General y Aplicada: Revista de la Federación Española de Asociaciones de Psicología.*, v. 52, nº 4, pp. 499-519.

GONZÁLEZ, E. (2007). “Aumentan los riesgos en la seguridad de web 2.0”. *PCWorld España* del 5 de octubre. < <http://www.pcworld.es/archive/aumentan-los-riesgos-en-la-seguridad-de-web-20> > [Consulta: 19-03-2015].

GORE, A. (1993). *Technology for America's economic growth: A new direction to build economic strength*. San José: Secretaría de prensa de la Casa Blanca. < <http://ntl.bts.gov/lib/jpodocs/briefing/7423.pdf> > [Consulta: 3-04-2015].

GORSUCH, R.L. (1988). “Exploratory factor analysis ”. En Nesselroade, J.R. y Cattell, R.B. (Eds.), *Handbook of Multivariate Experimental Psychology*, 2nd ed. New York: Plenum Press, pp. 231-258.

GREENE, B.A. y MILLER, R.B. (1996). “Influences on Achievement: Goals, Perceived Ability, and Cognitive Engagement”. *Contemporary Educational Psychology*, v. 21, nº 2, pp. 181-192.

GUERRERO PICÓ, M^a. C. (2004). *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal*. Tesis doctoral. Universidad de Granada. <<https://www.educacion.gob.es/teseo/mostrarRef.do?ref=373329>> [Consulta: 19-03-2015].

GUINALIU BLASCO, M. (2005). *La gestión de la confianza en internet: un factor clave para el desarrollo de la economía digital*. Tesis doctoral. Universidad de Zaragoza. <<https://www.educacion.gob.es/teseo/mostrarRef.do?ref=380889>> [Consulta: 19-03-2015].

GUITERT, M. *et al* (2008). "Implementación de la competencia transversal "Uso y aplicación de las TIC en el ámbito académico y profesional" en el contexto universitario de la UOC". *RELATEC: Revista Latinoamericana de Tecnología Educativa*, v. 7, nº 2, pp. 81-89.

GUITERT, M.; ROMEU, T. (2011). "La formación en línea: un reto para el docente". *Cuadernos de Pedagogía*, nº 418, pp. 77-81.

GUTIÉRREZ, M. I. (2008). *Costes de agencia y de transacción como determinantes de las decisiones financieras. Un análisis de ecuaciones estructurales*. Tesis doctoral. Universidad Complutense de Madrid. <<http://eprints.ucm.es/8611/>> [Consulta: 19-03-2015].

GUTIÉRREZ, O. (2015). "La banda Carbanak está detrás del robo digital más grande de la historia". *Cnet*, 16 de febrero < <http://www.cnet.com/es/noticias/la-banda-carbanak-esta-detras-del-robo-digital-mas-grande-en-la-historia/>> [Consulta: 19-03-2015].

GUZMÁN, A. P. (2013). *Factores críticos de éxito en el uso de las Redes Sociales en el ámbito universitario: Aplicación a Twitter*. Tesis doctoral. Universitat Politècnica de València. <<http://riunet.upv.es/handle/10251/28212>> [Consulta: 19-03-2015].

HERNÁNDEZ, V. (2001). *Análisis causal de los intereses profesionales en los estudiantes de secundaria*. Tesis doctoral. Universidad Complutense de Madrid. <<http://eprints.ucm.es/4860/>> [Consulta: 19-03-2015].

HERNÁNDEZ, R.; FERNÁNDEZ, C.; BAPTISTA, P. (2003). *Metodología de la Investigación*. México: McGraw Hill.

HOLTON, G.J.; BRUSH, S.G. (1987). *Introducción a los conceptos y teorías de las ciencias físicas*. Barcelona: Editorial Reverté, 2ª edición.

HOOFNAGLE, C. *et al* (2010). “How different are young adults from older Adults when it comes to information privacy attitudes & policies?”. *SSRN (Social Science Research Network)*. < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864> [Consulta: 3-04-2015].

HU, L.; BENTLER, P. M. (1999). “Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives”. *Structural Equation Modelling: A Multidisciplinary Journal*, v.6, n° 1, pp. 1-55.
< <http://www.tandfonline.com/doi/pdf/10.1080/10705519909540118> > [Consulta: 19-03-2015].

HUERTA, J.E. (2010). “SEM: una breve introducción a los Modelos Estructurales”. En *1ª Escuela de Verano en Movilidad Social*. Universidad de Monterrey <<http://www.ceey.org.mx/site/files/Escuela%20MS/Talleres/Modelos%20Estructurales-Juan%20Enrique%20Huerta.pdf>> [Consulta: 19-03-2015].

INTECO (2010a). *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles*. Madrid: Instituto Nacional de Tecnologías de la Comunicación. <http://www.osimga.org/export/sites/osimga/gl/documentos/d/estudio_sobre_seguridad_informacion_econfianza_hogares_espanoles_4t2009.pdf> [Consulta: 19-03-2015].

INTECO (2010b). *Cuaderno de notas del Observatorio. Seguridad de la Información y Redes Sociales*. Madrid: Instituto Nacional de Tecnologías de la Comunicación <www.inteco.es/file/gt1clfwY4jEGEiZI7GiXgQ> [Consulta: 19-03-2015].

INTECO (2012). *Guía para usuarios: Identidad digital y Reputación online*. Madrid: Instituto Nacional de Tecnologías de la Comunicación. <http://www.inteco.es/CERT/guias_estudios/guias/Guia_Identidad_Reputacion_usuarios> [Consulta: 19-03-2015].

ITU (2006). *Internet used per 100 inhabitants (1994-2006)*. International Telecommunications Union: ITU World Telecommunications. <<http://www.itu.int/ITU-D/ict/statistics/ict/graphs/internet.jpg>> [Consulta: 19-03-2015].

ITU (2011). *Indicators database (2006-2011)*. International Telecommunications Union: ITU World Telecommunications. <<http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf>> [Consulta: 19-03-2015].

JIANG, Z.; SUANG, C., CHOI, B. (2013). "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions". *Information Systems Research*, v. 24, n° 3, pp. 579-595.
<<http://www.comp.nus.edu.sg/~jiang/Jiang%20et%20al.%202013.pdf>> [Consulta: 3-04-2015].

JÖRESKOG, K. G. (1971). "A general method for analysis of covariance structure". *Biometrika*. v. 57, n° 2, pp.239-251.

KAPLAN, A. (1964). *The conduct of inquiry*. San Francisco: Chandler, pp. 10-11

KERLINGER, F.N.; LEE, H. B. (1999). *Foundations of Behavioral Research*. Boston: Cengage Learning; 4 ed.

KERLINGER, F.N.; LEE, H.B. (2002). *Investigación del Comportamiento. Métodos de Investigación en Ciencias Sociales*. Cuarta edición. México, D.F.: McGraw-Hill / Interamericana Editores, S. A.
<http://www.academia.edu/6753714/Investigacion_Del_Comportamiento_-_Kerlinger_Fred_N_PDF> [Consulta: 17-04-2015].

KIM, J.; MUELLER, C. (1978). *Introduction to Factor Analysis: What it is and How To Do It (Quantitative Applications in the Social Sciences)*. Beverly Hills: SAGE Publications.

KLINE, R. (2005). *Principles and Practice of Structural Equation Modeling*. New York: The Guilford Press.
<<http://dspace.hoasen.edu.vn/xmlui/bitstream/handle/123456789/4204/Principles%20and%20Practice%20of%20Structural%20Equation%20Modeling%20%20%20%202010.pdf?sequence=1>> [Consulta: 16-04-2015]

KOOPMAN, T.C. (1949). "Identifications problems in economic model construction". *Econométrica*, v. 17, pp 125-143.

KOSINSKI, M.; YOUYOU, W.; STILLWELL, D. (2014). "Computer-based personality judgments are more accurate than those made by humans". *Proceedings of the National Academy of Sciences*. v. 112, nº 4, pp. 1.036-1.040.

Doi: 10.1073/pnas.1418680112 [Consulta: 19-03-2015].

LAHEY (1999). *Introducción a la Psicología*. Madrid: Mc Graw Hill.

LANEY, D. (2001). "3D Data management: Controlling Data Volume, Velocity, and Variety". *Application Delivery Strategies*, by META Group Inc., nº 949 de 6 de febrero. <<http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>> [Consulta: 19-03-2015].

LASNIER, F. (2000). *Réussir la formation par compétences*. Montreal: Guérin.

LERMA, H. D. (1999). *Metodología de la investigación: propuesta, anteproyecto y proyecto*. Pereira: Ecoe Ediciones.

LIAW, S.S.; HUANG, H.M. (2003). "An investigation of user attitudes toward search engines as an information retrieval tool". *Computers in Human Behavior*, v. 19, nº 6, pp.751– 765.

LIKERT, R. (1932). "A technique for the measurement of attitudes". *Archives of Psychology*, v. 22, nº 140, pp. 1-55.

LIN, S-W; LIU, Y-C (2012). "The effects of motivations, trust, and privacy concern in social networking", *Service Business* 6, pp. 411-424. DOI 10.1007/s11628-012-0158-6.

LLAMAS, R. (2005). *Un análisis institucional de la implantación de la Agenda local 21 por los Ayuntamientos españoles*. Tesis doctoral. Universidad de Granada. <<http://digibug.ugr.es/bitstream/10481/585/1/15403051.pdf>> [Consulta: 19-03-2015].

LOEHLIN, J.C. (1992). *Latent Variable Models: An Introduction to Factor, Path and Structural Analysis*. Hillsdale NJ: Lawrence Erlbaum Associates Inc.

LÓPEZ, R. *et al* (2010). “Elaboración y validación de un cuestionario de actitudes hacia el uso de la tecnología para el aprendizaje de las matemáticas”, en *I Encuentro Nacional TIC en Educación*, 19-20 de Noviembre, en Lisboa.

<<http://funes.uniandes.edu.co/1559/>> [Consulta: 19-03-2015].

LÓPEZ-ARAUJO, B.; OSCA, A. (2010). “Influencia de algunas variables organizacionales sobre la salud y la accidentabilidad laboral”. *Anales de Psicología*, v.26, nº 1, pp. 89-94.

LÓPEZ BORRULL, A. (2005). “Censura de Continguts a Internet: riscos i oportunitats”. *Bid – textos universitaris de biblioteconomia i documentació*, nº 14.

<http://www2.ub.edu/bid/consulta_articulos.php?fichero=14lopez2.htm> [Consulta: 19-03-2015].

LORENZO ROMERO, C. (2011). “Adopción de redes sociales virtuales: ampliación del modelo de aceptación tecnológica integrando confianza y riesgo percibido” *Cuadernos de Economía y Dirección de la Empresa*, vº 14, nº 3, pp. 194-205.

MALHOTRA, N. (2004). *Investigación de Mercados: Un enfoque aplicado*. México: Pearson Prentice Hall.

MANZANO, A.; ZAMORA, S. (2009). *Sistemas de ecuaciones estructurales: una herramienta de investigación. Cuaderno técnico 4*. México: Centro Nacional de Evaluación para la Educación Superior (CENEVAL).

<<https://es.scribd.com/doc/144255933/Sistema-de-ecuaciones-estructurales-una-herramienta-de-investigacion>> [Consulta: 19-03-2015].

MARTÍNEZ GARCÍA, J.A.; MARTÍNEZ CARO, L. (2009). “Los test estadísticos y la evaluación de escalas; el caso de la invalidez discriminante”. *Investigaciones Europeas de Dirección y Economía de la Empresa*, v. 15, nº 2, pp. 15-24.

<<http://repositorio.bib.upct.es:8080/jspui/handle/10317/1600>> [Consulta: 19-03-2015].

MARTÍNEZ LÓPEZ, F.J. *et al* (2006). “Confianza del consumidor en la compra a través de Internet: una propuesta de modelización basada en la jerarquía de aprendizaje estándar”. *Cuadernos de Gestión*, v. 6, n° 2, pp 59-79.

MARWICK, A.; MURGÍA, D.; PALFREY, J. (2010). “Youth, privacy and reputation”. *SSRN (Social Science Research Network)*. Berkman Center Research Publication n° 5, Harvard Public Law Working Paper n° 10-29.

< http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163> [Consulta: 3-04-2015].

MATEOS-APARICIO, G. (2011). "Los modelos de ecuaciones estructurales: una revisión histórica sobre sus orígenes y desarrollo", en Riobóo, V.; Almanzor, J. M.; Riobóo Lestón, I. *Historia de la Probabilidad y la Estadística*. Santiago de Compostela: Eds. AHEPE, pp: 289-301.

MCCREA, B. (2009). “Managing social media risks”. *The Journal: Technological Horizons in Education*, del 10 de septiembre. <<http://thejournal.com/Articles/2009/10/08/Managing-Social-Media-Risks.aspx?Page=2>> [Consulta: 19-03-2015].

MEDINA RIVILLA, A.; CASTILLO ARREDONDO, S. (2003). *Metodología para la realización de proyectos de investigación y tesis doctorales*. Madrid: Editorial Universitas, S.A.

MEJÍA, E. (2005). *Metodología de la Investigación Científica*. Tesis doctoral. Universidad Nacional Mayor de San Marcos, de Lima. <<https://es.scribd.com/doc/56942915/Libro-Metodologia-de-La-Investigacion-2005>> [Consulta: 19-03-2015].

MIKULIC, I.M.; MUIÑOS, R. (2005). “Una explicación integrativa de la Calidad de Vida: La Evaluación Psicológica y el Análisis Factorial Confirmatorio”, en *Memorias de las XII Jornadas de Investigación*, del 4-6 de agosto. Facultad de Psicología, Universidad de Buenos Aires, v. 2, pp. 287-289.

MINET (2010). *Estrategia 2011-2015. Plan Avanza 2*. Ministerio de Industria, Turismo y Comercio.

MIÑANO, P.; CASTEJÓN, J.L., (1997). “Capacidad predictiva de las variables cognitivo-motivacionales sobre el rendimiento académico”. *Revista Electrónica de Motivación y Emoción (R.E.M.E.)*, v. XI, nº 31.

MONSORIU, M. (2008). *Manual de Redes Sociales en Internet*. Madrid: Creaciones Copyright, S. L.

MOYER, K. (2009). "Risk Management and Social Media: A Paradigm Shift". *Gartner Blog Network*, 9 de febrero.

<http://blogs.gartner.com/kristin_moyer/2009/02/09/risk-management-and-social-media-a-paradigm-shift/> [Consulta: 19-03-2015].

NAONE, E. (2011). “Las personas difunden sus ubicaciones sin querer hacerlo”. *MIT Technology Review*, 22 de Abril.

<http://www.technologyreview.es/read_article.aspx?id=37461&pg=2> [Consulta: 3-04-2015].

NIKIFORAKIS, N. y ACAR, G. (2014). “Browser Fingerprinting and the Online-Tracking Arms Race”. *IEEE Spectrum*, agosto.

<<http://spectrum.ieee.org/computing/software/browser-fingerprinting-and-the-onlinetracking-arms-race>> [Consulta: 19-03-2015].

OBSERVATORIO de Redes Sociales (2011). *Tercera oleada*. Madrid.
<<http://www.slideshare.net/TCAnalysis/tca-observatorio-redes-sociales2011publico>>
[Consulta: 19-03-2015].

OBSERVATORIO de Redes Sociales (2012). *Cuarta oleada*. Madrid.

<<http://www.slideshare.net/TCAnalysis/4-oleada-observatorio-de-redes-sociales>>
[Consulta: 19-03-2015].

OLTRA, J.V. (2003). *Estudio de la capacidad de uso y personalización como posibles factores de éxito en el comercio electrónico empresa a consumidor (B2C): aplicación a empresas del Centro Histórico de Valencia*. Tesis doctoral. Universitat Politècnica de València.

http://www.worldcat.org/title/estudio-de-la-capacidad-de-uso-y-personalizacion-como-posibles-factores-de-exito-en-el-comercio-electronico-empresa-a-consumidor-b2c-aplicacion-a-empresas-del-centro-historico-de-valencia-tesis-doctoral/oclc/433380219&referer=brief_results [Consulta: 19-03-2015].

PAVLOU, P.A. (2003). “Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model”. *International Journal of Electronic Commerce*, v. 7, nº 3, pp. 69–103.

PEINADO, S.; BOLÍVAR, J.M.; BRICEÑO, L.A. (2011). “Actitud hacia el uso de la computadora en docentes de Educación Secundaria”. *CONHISREMI, Revista Universitaria Arbitrada de Investigación y Diálogo Académico*, v. 7, nº 1, pp. 86-105.

PEÑA, D.; ROMO, J. (1997). *Introducción a la Estadística para las Ciencias Sociales*. Madrid: McGraw-Hill.

PINTRICH, P.R.; DE GROOT, E.V. (1990). “Motivational and self-regulated learning components of classroom performance”. *Journal of Educational Psychology*, nº 82, pp. 33-40.

PINTRICH, P. R. (2000). “The role of goal orientation in selfregulated learning”, en Boekaerts, M.; Pintrich, P. R.; Zeidner, M. (Eds). *Handbook of self-regulation*. San Diego: Academic Press, pp. 451-502.

PORTILLA, J.A., SANTAELLA, J. (2014). “Regulación: situación actual y análisis a futuro. Recomendaciones del COIT”. *Revista Bit* nº 197, pp. 46-49.

POZUELO, J. (2014). “¿Y si enseñamos de otra manera?. Competencias digitales para el cambio metodológico”. *Caracciolos – Revista digital de investigación en docencia*, v. II, nº 1.

<<http://www3.uah.es/caracciolos/index.php/caracciolos/article/view/17/36> > [Consulta: 29-03-2015].

RECEU (2001). *Puntos de contacto en los que se ofrece un servicio ininterrumpido de veinticuatro horas para luchar contra la delincuencia en el ámbito de la alta tecnología*. Recomendación del Consejo, de 25 de junio de 2.001

<http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/133157_es.htm> [Consulta: 19-03-2015].

REGEU (2004). *Creación de la Agencia Europea de Seguridad de las Redes y de la Información*. Reglamento nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo.

REJÓN GUARDIA, F.; LIÉBANA CABANILLAS, F.; MARTÍNEZ FERNÁNDEZ, M. (2011). “Factores motivacionales de la aceptación de Redes Sociales de Microblogging: Modelo μ BTAM”, en *Univest 2011. III Congreso Internacional. La Autogestión del Aprendizaje*. (Junio, 2011. Girona). < <http://dugi-doc.udg.edu/bitstream/handle/10256/3702/262.pdf?sequence=1> > [Consulta: 4-04-2015].

RIBES, E. (1990). *Psicología General*. México: Editorial Trillas.

RISNES, A. (1999). “School Background, Motivational Belief and Achievement in Mathematics”. *Proceedings of the Twenty First Annual Meeting Phychology of Mathematics Education*, v. 1.

ROJAS, A.; FERNÁNDEZ, J.; PÉREZ, C. (2010). *Investigar mediante encuestas. Fundamentos teóricos y aspectos prácticos. Metodología de las Ciencias del Comportamiento*. Editorial Síntesis, Madrid.

RTVE (2010). *Wikileaks destapa más de 250.000 cables diplomáticos*. 28 de noviembre. < <http://www.rtve.es/noticias/20101128/eeuu-pidio-diplomaticos-espiasen-extranjero-onu/376896.shtml> > [Consulta: 24-04-2015].

RTVE (2013). *Cronología del caso Snowden*. 28 de octubre.
<<http://www.rtve.es/noticias/20131028/cronologia-del-caso-snowden/696721.shtml>>
[Consulta: 19-03-2015].

RUIZ, M. A.; PARDO, A., SAN MARTÍN, R. (2010). “Modelos de Ecuaciones Estructurales”. *Papeles del Psicólogo*, v. 31, nº 1.
<<http://www.papelesdelpsicologo.es/vernumero.asp?id=1794>> [Consulta: 4-04-2015].

RUIZ LIMÓN, R. (2006). *Historia y Evolución del Pensamiento Científico*. Enciclopedia y biblioteca virtual de las ciencias sociales económicas y jurídicas.
< <http://www.eumed.net/libros-gratis/2007a/257/>> [Consulta: 4-04-2015].

SÁEZ, F. (1991). “Los derechos humanos y la nueva frontera de la información”. < http://oa.upm.es/22422/1/Los_derechos_humanos.pdf > [Consulta: 19-03-2015].

SÁEZ, F. (2004). *Más allá de internet: la Red Universal Digital. X-Economía y Nuevo Entorno Tecnosocial*. Madrid. Editorial Universitaria Ramón Areces, S. A.

SALIM, R. (2004). “El cuestionario CEPEA: Herramientas de evaluación de enfoques de aprendizaje en estudiantes universitarios”. *Revista Iberoamericana de Educación*, nº 36/4. < <http://www.rieoei.org/investigacion/1060Salim.PDF>> [Consulta: 19-03-2015].

SALIM, R. (2006). “Motivaciones, enfoques y estrategias de aprendizaje en estudiantes de Bioquímica de una universidad pública argentina”. *Revista Electrónica de Investigación Educativa*, v. 8, nº 1.
<http://www.erevistas.csic.es/ficha_articulo.php?url=oai_revista661:186&oai_iden=oai_revista661> [Consulta: 4-04-2015].

SALINAS, M.; SILVA, C. (2006). “Modelos de regresión y correlación (I)”. *Revista Ciencia y Trabajo*, v. 8, nº 22, pp. 185-189.

SALINAS, M.; SILVA, C. (2007). "Modelos de regresión y correlación (II). Regresión lineal múltiple". *Revista Ciencia y Trabajo*, v. 9, n° 23, pp. 39-41.

SÁNCHEZ GUEVARA, I. (2009). *Ecuaciones Estructurales en la Enseñanza-Aprendizaje de Matemáticas*. México: Universidad Autónoma Metropolitana Xochimilco.

<http://dcsh.xoc.uam.mx/congresodcsh/ponencias_fin/30sep/ConsejoamDocencia/Ecuacionesestructuralesenlaense.pdf> [Consulta: 29-03-2015].

SCHILLER, H. (1996). *Information Inequality. The deepening social crisis in America*. Nueva York: Routledge.

SCHUMACHER, R.; LOMAX, R. (1996). *A beginners Guide to Structural Equation Modeling*. New Jersey: Lawrence Erlbaum Associates Inc.

SHIH, Y.; FANG, K. (2004). "The use of a decomposed Theory of Planned Behavior to study Internet banking in Taiwan". *Internet Research*, v. 14, n° 3, pp. 213–223.

<<http://ir.nctu.edu.tw/bitstream/11536/27251/1/000222845900003.pdf>> [Consulta: 4-04-2015].

SHIN, D.H.; KIM, W.Y (2008). "Applying the technology acceptance model and flow theory to Cyworld user behavior". *CyberPsychology and Behavior*, v. 11, n° 3, pp. 378-382.

SILVA, C.; SCHIATTINO, I. (2008). "Modelos de ecuaciones estructurales, ¿qué es eso?" *Revista Ciencia y Trabajo*, año 10, n° 29 (julio/septiembre).

<<http://prof.usb.ve/jjramirez/POSTGRADO/AFC/Art02%202008%20Art%20Que%20son%20MEE%20con%20Ejemplo%20Esp.pdf>> [Consulta: 19-03-2015].

SOLOVE, D. J. (2007). "Rumor and reputation in a digital world", en *The future of reputation: gossip, rumor, and privacy on the Internet*. New Haven: Yale University Press, pp. 17–102.

STEENKAMP, J.B.E.M., GEYSKENS, I. (2006). “How country characteristics affect the perceived value of a website”. *Journal of Marketing*, v. 70, nº 3, pp. 136–150.

STEIGER, J.H. (1990). “Structural model evaluation and modification: an interval estimation approach”. *Multivariate Behavioral Research*, v. 25, nº 2, pp. 173-180.

STEVENS, J. (2009). *Applied Multivariate Statistics for the Social Sciences*. Nueva York: Routledge, edición 5ª.

TAMAYO y TAMAYO, M. (2003). *El proceso de la investigación científica*. México: Editorial Limusa.

THURSTONE, L. (1928). “Attitudes can be measured”. *American Journal of Sociology*, v. 33, nº 4, pp. 529-554.

TJUE (Tribunal de Justicia de la Unión Europea) (2014). Sentencia del 13-V-2014 en el procedimiento entre Google Spain, S.L.-Google Inc. y la Agencia Española de Protección de Datos – Mario Costeja González.

<https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/common/3_Sentencia_Gran_Sala_de_13_de_mayo_de_2014_Asunto_C-131-12_Google_v_AEPD_y_Mario_Costeja.pdf> [Consulta: 19-03-2015].

TORRES, P. (2010). “Modelos de Ecuaciones Estructurales”. *El evaluador educativo*, nº 10, Año 1, de Junio <<http://www.cubaeduca.cu/medias/evaluador/junio2010-1.pdf>> [Consulta: 19-03-2015].

URLEU (2000). *Consejo Europeo de Santa María da Feira, de 19 y 20 de junio*. Parlamento Europeo. <http://www.europarl.europa.eu/summits/fei2_es.htm> [Consulta: 19-03-2015].

URUEÑA, A. (2011). *Las redes sociales en internet*. Ontsi (Observatorio nacional de las telecomunicaciones y la Sociedad de la Información).

<http://www.ontsi.red.es/ontsi/sites/default/files/redes_sociales-documento_0.pdf> [Consulta: 19-03-2015].

USHER, E.L.; PAJARES, F. (2006). "Sources of academic and self-regulatory efficacy beliefs of entering middle school students". *Contemporary Educational Psychology*, v. 31, n° 2, pp. 125-141.

VIEJO GALICIA, A. (2008). *Security and privacy issues in some special-purpose networks*. Tesis doctoral. Tarragona: Universidad Rovira i Virgili.
<<http://www.tdx.cat/handle/10803/8484>> [Consulta: 19-03-2015].

WOLTERS, C.; PINTRICH, P.; KARABENIC, S. (2003). "Assessing academic self-regulated learning", en *Conference on Indicators of Positive Development: Definitions, Measures, and Prospective Validity*, en marzo en el Bureau of Labor Statistics. (Washington) <http://www.childtrends.org/wp-content/uploads/2013/05/Child_Trends-2003_03_12_PD_PDConfWPK.pdf> [Consulta: 19-03-2015].

WRIGHT, S. (1921). "Correlation and causation". *Journal of Agricultural Research*, v. 20, n° 7, pp. 557-585.

WRIGHT, S. (1934). "The Method of Path Coefficients". *The Annals of Mathematical Statistics*, v. 5, n° 3, pp. 161-215.
<http://www.ssc.wisc.edu/soc/class/soc952/Wright/Wright_The%20Method%20of%20Path%20Coefficients.pdf> [Consulta: 19-03-2015].

7.1 Cursos realizados en el Centro de Formación Permanente de la UPV (CFP)

“Herramientas Estadísticas para la Investigación en docencia universitaria”. Versiones Junio/2009 y 2010

“Herramientas para la Tesis y publicación (I): Introducción a la validación de escalas y manejo del Cuestionario-Datos. Análisis exploratorio de datos y relaciones entre variables en SPSS (ANOVA, Correlación, Tablas, Contingencia, etc.)”. Mayo/2010

“Herramientas para la Tesis y las publicaciones (I): Introducción a la creación y validación de escalas. Manejo del Cuestionario-Datos”. Versiones de Enero y Marzo/2012

“Herramientas metodológicas para la Tesis y las publicaciones (II): Métodos bivariantes y multivariantes: ANOVAs y regresión”. Marzo/2012

“Herramientas metodológicas para la Tesis y las publicaciones (III): Métodos multivariantes: Análisis factorial de componentes principales (ACP)”. Versiones de Enero y Marzo/2012

“Herramientas metodológicas para la Tesis y las publicaciones (IV): Métodos multivariantes de regresión lineal, logística binaria (LOGIT) y logística multinomial”. Abril/2012

“Herramientas metodológicas para la Tesis y las publicaciones (V): Técnicas de agrupación, cluster jerárquico y no jerárquico”. Abril/2012

“Seminario de Metodología de investigación: Introducción a los modelos de Ecuaciones Estructurales (SEM)”. Versiones Abril y Septiembre/2012, y Marzo/2013

“Metodología para la escritura de Artículos y Tesis”. Mayo/2012

“Internet seguro – Como proteger a los hijos”. Abril/2010

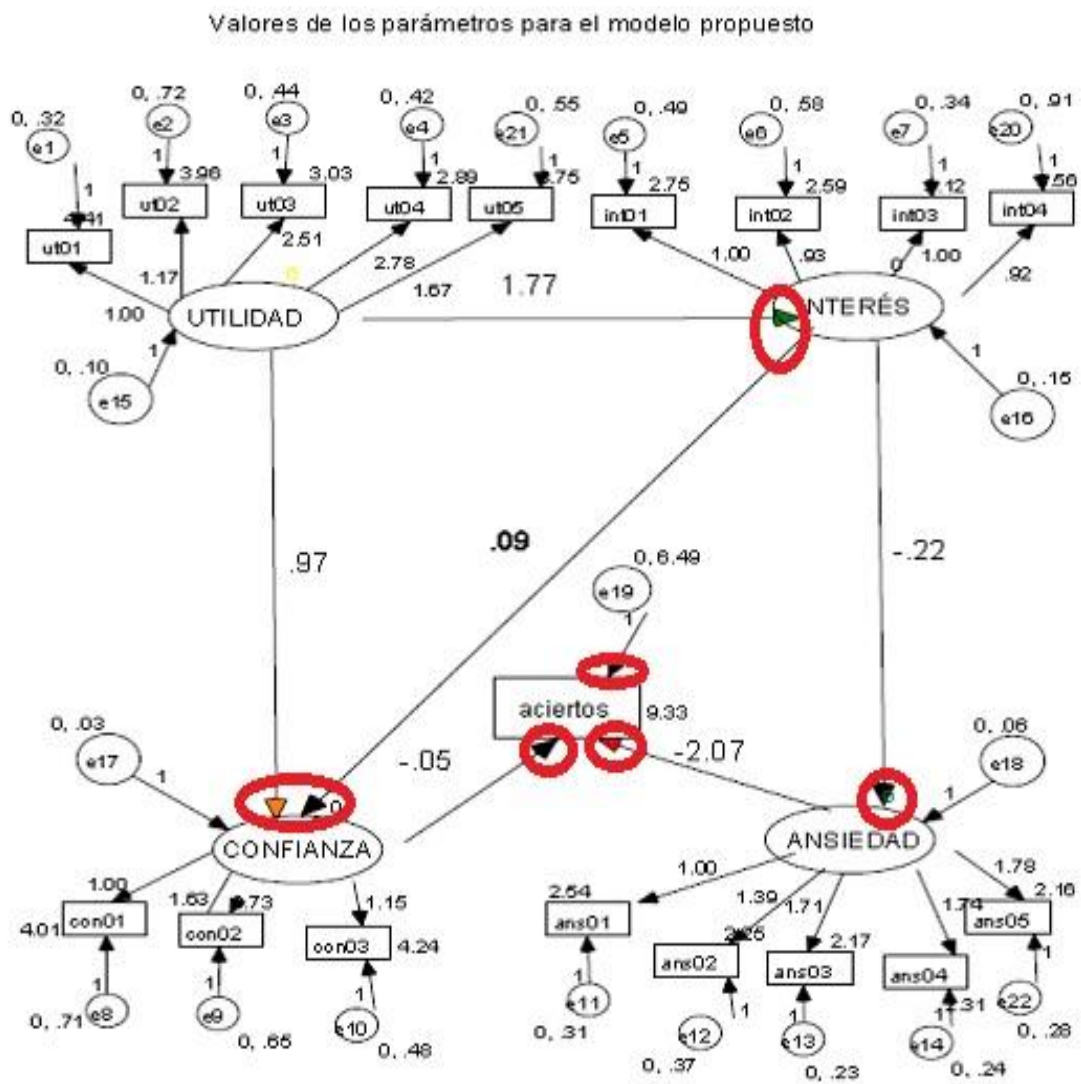
“Derechos de la Propiedad Intelectual: Compartir el Conocimiento”. Junio/2010

“Foro IV: Educación Digital”. Julio/2013

ANEXOS

ANEXO 1 – Grafos estructurales modelo

Gloria Baca es profesora-investigadora en el área de Investigación, Estrategia y Gestión de las Organizaciones del departamento de Producción Económica en la Universidad Autónoma Metropolitana de Xochimilco, en México.

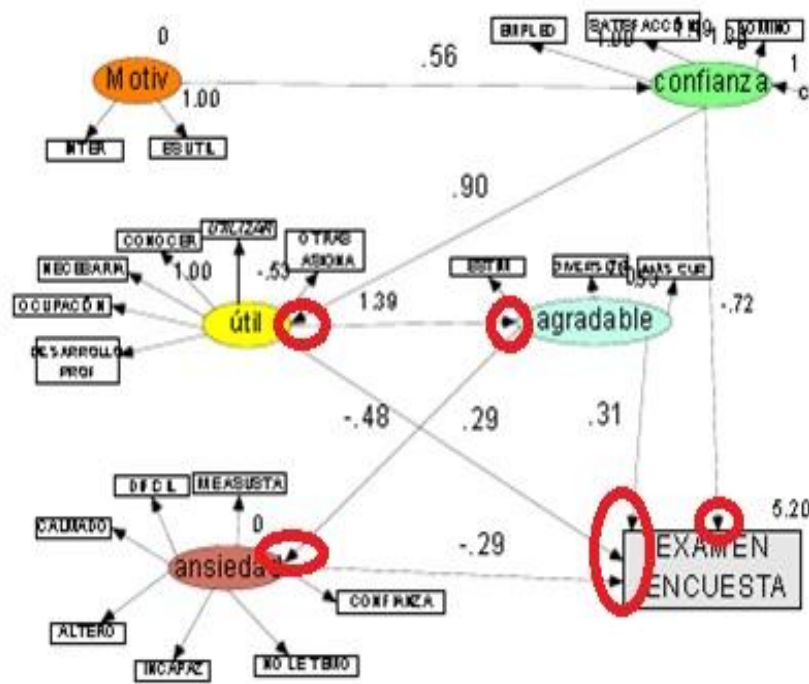


Modelo causal utilizado en investigación educativa. Baca Lobera, G. (2005)

Diseñó el modelo estructural basándose en las teorías motivacionales de Eccles (1995) y su grupo y en el modelo desarrollado por Risnes (1999).

Elaboró un cuestionario para medir las variables latentes (utilidad, interés, confianza y ansiedad) y un test sobre temas de aritmética, álgebra, ecuaciones y planteamiento de problemas a los alumnos de Administración para estudiar las características que relacionan la actitud receptiva de los alumnos con el aprendizaje de las Matemáticas.

Por su parte, Irene Sánchez Guevara, profesora del departamento de Política y Cultura de la misma Universidad que la anterior construyó su modelo con las respuestas de los alumnos de Administración, Economía, Política y Gestión Social a un cuestionario modificado del de la profesora de la Universidad de Deusto Elena Auzmendi, añadiendo un pequeño examen de conocimientos, para estudiar los problemas de enseñanza-aprendizaje de los cursos de Matemáticas.

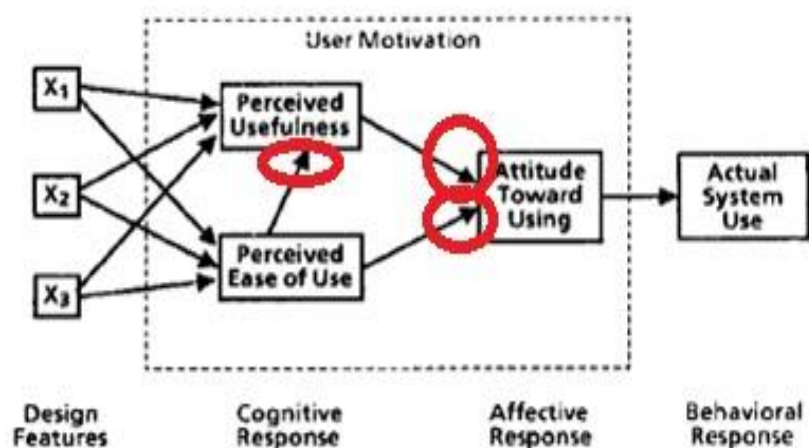


Modelo causal utilizado en la enseñanza-aprendizaje de Matemáticas.
Sánchez Guevara, I. (2009)

Hizo el análisis con ecuaciones estructurales construyendo varios modelos y buscando el de mejor ajuste, partiendo de las variables definidas por Eccles (1995) y Risnes (1999).

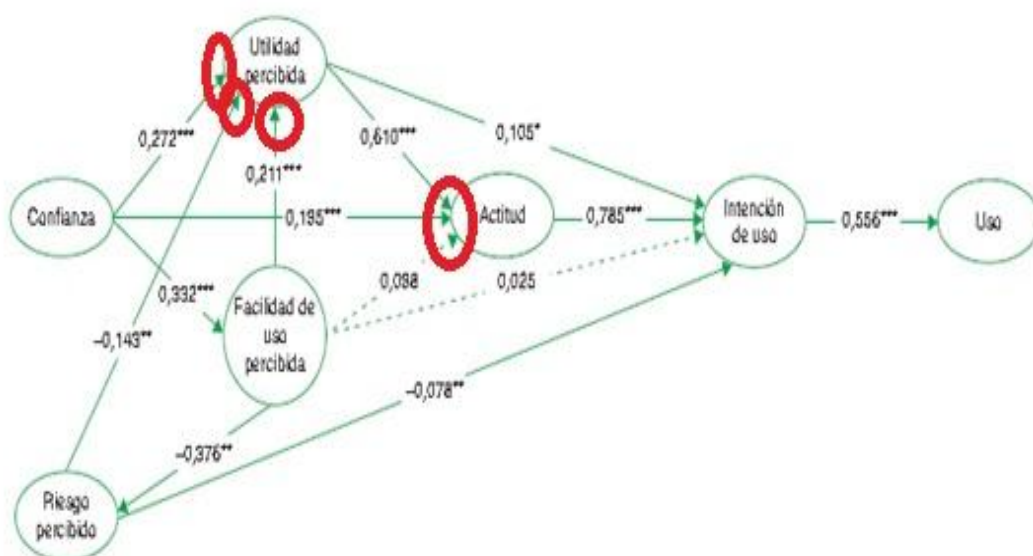
Fred Davis, publicó una investigación en la Universidad de Minnesota en la que validaba unas nuevas escalas incluyendo la utilidad y la facilidad de uso percibidas por los usuarios de nuevas Tecnologías, como determinantes principales para su aceptación. Estas escalas se probaron asegurando su fiabilidad y validez de contenido.

Los análisis de regresión sugieren que la facilidad de uso percibida puede ser un antecedente causal de la utilidad percibida, determinante directo del uso de los recursos



Modelo TAM de aceptación de la Tecnología. Davis, F.D. (1985)

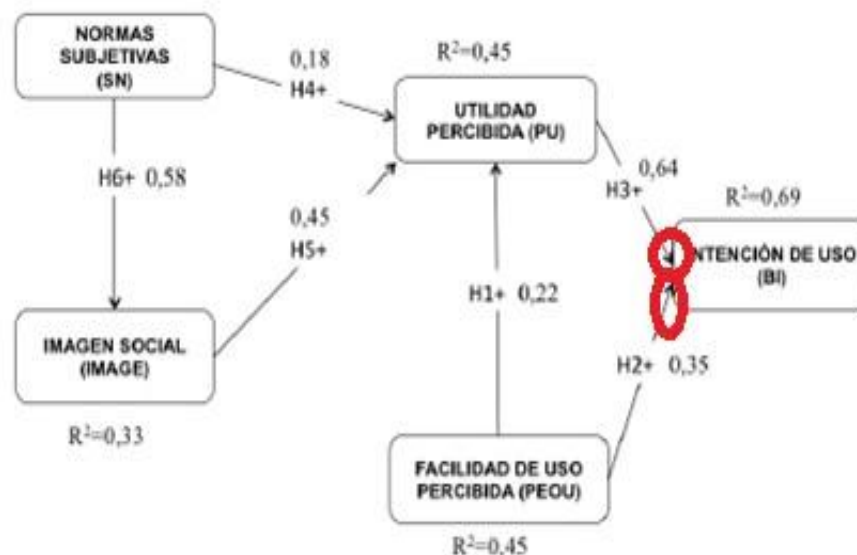
Carlota Lorenzo desarrolló su modelo partiendo de las variables del modelo de Davis (1985), concretándolo para el uso de redes sociales e incorporando nuevos constructos



Modelo causal utilizado en la adopción de redes sociales virtuales.
Lorenzo Romero, C. (2011)

Francisco Rejón y sus compañeros de la Universidad de Granada utilizan también el modelo de Davis (1985) sobre los factores motivacionales en su investigación al utilizar redes sociales con escaso número de caracteres, para compartir lo esencial, y aplicarlas a la docencia al ser una ventana al conocimiento informal.

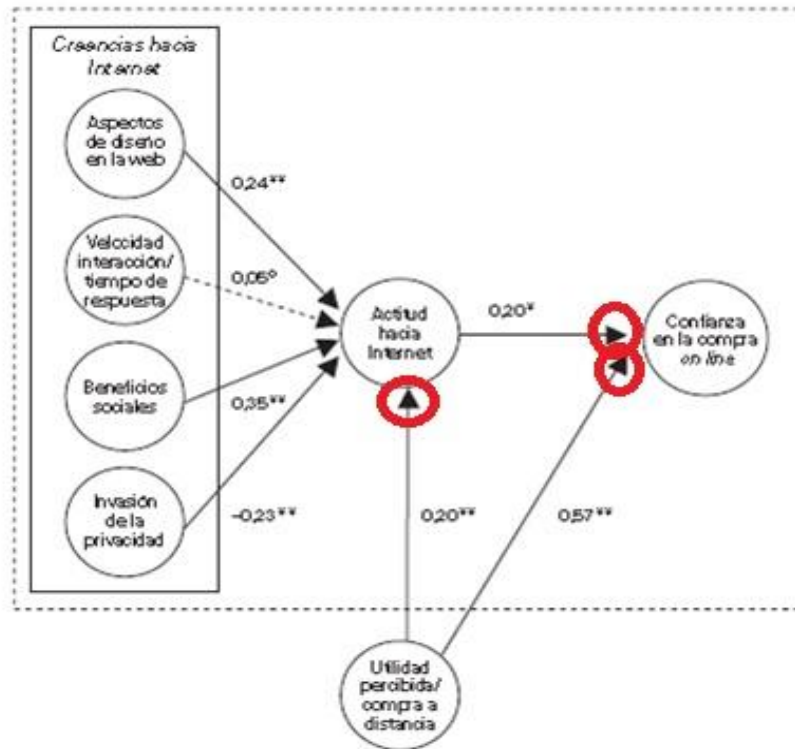
También añaden al modelo básico de Davis constructos para conocer la influencia de normas subjetivas (grado de influencia percibido por el encuestado sobre lo que personas importantes para él consideran sobre si debería usar o no el sistema) y la imagen social por el uso de esas tecnologías (grado de influencia percibido por el encuestado sobre lo que el uso de esa innovación mejorará su estatus en su contexto social).



Modelo de aceptación de redes sociales de microblogging (μBTAM).
Rejón, F.; Liébana, F.; Martínez, M. (2011)

En la construcción del siguiente modelo se tiene en cuenta la construcción clásica de actitudes compuestas por creencias, elementos afectivos y de comportamiento y su orden de influencia, así como su implicación en la Confianza del consumidor, el cual desarrolla unas opiniones (aspectos cognitivos) en función de características que condicionan su actitud (aspecto afectivo) que, a su vez, influye en su comportamiento.

La parte afectiva influye sobre la confianza y el conjunto de relaciones quedan representadas de forma gráfica en el siguiente grafo.



Modelo de confianza del consumidor en la compra a través de internet
Martínez, F.J. *et al* (2006)

Para facilitar la comprensión del lector, se rodean con círculo rojo las direcciones causales de los constructos utilizados en el estudio, recordando la nomenclatura:

Ansiedad = estrés = ... = -facilidad percibida = riesgo

Interés = atracción = ... = agradable = actitud positiva hacia... = intención de uso

Confianza

Utilidad

Aciertos = nota

ANEXO 2 – Aspectos básicos sobre Teoría Estadística en Ciencias Sociales

2A - El Método Científico en las Ciencias Sociales.

La vida social es el objeto de las Ciencias Sociales. Constituye una parte de la realidad observable en la que vivimos inmersos. Podemos formular cuestiones o problemas referidos a la vida social y anticipar soluciones mediante la observación sistemática de los fenómenos sociales.

El método científico en las Ciencias Sociales presenta algunas particularidades especiales, debido a las características peculiares de su objeto de estudio, la Sociedad. Debido a su diversidad y complejidad, en continua evolución y sujeta a la incertidumbre e indeterminación propia de la libertad del hombre, hace difícil aplicar técnicas de observación experimentales. Pero podemos utilizar el método cuantitativo, predominantemente inductivo, que determina las características generales de una población basándose en la observación de suficientes casos individuales de la misma para comprender la situación global lo más profundamente posible.

Los métodos cuantitativos son objetivos y tienen un acusado carácter numérico. Nos proporcionan el marco concreto para el estudio de la realidad social o paradigmas, que definen lo que debemos estudiar y las preguntas que son necesarias responder.

Nuestra investigación consiste en un proceso formado por un conjunto de fases de actuación sucesiva, orientadas a descubrir la realidad en el campo social siguiendo normas y reglas genéricas de actuación científica.

La recogida de información debe ser estructurada y sistemática, utilizando el Análisis Estadístico para cuantificar la realidad social, las posibles relaciones causales y su intensidad. Los resultados obedecerán a la búsqueda cuantitativa de las leyes generales de la conducta.

Aunque nuestra investigación científico social tiene como finalidad hallar respuesta a problemas intuitos pero desconocidos, exigirá la aplicación lo más rigurosa posible del método y las técnicas científicas al campo social, referidas a problemas concretos, lo más precisos, reales y específicos que sea posible, de la realidad social.

Asumimos encontrarnos con una serie de problemas y dificultades en la investigación social, tales como:

- La variabilidad de los fenómenos sociales y las pautas de comportamiento, pues los fenómenos sociales cambian a lo largo del tiempo y del espacio, lo que nos puede dificultar la generalización de resultados empíricos o explicaciones a un fenómeno que tenga validez en cualquier momento del tiempo y la geografía.
- La complejidad. Los fenómenos sociales están integrados por una diversidad de factores y variables que interactúan entre sí, con la dificultad de estudiar todos los factores desde el punto de vista del análisis, debiendo aislar y determinar la influencia de unos factores a otros.
- La realidad social está constituida por personas o individuos.

Pasado un cierto tiempo, hay que volver a empezar para observar los resultados de los planes recomendados, tal y como recomienda la metodología conocida como PDCA, que puede verse en la figura 38, denominada círculo de Deming (Plan / Do / Check / Act) que persigue:

- Planificar: analizar la situación, determinar objetivos, forma de alcanzarlos, etc.
- Hacer: llevar a cabo el trabajo y las acciones planificadas
- Comprobar: verificar los efectos y resultados sobre los objetivos propuestos
- Actuar: llevar a cabo documentación, generalización de resultados, sistematización, emprender nuevas mejoras....



Fig. 38: Círculo de Deming. (EP)

Es decir, seguir estudiando la sensibilidad de los estudiantes respecto su propia seguridad y privacidad y su consiguiente forma de actuar al navegar por la red. Y, pasado un cierto tiempo, volver a empezar hasta estar lo bastante seguros que las precauciones adoptadas son suficientes.

2A.1 - Métodos cuantitativos en las Ciencias Sociales

La investigación social cuantitativa está directamente basada en el paradigma explicativo, que utiliza preferentemente información cuantitativa o cuantificable para describir o tratar de explicar los fenómenos que estudia.

La reconstrucción de la práctica científica, que se hace habitualmente en los textos de metodología de la investigación, presenta ese proceso en una forma un tanto idealizada, ya que consiste en una serie de etapas que se dan en forma lineal, unas tras otras. Si bien ésta será la forma didáctica que utilizaremos, reconocemos que *“una lógica reconstruida no es una descripción (exacta), sino más bien una idealización de la práctica científica. Ni siquiera el más grande de los científicos tiene un estilo cognitivo que sea entera y perfectamente lógico...”* (Kaplan, 1964: 10-11).

Reconocido el carácter didáctico de la lógica reconstruida, según la expresión del epistemólogo norteamericano citado, podemos distinguir tres momentos principales en el proceso de investigación:

- 1) uno de acercamiento inicial al tema y a la problemática existente en el área de interés,
- 2) otro segundo momento, representado por la preparación del proyecto de investigación; y
- 3) un tercer momento, en el cual se realiza o ejecuta la investigación, es decir, se pone en práctica el proyecto de investigación.

Probablemente, como consecuencia del arranque de los Planes de Calidad en las Universidades, se ha provocado una masiva consulta hacia los estudiantes que, en forma de encuestas, están ayudando a analizar diversos aspectos para que se pueda mejorar la educación y el aprendizaje aparejado. En muchos casos se limitan a simples análisis estadísticos descriptivos básicos, pero en otros también profundizan con herramientas más sofisticadas. (García Clavel y Arques, 2003)

Teniendo en cuenta que las etapas de adopción de las tecnologías, estudiadas por Christiansen y Knezech (2007) pasan por diversos niveles tales como:

- a) concienciación, o primera aproximación, sabiendo de su existencia sin más
- b) conocimiento, cuando empezamos a estudiar su funcionamiento y nos sentimos más atraídos
- c) utilización básica, con el software más sencillo, pero descubriendo las posibilidades que se perciben
- d) Confianza, o familiaridad, donde se profundiza en su uso y se descubren recursos para nuestro sector concreto
- e) Aplicación, cuando se ponen en práctica los recursos que se han descubierto y se comparten y muestran a los demás
- f) Integración, cuando se utilizan todas las metodologías, incluidas las aportadas por las aplicaciones tecnológicas, y se comparten con el equipo de trabajo (profesor-alumnos), enriqueciendo el proceso

en nuestro caso el acercamiento al tema específico tiene su origen en la formación teórica y práctica y en los trabajos realizados en el entorno de la seguridad tanto en internet a nivel general como en las aplicaciones desarrolladas para potenciar las redes sociales, así como sobre la actuación de los usuarios en las medidas de autoprotección para minimizar riesgos de privacidad de modo tal que las nuevas investigaciones que realizamos corresponden a una misma línea de indagación que profundiza en el estudio del riesgo real existente en una población con mayor preparación, como es la de los estudiantes de carreras más técnicas de la UPV.

2A.2 - Diseño de la investigación

El diseño metodológico de la investigación propuesta es la estrategia que se utilizará para cumplir con los objetivos de esta investigación. En términos prácticos, tal estrategia está compuesta por una serie de decisiones, procedimientos y técnicas que cumplen funciones particulares, así que utilizaremos la encuesta social.

En relación con esa decisión, debemos especificar los siguientes componentes y tareas:

- Población en la cual se realizará el estudio.
- Tipo y tamaño de la muestra, si procede.
- Descripción de los instrumentos que se utilizarán en la recolección de informaciones: cuestionarios, observación estructurada, escalas para la medición de actitudes, etc.
- Plan general para la recolección de información o trabajo de campo.
- Procedimientos para el procesamiento de la información: codificación.
- Técnicas que se emplearán en el análisis de los datos:
 - a) Para el análisis descriptivo: tablas de frecuencias, medidas de tendencia central, de variabilidad, representaciones gráficas, etc.
 - b) Para el análisis relacional: tabulaciones cruzadas, medidas de asociación para variables nominales, ordinales y proporcionales.
 - c) Para el análisis tipológico: espacio de propiedades, análisis de conglomerados.
 - d) Para el análisis comparativo-descriptivo en la muestra: comparación de distribuciones de frecuencias, proporciones, medias aritméticas, etc. y, según el caso, uso de la estadística t, análisis de la varianza, etc.
 - e) Para el análisis explicativo: en general, técnicas de análisis multivariado como la regresión múltiple, regresión logística, análisis de senderos, etc.

En el caso de variables subyacentes (como actitudes y motivaciones) y de variables complejas, el investigador debe dar definiciones operacionales de tales variables. Por ejemplo, se dirá que será medida con preguntas del tipo de una escala Likert, en las cuales cada individuo señala una opción de respuesta entre las proposiciones que se definen en el conjunto.

Una vez terminado y revisado el proyecto de investigación, podemos iniciar su ejecución. Esto implica cumplir las etapas y tareas especificadas como son la preparación de la población con la que se trabajará, la selección del tipo de muestra que se va a emplear y determinación de su tamaño, la elaboración de los instrumentos que se utilizarán en la recolección de información, la revisión de la información recogida, la codificación de esa información revisada de acuerdo con un código previamente preparado, la preparación de un plan de análisis de acuerdo con los objetivos de la investigación, la preparación de la estructura del informe, análisis e interpretación de los resultados, y la redacción del informe definitivo.

Los medios a utilizar serán:

- Revisión bibliografía.
- Entrevistas con profesionales docentes de los centros estudiados
- Encuestas presenciales (para el piloto) y vía internet (las definitivas)
- Software estadístico SPSS.
- Software de ecuaciones estructurales y análisis de caminos, AMOS
- Asistencia a Congresos de Tecnología Educativa.
- Asistencia a Cursos CFP-UPV adecuados para el uso de las herramientas necesarias realizados por los profesores Carot, J., Hervás, J.L. (sobre SPSS) y Montoro, J. (sobre AMOS) en varias versiones.

2B - Encuestas

El diseño tipo encuesta es exclusivo de las Ciencias Sociales y parte del hecho de que si queremos conocer algo sobre el comportamiento de las personas, lo mejor, más directo y simple, es preguntárselo a ellas. Se trata de obtener información de un grupo significativo de personas acerca de los problemas en estudio para después, a través de un análisis de tipo cuantitativo, llegar a las conclusiones que correspondan con los datos recogidos. Este método ha alcanzado gran popularidad entre los investigadores sociales, pues la encuesta es uno de los métodos posibles de estudio de la realidad social.

Entre las principales ventajas del método de la encuesta tenemos las siguientes:

- a) El conocimiento de la realidad es directo, no intermediado, y por lo tanto más real. Al interrogar abiertamente a las personas para conocer su situación, forma de actuar u opinión, hay que prevenirse contra interpretaciones muy subjetivas.
- b) Como es fácil agrupar los datos en forma de cuadros estadísticos, se facilita la medida de las variables en estudio con las que podemos operar y cuantificar con mayor precisión, permitiendo el uso de correlaciones y otros recursos matemáticos; superando una de las dificultades básicas de la investigación social que es su limitada rigurosidad y la alta posibilidad de errores por un tratamiento poco exacto de los fenómenos.
- c) La encuesta es un método de trabajo relativamente económico y rápido. Resulta fácil llegar rápidamente a una multitud de personas y obtener una gran cantidad de datos en poco tiempo. Su coste, para casos simples, es sensiblemente bajo.

Pero, en determinadas situaciones, aparecen una serie de inconvenientes que le restan validez como diseño. Las desventajas más frecuentes que se le han reconocido son:

- a) La encuesta recoge la visión que la gente tiene de sí misma, muy subjetiva y, para algunos temas, falsa e imprecisa. No es lo mismo lo que las personas hacen o sienten o creen, que lo que ellas mismas dicen que hacen, sienten o creen. Hay recursos para reducir este problema, como omitir algunas preguntas que sabemos no gustan a la mayoría y a las que no van a contestar con sinceridad, también podemos contrastar respuestas, etc.

- b) El diseño de información a través de la encuesta es estático, por lo que conviene repetirla con cierta frecuencia. De lo contrario tendríamos una imagen instantánea de una determinada situación, pero sin conocer su evolución o tendencia al cambio.
- c) El tratamiento de la información es estadístico, lo que supone agrupar a todas las respuestas dándole a cada una igual peso relativo.

La lógica de la verificación mediante encuestas se basa en la correlación estadística que presentan las distribuciones de frecuencias (o los porcentajes) de dos o más variables sobre las cuales se supone que existen relaciones de determinación. De este modo se puede inferir si existe o no una asociación entre los valores de las mismas, con lo cual queda establecida una cierta relación.

Podemos concluir que las encuestas resultan apropiadas casi siempre para estudios de tipo descriptivo, aunque no tanto para los explicativos. Son inadecuadas para profundizar ciertos aspectos psicológicos o psico-sociales profundos pero muy eficaces para problemas menos delicados, como los de las actitudes, o las conductas más simples o los comportamientos, y opiniones masivas, donde sí son más eficaces.

La encuesta descriptiva tiene como objetivos principales:

- 1) describir la distribución de una o más variables en el total del colectivo objeto de estudio o en una muestra del mismo;
- 2) realizar la misma operación en subgrupos significativos de ese colectivo o en su muestra;
- 3) calcular medidas de tendencia central y de dispersión de esas variables en el colectivo total o en la muestra utilizada y en los subgrupos.

El cumplimiento de los dos primeros objetivos permite hacer diversas comparaciones entre las formas de distribución y los valores que toman las variables en esos contextos.

2B.1 - El cuestionario

El cuestionario es el componente principal de una encuesta. Su construcción es más bien la expresión de la experiencia del investigador y de su sentido común, siendo muy recomendable atender a las siguientes indicaciones:

1. Las preguntas del cuestionario deben derivarse de los objetivos del estudio y, por lo tanto, del problema de investigación planteado.
2. No hay un criterio único para saber cuántas preguntas debe contener un cuestionario. Conviene, en una primera etapa, formular cuantas preguntas parezcan apropiadas para cubrir el problema de investigación. En sucesivas revisiones posteriores se podrán encontrar preguntas que aunque parecieron importantes en cierto momento, dejaron de serlo más adelante.
3. El cuestionario debe comenzar con preguntas generales simples, al alcance de cualquier persona, con el fin de establecer un clima favorable, de atracción y armonía.
4. Una pregunta puede influir sobre la siguiente. Para evitarlo colocamos primero las preguntas generales y luego las más específicas sobre el tema concreto, que proporcionan al entrevistado un marco de referencia para contestarlas.
5. Las preguntas deben organizarse en una secuencia lógica, como siguiendo el hilo de una conversación.
6. No hay que utilizar preguntas que pueden inducir la respuesta. Ni tampoco preguntas directas que puedan colocar al encuestado en una situación incómoda. Hay que despersonalizarlas.
7. Debemos evitar utilizar palabras vagas que proporcionan respuestas también vagas, como expresiones tales como: con qué frecuencia, con qué regularidad, diría usted que generalmente, a menudo, etc.

8. El cuestionario debe comprender tres secciones con preguntas de:

- a) determinación del encuestado, que permiten saber si corresponde o no al grupo de personas requeridas por el estudio;
- b) preguntas demográficas o de clasificación (edad, sexo, etc.); y
- c) las preguntas referidas al tema central del estudio (pueden ser preguntas abiertas o cerradas). Forman la parte más larga del cuestionario.

9. Según los objetivos y las necesidades de análisis, el cuestionario podrá utilizar tipos de preguntas como las que presentamos a continuación.

- Preguntas cerradas: Dicotómicas (Sí – No), de respuesta única o múltiple
- Preguntas abiertas: Introdutorias, filtro, de control, de relleno, de clasificación....
- Preguntas con graduaciones en una dirección (unipolar).Muy buena.- Buena.- Regular.- Mala.- Muy mala.-
- Preguntas con graduaciones en dos direcciones (bipolar).Demasiado práctica. Algo práctica.- Sin orientación.- Algo teórica.- Demasiado teórica.-
- Preguntas de acuerdo - desacuerdo. Son, en general, las preguntas que se utilizan en la construcción de escalas tipo Likert o en la construcción de índices con una, dos o tres preguntas que representan indicadores de una misma variable (por ejemplo, intolerancia, individualismo, autoritarismo, etc.). Rojas *et al* (2010)

2B.2 - Presentación del cuestionario

Podemos realizar el cuestionario sobre dos formatos diferentes:

- A través de una página Web, y
- A través de un formulario realizado con MS Word.

Los cuestionarios realizados sobre páginas Web han sido diseñados y desarrollados en HTML, y proporcionan la opción de enviar la información directamente a una base de datos para procesarla posteriormente.

En cambio, el cuestionario en formato MS Word no está enlazado directamente a la base de datos del investigador, por lo que el encuestado debe reenviar el archivo resultante por e-mail al investigador o proponerlo en alguna de las clases para recogerlo en el momento e introducir los resultados de la encuesta a la base de datos uno por uno para su proceso. Este método tiene el inconveniente de la posibilidad de errores de transcripción del formulario a la base de datos. Pero se ha creído conveniente plantearlo para las pruebas piloto.

Se intentó conseguir el apoyo de los departamentos pertinentes de la UPV para llevar a cabo la encuesta a través de alguna aplicación que nos permitiese incluir la página web de forma que diese libertad a los encuestados en elegir el momento de formulación de sus respuestas así como para simplificar el manejo y obtención de datos. Pero debido a la carga de trabajo existente, decidimos utilizar los propios recursos abiertos en la Red.

2B.3 - Prueba del cuestionario

Se realiza la prueba del cuestionario en una pequeña muestra o grupo de personas con características similares a las de la muestra total del universo elegido para cumplir con los objetivos del estudio, y que sirve para algunas o todas de estas funciones:

1. Comprobar la comprensión de las preguntas por parte del encuestado.
2. Descubrir preguntas que suscitan rechazo o inhibición.
3. Examinar las respuestas a preguntas abiertas que puedan reemplazarse por preguntas cerradas.
4. Considerar la eliminación de preguntas con respuestas obvias, similares.

Con la experiencia previa adquirida al pasar un borrador de cuestionario a una población reducida de alumnos de la EPSG, con la que se desarrolló la tesina del Máster CALSI, se observaron las siguientes deficiencias que nos guiaron para la confección de un nuevo cuestionario más adecuado:

➤ El número de preguntas propuesto es excesivo. En una población pequeña que, voluntariamente se ha prestado a rellenar el cuestionario, se puede preparar un formulario relativamente exhaustivo con el fin de tener toda la información que pueda facilitar el estudio posterior. Pero para obtener los datos necesarios para una tesis ulterior, con una población mayor, había que limitar el número de preguntas a las estrictamente relacionadas con el objeto de la investigación. Aunque sea conveniente incluir preguntas tanto de relleno como de control, hay que limitar el número de las mismas para:

- no cansar a los encuestados,
- no complicar innecesariamente la codificación, y
- simplificar la interpretación de los análisis y reportes obtenidos.

- Consecuencia inmediata del punto anterior es que, si reducimos el número de preguntas pero aumentamos la población a encuestar, es muy conveniente automatizar la recogida de resultados. Disminuirá el tiempo de estudio y, sobre todo, desaparecerá el riesgo de errores al trasladar la codificación de resultados a una hoja de cálculo que contenga la entrada de datos al programa de análisis estadístico utilizado.
- Simplicidad en las preguntas. Preguntábamos por la actividad del encuestado en cuanto a si estudiaba, trabajaba o ambas cosas. Bastaba preguntar si trabajaba o no, ya que la población que fue encuestada era, obviamente, estudiante.
- Claridad en las preguntas. Quisimos saber cuántas horas por semana se conectan a internet y dejamos unos puntos suspensivos en el texto de la pregunta que era donde se solicita la información sobre cuántos días a la semana se conectan. Lo mismo al final de la encuesta sobre el tiempo que dedican a conectarse a las redes sociales. En ambos casos hubo un número alto de encuestados que no entendieron que debían dar el dato en los puntos suspensivos, dejando en blanco ese campo.
- Eliminar posibles ambigüedades. En la pregunta referida al uso que se hace de internet, se daban como posibles respuestas: Formación, Trabajo y Otros, entre otras varias alternativas. Al ir a codificar las respuestas manualmente, hemos comprobado que para algunos alumnos la respuesta Trabajo es, en su caso, similar a Formación y, sin embargo, algunos la han indicado en la casilla Otros.
- Asegurar coherencia en el formato de las respuestas. En las preguntas sobre condiciones de alta y perfil del usuario de redes sociales, hay que mantener las alternativas de respuesta de forma creciente (o decreciente) respecto el parámetro (seguridad) que estamos tratando de obtener.
- Homogeneizar el número de respuestas alternativas, el sentido de las mismas (como se ha indicado en el punto anterior), y la “proporcionalidad” de las distancias entre unas y otras para que el tratamiento por los programas estadísticos no nos induzcan a error a la hora de estimar medias, varianzas, desviaciones, nubes de puntos

➤ Meticulosidad en el análisis de las variables para desestimarlas si aportan poco o nada al estudio por la escasa variabilidad. En la primera variable, la edad tenía como única opción ser menor o mayor de 25 años. Para tener una información sobre ese parámetro deberíamos haber permitido más franjas de edad, máxime teniendo en cuenta que la población de aquella encuesta (alumnos de primer curso) es mayoritariamente muy joven. El resultado ha sido que de todas las encuestas solo dos eran mayores de 25, luego no podíamos extrapolar ninguna conclusión en base a las respuestas diferenciadas o no de dos individuos frente a los restantes.

Más flagrante aún fue el caso de la nacionalidad ya que, aún teniendo alumnos Erasmus, rellenaron la encuesta solo estudiantes nacionales de donde suele ser originaria la mayoría objeto del estudio, sobre la puntual de un curso concreto con más extranjeros.

➤ Es fundamental incluir preguntas que permitan detectar incoherencias, para desestimar las respuestas de encuestados poco fiables.

➤ Decidir si conviene más hacer las preguntas en base a criterios tipo examen para conocer el grado de conocimiento, calificando como sabe mucho-poco-regular-..., o hacerlas directamente para que indiquen su “subjetivo” grado de conocimiento, confiando en la sinceridad de las respuestas.

Inicialmente, caímos en el error típico de querer abarcar más de lo que nuestro estudio perseguía y, aún reconociendo la extensión del cuestionario, nos hicimos las siguientes reflexiones al preparar los cuestionarios piloto pues, aunque en principio parece que son muchas preguntas, para asegurar la idoneidad de constructos, hay que tener que:

- a) Es interesante analizar los diferentes perfiles de usuarios por conceptos tales como características personales, estudiantiles y como usuarios tanto de internet como de las redes sociales
- b) Hay que conocer las actuaciones que realizan respecto temas de passwords, back-ups, seguridad, registro de aplicaciones...
- c) Conviene hacer un pequeño test de conocimientos reales
- d) El número de preguntas motivacionales (interés, utilidad, confianza, ansiedad) es mínimo
- e) Es bueno tener preguntas de control para asegurar coherencias (12 y 52)

2B.4 - Constructos y variables

Un constructo es una propiedad supuesta en una persona, que permite explicar su conducta en determinadas ocasiones. Es un concepto teórico, hipotético, tales como la inteligencia, la motivación, la creatividad, las actitudes, etc.

Las variables son propiedades, características o atributos que se dan en grados o modalidades diferentes en las personas y, por derivación de ellas, en los grupos o categorías sociales. Son variables la edad, los ingresos, la educación, el sexo, la ocupación, etc., que, corresponden a grados diferentes o iguales de darse una cierta propiedad o en modalidades diferentes.

Los constructos se definen como propiedades subyacentes, que no pueden medirse en forma directa, sino mediante manifestaciones externas de su existencia, es decir, mediante indicadores también llamados factores. En otras palabras, los constructos son variables subyacentes a las que habitualmente, se denomina variables latentes. Como señala Ribes (1990), los constructos son colecciones de eventos que la mayoría de las veces conforman, al correlacionarse, tendencias o categorías funcionales dentro de los fenómenos psicológicos.

Las variables se clasifican según diversos criterios. Una clasificación básica es aquella que distingue entre variables independientes y variables dependientes. Nombramos variable independiente a la que produce modificaciones en otra variable con la que está relacionada. Suele designársele como variable causal. La variable dependiente experimenta modificaciones siempre que la variable independiente cambia de valor o modalidad de darse. También recibe el nombre de variable efecto. Así, por ejemplo, la escolaridad de una persona es una variable independiente respecto de sus ingresos, el tradicionalismo lo es respecto al autoritarismo, etc. Hay que señalar que una variable independiente en una cierta relación puede ser dependiente en otra, o viceversa, como podría ser el caso del autoritarismo que resultaría ser la causa de determinada orientación política de una persona, etc. (Briones, 2002)

Pero aunque haya variables que tiendan a moverse conjuntamente, la simple asociación estadística entre variables no es condición suficiente para que exista causalidad. “*La condición suficiente y necesaria del principio de causalidad podría ser expresada en estos términos: una variable A es causa de B si siempre que se da A acontece B, y nunca acontece B si previamente no se ha dado A*”. Únicamente existe relación causal en el sentido $A \rightarrow B$, puesto que la causalidad es asimétrica. Sin embargo, no es posible distinguir entre regularidades aisladas en la ocurrencia de dos fenómenos y una relación causal, por lo que, podemos decir que existe causalidad cuando se halla una relación entre dos variables y se ha podido descartar que sea espúrea o no causal. (Caballero, 2006).

De manera general, pero simplificada, podemos decir que entre una variable independiente y su correspondiente variable dependiente se puede dar una variable subyacente, que actúa como puente entre las dos primeras. La religiosidad podría ser una variable subyacente entre las variables tradicionalismo y autoritarismo.

Este juego de variables, cuando implica a varias de ellas, es especialmente tratado con la técnica denominada análisis de senderos, que veremos más adelante.

Otra clasificación importante de las variables es la que las diferencia entre variables individuales y variables colectivas. Las primeras son las propiedades que se dan en las personas, consideradas individualmente, por ejemplo, su nivel de escolaridad formal. Las variables colectivas son propiedades atribuidas a grupos o categorías sociales con base en las propiedades individuales que poseen sus miembros. Resultan de una operación aritmética que se realiza sobre estas últimas propiedades.

Por ejemplo, la tasa de escolaridad de un colectivo, grupo o categoría social, es el promedio de las escolaridades que poseen sus miembros, o la innovación es el porcentaje de personas que según una cierta escala caen en la categoría de innovadores. Respecto de esta clasificación es importante señalar que las mismas técnicas que se emplean en el análisis de variables individuales se utilizan también en el análisis de variables colectivas.

Una clasificación adicional de las variables, de especial importancia para la elección correcta de las técnicas de análisis, se basa en las propiedades matemáticas que poseen los números que se les asignan a los diversos grados o modalidades de manifestación de variables en las personas y, a través de ellas, en los correspondientes colectivos. En esas propiedades o niveles de medición se distinguen tres tipos principales de variables: las nominales, las ordinales y las proporcionales.

Variabes nominales son aquellas en las cuales los números sólo se utilizan para distinguir unos individuos de otros. Por ejemplo, dar un 1 a los hombres y un 0 a las mujeres es sólo una identificación que puede cambiarse sin ninguna consecuencia. Esos números permiten saber, en cierto momento del procesamiento de la información, cuántas personas hay en la categoría 1 y cuántas personas en la categoría 0.

Las variables ordinales son propiedades que pueden darse en las personas en diferentes grados, a los cuales se les puede asignar números que sólo indican relaciones de mayor o menor que. Por ejemplo, si se ha aplicado una escala de dependencia social a algunas personas, y si a una de ellas, con base en sus respuestas, se le ha asignado el número 6 y a otra, con igual base, el número 3, esos números no quieren decir que la segunda es la mitad de dependiente que aquella que ha obtenido el número 6. Sólo significa que la primera es más dependiente que la segunda. En este sentido, se le pudo asignar un número 9 y a la segunda un número 6 para indicar la relación de mayor que y menor que. Digamos, a propósito de este ejemplo, que todas las actitudes son, metodológicamente, variables ordinales y, como tales, tienen, como veremos, sus propias técnicas de análisis, apropiadas para tratar números que se encuentran en relaciones de simple orden.

El tercer grupo de variables que se distinguen, según su nivel de medición, son las variables proporcionales o de razón. En este caso, los números asignados a los grados, o intensidades de darse en las personas, tienen las propiedades de la aritmética. Por lo tanto existe un valor cero y los números corresponden a la cantidad de la propiedad que se posee, pueden sumarse y entre ellos existen relaciones de proporcionalidad, etc. Así, si una persona gana 5.000 euros en un cierto período y otra, en el mismo período, gana 10.000, entonces, puede afirmarse que la segunda gana el doble que la primera o que la primera gana la mitad que la segunda, y sumados sus ingresos ganan 15.000 euros; etc.

La clasificación de las variables, basada en las propiedades matemáticas de los números utilizados en la asignación a las personas o colectivos, tiene, como lo dijimos más arriba, especial importancia para elegir las técnicas apropiadas de su tratamiento analítico. Esto quiere decir que si necesitamos saber si existe o no asociación entre dos variables de tipo ordinal, digamos entre autoestima y rendimiento escolar, entonces debemos utilizar una técnica no paramétrica como lo es, en este caso, el coeficiente gamma⁴⁶ de Goodman y Kruskal. Y así sucede con los otros tipos de variables.

En el modelo estructural distinguimos las variables según sea su papel y su medición:

- Variable observada o indicador, por la que se mide a los encuestados.
- Variable latente. Característica que se desearía medir pero que no se puede observar y que está libre de error de medición. Por ejemplo, una dimensión de un cuestionario o un factor en un análisis factorial exploratorio.
- Variable error. Representa tanto los errores asociados a la medición de una variable como el conjunto de variables que no han sido contempladas en el modelo y que pueden afectar a la medición de una variable observada. Se considera que son variables de tipo latente por no ser observables directamente. El error asociado a la variable dependiente representa el error de predicción.
- Variable de agrupación. Variables categóricas que representan la pertenencia a las distintas subpoblaciones que se desea comparar. Cada código representa una subpoblación.
- Variable exógena, que afecta a otra variable y que no recibe efecto de ninguna variable. Las variables independientes de un modelo de regresión son exógenas.
- Variable endógena, que recibe efecto de otra variable. La variable dependiente de un modelo de regresión es endógena. Toda variable endógena debe ir acompañada de un error.

⁴⁶ Es el cociente entre la diferencia entre concordancias y discrepancias y su suma

Una variable endógena puede afectar a otra variable endógena (pueden actuar tanto como variable independientes como dependientes). La diferencia importante con la regresión lineal es que las variables involucradas son latentes, cada una medida por múltiples indicadores, por lo cual también se les conoce como *constructos*. Es precisamente por esta causa que no se pueden utilizar las técnicas de regresión comunes.

Las mediciones empíricas siempre tendrán algún fallo, por lo que las representaciones de las variables latentes nunca son perfectas. Además de esto, se tiene el hecho de que las variables latentes estudiadas no tiene por qué estar completa y exclusivamente determinadas por los indicadores medidos, por lo que habrá una variación que no se pueda explicar y que se debe a aquellas influencias sobre la variable latente que no han sido explícitamente modeladas.

2B.5 - Causalidad

El concepto de análisis causal en ciencias sociales se refiere a las estrategias y técnicas de elaboración de modelos de este tipo que expliquen los fenómenos, para contrastarlos empíricamente. Sus orígenes se encuentran en el “path-analysis”, literalmente traducido como análisis de senderos, cuyo objeto es el estudio de los efectos de unas variables consideradas como causas sobre otras tomadas como efectos.

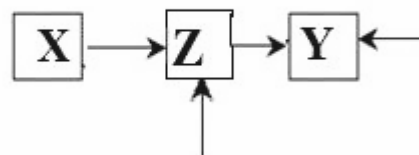
La variable que es efecto se denomina variable dependiente, endógena o explicada y las que originan o causan a la anterior, son las variables independientes, exógenas o explicativas. El análisis path es una técnica similar a la regresión pero con poder explicativo, que estudia los efectos directos e indirectos en el conjunto de las variables observables, asumiendo la existencia de relaciones lineales entre ellas, la incorrelación de los errores de regresión y la ausencia de errores de medición de las variables. Los coeficientes path (C_{ij} : donde i se refiere a la variable efecto y j a la variable causa) explican el impacto de una variable en otra mediante la descomposición de los mismos en tres bloques: path de la variable independiente a la intermedia, path de la intermedia a la dependiente y resto de path que llevan a la variable final, que no incluyen a la interviniente.

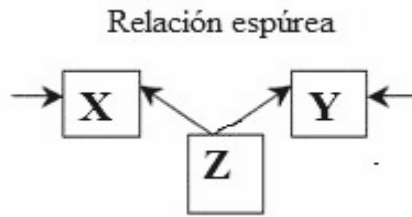
Los efectos causales entre las variables podemos agruparlos en directos, indirectos y espúreos, considerando solamente aquellos que no contemplan reciprocidad entre las variables se pueden representar empleando diagramas de rutas (grafo 8):

Causa - Efecto, directo



Causa - Efectos directo/indirecto



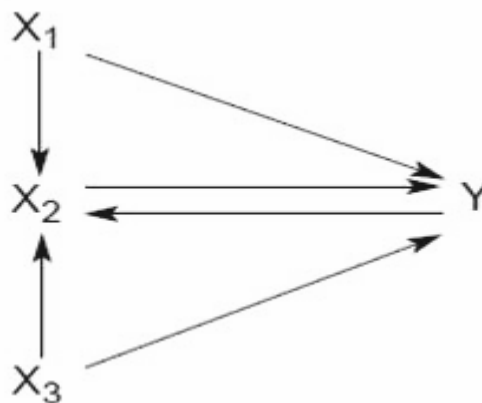


Grafo 8. Diversos tipo de Relación entre variables (EP)

Se pueden obtener las diferentes correlaciones entre las variables analizando el conjunto de los efectos, sean directos, indirectos o espúreos, empleando los coeficientes path.

Con frecuencia recurrimos a un modelo de regresión lineal simple para describir la relación entre una respuesta cuantitativa (Y) de interés y una variable predictiva o descriptora (X) que pensamos es influyente en esa respuesta. (Salinas y Silva 2006). En base a información adecuada sobre estas características estimamos los parámetros de ese modelo, verificamos su validez y precisión y lo aceptamos o descartamos según corresponda.

¿Qué podemos hacer si nos parece evidente que hay más de un factor influyente sobre Y, digamos X_1 , X_2 y X_3 ? Podemos plantear un modelo de regresión lineal múltiple para Y vs X_1 , X_2 y X_3 (Salinas y Silva 2007). Pero ¿si la situación es más compleja? Por ejemplo, si Y influye en los valores que toma X_2 y X_2 es influida por X_1 y X_3 . Lógicamente, aquí se necesitaría más de una ecuación para describir toda esta estructura



Grafo 9. Diversas influencias internas entre variables

Fuente: Silva Zamora y Schiattino Lemus (2008)

Cuando se proponen hipótesis de este tipo, es necesario emplear estrategias factoriales para contrastar dichas hipótesis, debido a que se desea estudiar el efecto de dos o más variables independientes, llamados factores, sobre una variable dependiente, llamada efecto. En este caso, las preguntas a plantear se ajustan a los siguientes modelos:

- ¿Cuál es el efecto del factor X_1 sobre Y ?
- ¿Cuál es el efecto del factor X_2 sobre Y ?
- ¿Cuál es el efecto conjunto de los factores X_1 y X_2 sobre Y ?

Las dos primeras preguntas están orientadas al estudio de los efectos que producen los factores: ' X_1 ' y ' X_2 ', mientras que la tercera, lo está para estudiar el efecto de la interacción o efecto conjunto de los factores ' X_1 ' y ' X_2 '.

Estas ideas comienzan a ser planteadas sistemáticamente por Sewall Wright (Wright 1934) en su análisis de trayectorias (path analysis) y se reafirman con Karl Jöreskog (Jöreskog, 1971; Goldberger y Jöreskog, 1975). Los problemas abordables por esta metodología abundan en Ciencias Sociales (Barrón y Sánchez, 2001). Las asociaciones detectadas entre variables observables o entre variables observables y variables latentes nos llevan a enunciar relaciones de causalidad.

No obstante, aunque sea atractivo poder representar gráficamente la influencia causal de una variable sobre otra y aunque podamos estimar el parámetro que cuantifica ese efecto, debemos considerar que esa estimación no demuestra la causalidad. La relación causal entre las variables debe estar soportada por la sustentación teórica del modelo, no por la medida con datos de tipo transversal. (Ruiz, Pardo y San Martín, 2010).

2C - Introducción a las Escalas de Medición

Las escalas de actitud son instrumentos de medida que nos ayudan a aproximarnos a la variabilidad afectiva de las personas respecto temas de carácter psicológico. Utilizamos las respuestas a un cuestionario como indicadores de una variable subyacente, su actitud. Lo que nos lleva a tener que definir en qué consiste ese atributo (la actitud) y cómo podemos estar seguros de su correcta medición.

Ha habido muchas definiciones de las actitudes, como la clásica: "*Una actitud es un estado mental y neurofisiológico de disponibilidad, organizado por la experiencia, que ejerce una influencia directiva sobre las reacciones del individuo hacia todos los objetos o todas las situaciones que se relacionan con ella*". (Allport, 1935: 45). Aunque generalmente se acepta que la actitud consiste en una predisposición para pensar, sentir, percibir, y, comportarse ante un determinado tema. Teniendo en cuenta que no es lo mismo pensar que sentir o comportarse. Un alcohólico sabe que beber en exceso es perjudicial para su salud, y lo percibe en su propio organismo, pero no deja de hacerlo. En consecuencia, la actitud tiene su propia organización psicológica particular respecto diferentes procesos psicológicos. (Elejabarrieta e Iñiguez, 1984).

Es decir, podemos diferenciar tres dimensiones que organizan la actitud:

- cognitiva, que incluye las creencias y conocimiento respecto un tema
- afectiva, se refiere al agrado hacia ese tema
- comportamental, que controla la relación del individuo con respecto al asunto en cuestión

Louis Leon Thurstone (1928) afirmaba que las actitudes estaban íntimamente ligadas a su medida. Consideraba la opinión como la expresión verbal de la actitud de tal forma que, aunque no podamos acceder directamente a la observación de la actitud, la opinión verbal expresada por las personas nos puede servir como indicador de su actitud.

Si obtenemos un índice que exprese el grado de aceptación o rechazo de las opiniones de las personas sobre temas concretos podremos conocer, aunque sea indirectamente, una medida de sus actitudes, independientemente de lo que esas personas sientan en realidad o la forma en la que actúen.

Ante las críticas que recibió sobre sus métodos de medición se defendió con la siguiente analogía: "*La medida de cualquier objeto o entidad describe sólo un atributo (o sea, propiedad) del objeto medido. Tal es la característica universal de toda medición. Si medimos la altura de una mesa, no describimos la mesa en su totalidad, sino sólo el atributo que se ha medido*" (Elejabarrieta, 1984: 2).

De los tres componentes de la actitud que hemos indicado, las escalas solo miden la dimensión afectiva. Por tanto, para medir las actitudes haremos una clasificación con los individuos según tengan una tendencia más o menos favorable a cierto tema.

Los conocimientos los obtendremos mediante un test y sus comportamientos preguntándoselo directamente, asegurando coherencias.

Hay métodos para analizar los tipos de escalas que miden el componente afectivo de la actitud y se corresponden con las que diferencian tipos de variables, concretamente utilizaremos las de los tipos:

✓ Nominal

Clasifican por alguna característica claramente diferenciable en dos o más grupos (por ejemplo, Si / No). Diferenciamos a las personas en función de poseer un atributo. Por ejemplo, la raza, el sexo, la nacionalidad, etc.

✓ Ordinal

Se basa en el orden de los objetos y, aunque no de información sobre la distancia que hay entre ellos, clasifica a las personas en función del grado en que tienen cierto atributo. Por ejemplo, si en una determinada pregunta hacemos contestar con las categorías: a) totalmente de acuerdo, b) de acuerdo, c) indiferente, d) en desacuerdo y, e) totalmente en desacuerdo, ordenamos a las personas de acuerdo a estas categorías, aunque no sepamos la distancia entre respuestas diferentes. Ordenamos aunque no podamos medir las distancias que los separan.

2C.1 - Escala de Likert

La escala de actitud que definimos a continuación es la de Calificaciones sumadas de Likert. Forman parte de las que hemos llamado escalas ordinales, utilizando series de afirmaciones o ítems sobre los cuales se obtiene una respuesta por parte del individuo. (Elejabarrieta e Iñiguez, 1984)

Este método de medida de actitudes lo desarrolló Rensis Likert en 1932 y es utilizado habitualmente en las encuestas realizadas por la propia UPV. Sigue de plena vigencia y muy popularizado. Bajo la perspectiva de considerar las actitudes como una dimensión lineal continua que se mueve entre lo más favorable y lo más desfavorable, sitúa a cada encuestado en un punto determinado y tiene en cuenta la amplitud y la consistencia de las respuestas actitudinales. La escala enuncia reflexiones sobre las que se tiene que definir el encuestado.

Consiste en un conjunto de ítems presentados en forma de afirmaciones o juicios ante los cuales se pide la opinión de las personas a encuestar. Es decir, se desarrolla cada afirmación y se pide a la persona que indique su reacción eligiendo uno de los puntos en los que se construye la escala. A cada punto se le asigna un valor numérico y, de esta forma, obtenemos una valoración respecto al enunciado propuesto, obteniendo una puntuación total final, simplemente sumando las puntuaciones obtenidas en cada uno de los enunciados.

Las afirmaciones califican al tema de actitud que estamos midiendo utilizando frases sencillas y cortas y deben expresar sólo una relación lógica. Las alternativas de respuesta o puntos de la escala son cinco e indican cuánto se está de acuerdo con cada afirmación. A cada una de ellas se asigna un valor numérico y sólo se puede marcar una opción. Se considerará inválido marcar dos o más opciones.

Tenemos en un eje la Probabilidad de Respuesta favorable, en el otro el continuum de la actitud y dentro dibujamos la Probabilidad de Respuesta de diferentes enunciados (figura 39). Cuanto más favorable sea la actitud, deberíamos obtener una mayor Probabilidad de Respuesta favorable. La curva P_1 correspondiente a una proposición nos proporciona las probabilidades de respuesta favorables a una respuesta "neutra",

porque incluso algunos individuos que tienen una actitud poco favorable pueden manifestar una alta probabilidad de respuesta favorable. La proposición 2 (P_2) es intermedia y la proposición 3 (P_3) es apropiada porque sólo recibe respuestas favorables por parte de los encuestados con una actitud muy favorable.

Prob.de respuesta favorable

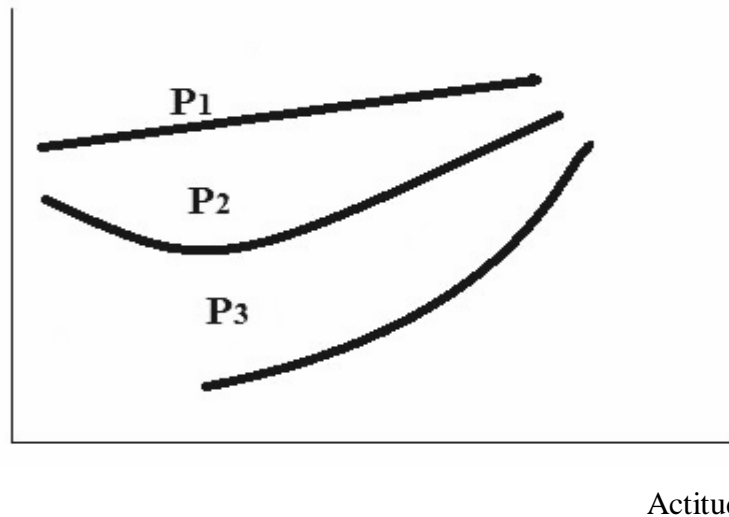


Fig. 39: Curvas actitud-probabilidad de respuesta 1 - (EP)

Sin embargo, estas curvas no representan todas las posibilidades de las proposiciones que debemos asociar a una actitud. Algunas de estas proposiciones deberán ser rechazadas por no discriminar y otras habrán de ser corregidas (figura 40).

Prob.de respuesta favorable

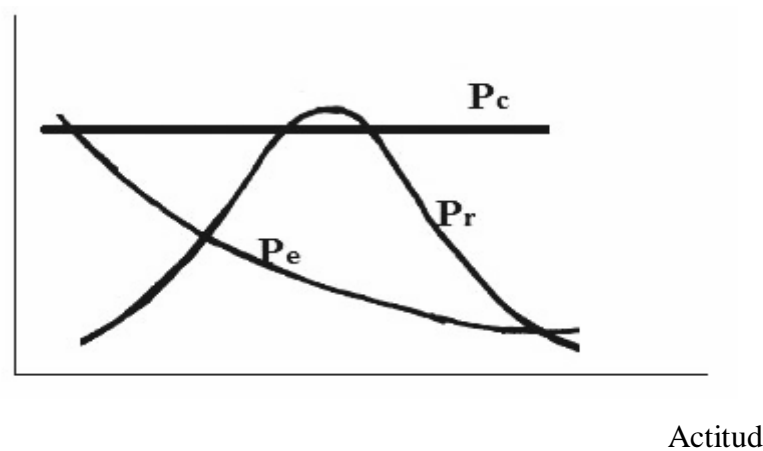


Fig. 40: Curvas actitud-probabilidad de respuesta 2 - (EP)

La recta P_c nos refleja una proporción constante de respuestas favorables. Con independencia de su actitud, todos los encuestados dan una respuesta con el mismo grado de aceptación. La curva P_e implica un simple error de codificación pues si invertimos sus valores tendremos una propuesta lógica. La curva P_r se obtendría por un enunciado que implicase una respuesta media rechazada tanto por los encuestados claramente favorables como por los claramente desfavorables.

Esto nos muestra la propiedad fundamental de las escalas Likert, la relación monótona. Es decir, la probabilidad de que una persona acepte o rechace los enunciados de una escala, mantiene una relación monótona con la posición que la persona ocupa en el continuum hipotético de la actitud. Entendemos relación monótona a que la aceptación o rechazo de una afirmación está siempre ligada de forma monótona a la posición que la persona ocupa en la escala. O sea, aumenta o disminuye en función de la favorabilidad o contrariedad. Lo que implica que es necesario que los enunciados hayan sido aceptados para que la medida sea posible.

Cada propuesta de la escala da información sobre la actitud del individuo. La suma de respuestas nos permite decidir la posición que esa persona ocupa en el hipotético continuum de la actitud. Podemos decir que cada elemento proporciona una información insuficiente pero necesaria. (Elejabarrieta e Iñiguez, 1984)

2C.2 - Construcción de las escalas Likert

La escala Likert se construye creando un alto número de afirmaciones que califiquen al tema de actitud y se proponen a un grupo piloto para obtener las puntuaciones del grupo en cada afirmación. Las afirmaciones cuyas puntuaciones se correlacionen de forma significativa con las puntuaciones de toda la escala, se seleccionan para integrar la medida. Asimismo, hay que calcular la confianza y validez de la escala.

En primer lugar debemos definir las variables que forman la actitud que pretendemos medir. Para ello, consultaremos la información pertinente para construir los ítems. Con estas fases ya podemos tener una escala previa que utilizaremos en la prueba piloto con una muestra representativa de la población. Con el resultado podremos hacer un análisis de los ítems que nos permitirán decidir si son discriminativos o no y si los debemos modificar. Una vez analizada la muestra que nos interesa estudiar, verificaremos la validez y la fiabilidad de la escala diseñada.

Para esta escala sólo se recogen enunciados favorables o desfavorables, pero no neutros. Aunque no es estrictamente necesario, conviene que la mitad de los ítems sean favorables y la otra mitad sean desfavorables. Veremos cada una de estos pasos más detenidamente.

Nos aseguraremos de que las afirmaciones y alternativas de respuesta serán comprendidas por los encuestados a los que se les aplicará, que lógicamente tendrán la suficiente capacidad de discriminación.

Cada afirmación propuesta va seguida de una escala estimativa que consiste en una graduación que va desde el "totalmente de acuerdo" hasta el "totalmente en desacuerdo", con grados intermedios no tan radicales, con respecto a la afirmación.

En la escala de Likert los encuestados tienen que expresar su opinión sobre todos los ítems y además de forma gradual.

La escala de estimación incluye un valor numérico asignado a cada intervalo gradual, y previamente se explica al encuestado el significado de estos números.

Por ejemplo, diríamos que para cada afirmación se debe señalar si se está:

1 Totalmente en desacuerdo

2 En desacuerdo

3 Indiferente, indeciso o neutro

4 De acuerdo

5 Totalmente de acuerdo

Y, a continuación, vendría cada enunciado

2C.3 - Análisis de los ítems

Una persona muy favorable hacia el tema de actitud tendrá una mayor probabilidad de dar un gran número de respuestas favorables que otro encuestado menos proclive. A su vez una persona que haya dado muchas respuestas favorables presentará una alta probabilidad de tener una actitud favorable. El número de respuestas favorables, o una combinación más compleja, nos da un buen indicador de la actitud.

Para aceptar un ítem en la escala definitiva, éste debe mostrar que su aceptación o su rechazo tienen relación con la posición de cada persona en el continuum actitudinal, cumpliendo la relación monótona. Hay que comprobar la existencia de la relación y que es estadísticamente significativa.

Los ítems con respuestas favorables por parte de encuestados que, como grupo, no responden a la mayoría de los otros ítems de forma favorable (o viceversa) se descartan, al considerar que no detectan las mismas actitudes que los otros ítems. Es decir, tratamos de validar la significación de un ítem estableciendo la relación entre las calificaciones elementales que han sido dadas y las globales correspondientes. La global se comporta como el validante o criterio de la elemental.

Para estos análisis verificaremos la forma de las distribuciones de los ítems propuestos:

-si la distribución es normal, se utilizará la “t” de Student generalmente, puesto que son datos independientes y, en la mayoría de las ocasiones, muestras pequeñas.

--cuando la distribución no es normal utilizaremos una prueba no paramétrica

Para establecer la fiabilidad, o consistencia interna de las propuestas, podemos correlacionar las puntuaciones globales y la lista de puntuaciones elementales para todos los encuestados, quedándonos con los enunciados que demuestren una correlación estadísticamente aceptable con las puntuaciones globales. Esta decisión puede considerarse un tanto ambigua pues habitualmente se aceptan correlaciones de 0.35. Se utilizará el coeficiente de correlación (ρ) de Pearson. (Elejabarrieta e Iñiguez, 1984).

2C.4 - Maneras de aplicar la escala Likert

La forma básica de aplicar una escala Likert consiste en realizarla de manera auto administrada; es decir, se entrega el cuestionario al encuestado y éste marca la categoría de respuesta que mejor describe su reacción respecto a cada afirmación.

Para lo formulación de las preguntas Lerma (1999) sugiere las siguientes recomendaciones, de forma genérica:

Escribirlas de forma corta, clara y sencilla

Dar prioridad a preguntas cerradas –falso-verdadero-, si: no: no sé, o selección 1-5

Evitar el uso de negaciones en las preguntas

Deben aparecer en una secuencia lógica

La redacción debe ser neutral y no predisponer ningún tipo de respuesta

No deben dar lugar a varias interpretaciones

Evitar términos técnicos

Las opciones de respuesta deben ser mutuamente excluyentes

Las encuestas o formularios deben ser iguales para toda la población o muestra.

En nuestro caso concreto, para saber las razones con las que debemos ser capaces de reducir al mínimo los riesgos al realizar la actividad de manejo, proceso y navegación, el tipo de preguntas asociadas se muestran esquemáticamente en la tabla 28

Tabla 28. Formulación de preguntas correspondientes a valores

Valor adquirido	Trato de obtener buenas notas en los cursos de seguridad informática
intrínseco	Me da gran tranquilidad navegar seguro
utilitario	Considero que la seguridad me va a ser muy útil en mi vida
esfuerzo	Creo que dedico excesivo tiempo a resolver problemas de seguridad

Fuente: Pintrich y De Groot (1990)

La escala de Likert utilizada será de 1 a 5 para responder a las preguntas, donde:

1 = nunca, 2 = casi nunca, 3 = a veces, 4 = casi siempre, 5 = siempre

2C.5 - Fiabilidad y Validez de las Escalas de Actitud

Medir es el proceso de vincular conceptos abstractos con indicadores empíricos, mediante clasificación y/o cuantificación. Debe hacerse con confianza y validez.

La confianza se refiere al grado en que la aplicación repetida del instrumento de medición a la misma persona produce iguales resultados.

La validez se refiere al grado en que el instrumento de medida mide realmente las variables que pretende medir.

No hay medición perfecta, pero hay que conocer el orden de magnitud del posible error de medición y debemos reducirlo a límites tolerables.

Determinar la fiabilidad y la validez de las escalas de actitud utilizadas es importante a la hora de analizar los datos. Los procedimientos para obtener la fiabilidad y la validez de las escalas de actitud son comunes a otros muchos instrumentos de medición utilizados en Ciencias Humanas. Enumeraremos los más usuales y señalaremos la conveniencia de utilizar algunos de ellos para conocer cuál es la condición con la que debemos analizar los datos, pues conviene recordar que aunque las escalas de actitud se consideran instrumentos fiables y válidos, no son instrumentos estandarizados en la mayoría de los casos, dado que los construimos nosotros mismos.

Si no podemos medir de forma real la actitud, debemos considerar la fiabilidad de una escala como la amplitud de su dispersión ante las repetidas mediciones.

El indicador básico más aceptado para garantizar la fiabilidad de la escala de medición es el Alfa de Cronbach⁴⁷, que se puede combinar con un estadístico adicional como la fiabilidad del constructo. Cronbach (1951).

La validez puede verse afectada por la improvisación pero nos ayuda a saber si una escala de actitud mide lo que decimos que mide.

⁴⁷ Es una media ponderada de las correlaciones entre las variables (o ítems) que forman parte de la escala, indicando la consistencia interna dentro del constructo.

La validez de contenido verifica si la muestra es representativa de la población a investigar, con suficientes variables observables pero no redundantes, que miden lo que queremos. Valida la escala sobre dos grupos de individuos (uno normal y otro conocido). Si obtenemos una diferencia correlacionable entre las puntuaciones obtenidas por los dos grupos podemos decir que la escala es válida. En nuestro estudio hemos conseguido una escala basada en la amplia revisión de la literatura existente que garantiza la validez de contenido de la misma.

La validez de constructo se basa en establecer la relación entre dos variables objeto de actitud. Planteamos la relación hipotética entre dos variables, las medimos y comprobamos si existe la relación; si se confirma la hipótesis establecida, podemos conocer su validez. Es decir, establece si medimos lo que pretendemos. Bechtel, Marans y Michelson (1990).

2C.6 - Codificación

Este procedimiento tratará de agrupar numéricamente los datos expresados para poder operar con ellos como si se tratara, simplemente, de datos cuantitativos. Para ello se partirá de un acumulado de informaciones que tengan homogeneidad, lo cual es necesario para poderlas integrar. Podremos tratar cientos de respuestas a cada pregunta, o de una variedad de posibles situaciones observadas mediante un mismo ítem con una determinada pauta de observación. En ambos casos tendremos una variedad de respuesta que presenten las elecciones o los comportamientos de los encuestados.

Lo primero que hay que hacer con los datos obtenidos es agruparlos de acuerdo a un criterio elemental, separando de un lado la información de tipo numérica de la información expresada mediante palabras, si se hubiese planteado con esa posibilidad (por ejemplo, respuestas tipo abierto mediante comentario). Los datos numéricos quedarán como tales, sea cualquiera su naturaleza, y se procesarán para exponerlos en forma clara y fácilmente asimilable, construyendo con ellos cuadros estadísticos, promedios generales y gráficos ilustrativos, de modo que se sinteticen sus valores y se puedan extraer enunciados teóricos de alcance más general.

Debemos tener presente que siempre es preferible cuantificar en lo posible los datos obtenidos. No hay ninguna oposición entre datos cuantitativos y datos cualitativos, pero si un diferente grado de precisión y de complejidad en cada variable medida, de forma que siempre es posible abstraer de ellas algunos aspectos cuantitativos en tanto que otros, por su complejidad, tendrían que permanecer como cualitativos.

Tras adoptar un criterio frente a cada categoría o subconjunto de datos podremos abordar, con mayor claridad acerca de nuestros objetivos, las tareas básicas del proceso.

En primer lugar será preciso hacer una revisión detallada de todos los datos obtenidos, atendiendo en especial a su coherencia y buscar sus posibles incongruencias, omisiones o errores, y enmendarlos si cabe hacerlo. Es decir, se revisará sistemáticamente toda la información disponible, juzgando su calidad y el grado de confianza que merece, para determinar qué parte puede incluirse en el informe de investigación, cual debe corregirse o modificarse en algo (acudiendo, llegado el caso, a una nueva recolección de

datos) y cual, por sus graves deficiencias, deberá ser excluida sin más. Este proceso se facilitará mediante la utilización del software adecuado (una simple hoja Excel puede ser suficiente).

Por cada tipo de datos se procederá entonces como sigue:

a) Los datos numéricos se procesarán agrupándolos en intervalos y se tabularán, lo que implica hacer tablas y/o listados de datos que los muestren agrupados y contabilizados. Para ello hay que contar cada una de las respuestas que aparecen, distribuyéndolas de acuerdo a las categorías o códigos previamente definidos.

Cada pregunta del cuestionario tendrá que ser tabulada independientemente, por lo que hay que hacer un plan de tabulación que prepare adecuadamente la tarea a realizar.

Luego se construirán con ellos cuadros estadísticos, calculándose además las medidas de tendencia central, de dispersión o de correlación que resulten necesarias.

Para cada cuadro que se haya obtenido será preciso evaluar el comportamiento de las variables que aparezcan en él, precisando la forma en que actúan individualmente. Luego se observarán las relaciones que pueden percibirse entre una y otra variable, si el cuadro es de doble entrada, tratando de precisar la forma en que una afecta a la otra. Cuando se trate de un cuadro de tres variables será conveniente examinar primero los valores totales, pues en ellos se ve el funcionamiento global de cada variable operando de modo independiente, para luego pasar a confrontar, por pares, las variables, tratando de detectar las influencias que existan entre ellas.

b) Caso de tener datos cualitativos, sufrirán una primera operación que se denomina codificación para poderlos presentar como numéricos. De allí en adelante se trabajarán al igual que los otros datos numéricos, mediante la tabulación y el procesamiento en cuadros estadísticos.

Adicionalmente, utilizaremos la representación gráfica, como una actividad derivada de la anterior que consiste en expresar visualmente los valores numéricos que aparecen en

las tablas y nos hace apreciar más rápidamente, los resultados. Su objeto es permitir una comprensión global, rápida y directa, de la información que aparece en cifras y sumamente útil por el valor de síntesis que tiene.

Tampoco es necesario presentar gráficamente toda la información obtenida en la investigación, pues ocuparía un espacio excesivo en el informe derivado, siendo lo más aconsejable el recurrir a este tipo de presentación con las informaciones más importantes y generales, teniendo en cuenta que podemos recurrir a muchas formas de representación tales como gráficos de barras, histogramas, escalas gráficas, etc.

Esta forma de visualización de los datos obtenidos también se lleva a efecto con el software elegido, que no sólo dibuja e imprime los gráficos deseados, sino que además realiza labores de cálculo que facilitan la presentación de los datos de la investigación.

Así pues, partiremos de un conjunto de datos en los que se supone se encuentra la información necesaria para desarrollar una parte de nuestra investigación.

Estos datos permitirán desarrollar las respuestas a unos interrogantes iniciales de la investigación o servirán, de un modo más limitado, para esclarecer ciertos puntos específicos que es preciso tener en cuenta.

Si al comparar los datos no hay ninguna discrepancia seria y si cubren todos los aspectos previamente requeridos, habrá que tratar de expresar lo que de ellos se infiere redactando una pequeña nota donde se sinteticen los hallazgos. Si, en cambio, se aportan ideas o datos divergentes, será preciso primeramente determinar, mediante la revisión del material, si se ha cometido algún error en la recolección. Si esto no es así habrá que ver si la discrepancia se origina en un problema de opiniones o posiciones contrapuestas o si, por el contrario, obedece a alguna manera diferente de categorizar los datos o a errores de las propias fuentes con que estamos trabajando.

En todo caso será conveniente evaluar el grado de confianza que merece cada fuente, teniendo en cuenta la coherencia de sus respuestas y cualquier información que pueda resultar de valor al respecto. Ya adoptada una posición frente a las discrepancias encontradas será el momento de pasar a registrar los hallazgos, nuestras opiniones personales y las conclusiones parciales, con lo cual estaremos en condiciones de pasar a la síntesis. Rojas, A. *et al* (2010)

2C.7 - Análisis de datos

De la información procesada dependerá que se puedan o no resolver las dudas iniciales formuladas en nuestro estudio. Pero, no obstante, esa información no nos habla por sí misma, no es capaz por sí sola de darnos las respuestas deseadas hasta que no efectuemos sobre ella un trabajo de análisis e interpretación.

Desde un punto de vista lógico, analizar significa descomponer un todo en sus partes constitutivas para su examen más detallado. La actividad opuesta y complementaria a ésta es la síntesis, que consiste en recomponer lo que el análisis ha separado, integrar todas las conclusiones y análisis parciales en un conjunto coherente que cobra pleno sentido al integrarse como un todo único. Lo dicho tiene aplicación directa en la metodología de investigación.

El análisis de los datos no es una tarea que se improvisa, como si recién se comenzara a pensar en él después de procesar todos los datos. Por el contrario, el análisis surge más del marco teórico trazado que de los datos concretos obtenidos y deberemos, como estudiosos del caso que nos ocupa, ser capaces de definir, con suficiente antelación, con qué datos habrá que rechazar o afirmar una hipótesis, y qué resultados indicarán una u otra conclusión. Esta actividad es fundamental para evitar sorpresas como la de encontrar que no tenemos suficientes datos al final del proceso, o de que los que poseemos no nos sirven para mucho.

Para desarrollar la tarea analítica hay que tomar cada uno de los datos o conjuntos homogéneos de datos obtenidos, e interrogarnos acerca de su significado, explorándolos y examinándolos mediante todos los métodos conocidos, en un trabajo que para obtener los mejores frutos hay que ser pacientes y minuciosos. De acuerdo al tipo de datos que se estén analizando se procederá de un modo u otro.

Con la síntesis e interpretación final de todos los datos ya analizados podemos decir que finaliza la investigación, aunque teniendo en cuenta que la misma, considerada como intento de obtención de conocimientos, es siempre una tarea inacabada, que debe continuar por fuerza con otras investigaciones concretas. La síntesis es, pues, la conclusión final, el resultado aparentemente simple pero que engloba dentro de sí a todo

el cúmulo de apreciaciones que se han venido haciendo a lo largo del trabajo. Las conclusiones finales sólo resultan pertinentes para responder al problema de investigación planteado cuando, en la recolección, proceso y análisis de los datos, se han seguido las directrices surgidas del marco teórico.

Para alcanzar este resultado se deben tomar en consideraciones todas las informaciones analizadas, utilizando para ello todos los hallazgos parciales que hemos hecho. En el caso de los cuadros estadísticos procederemos a comparar los hallazgos de cada cuadro con los otros que tienen relación con el mismo. Así iremos avanzando hacia conclusiones cada vez más generales, menos parciales.

Se podrán confeccionar cuadros-resumen, que sintetizen la información más importante que se halla dispersa en otros, para poder presentar un panorama más claro y se procederá entonces, a extraer las conclusiones finales, que reflejen el comportamiento global de las variables de interés. En función de ellas redactaremos nuestra síntesis de forma ordenada, precisa y escuetamente, anotando sólo lo esencial y numerando nuestras conclusiones correlativamente, teniendo presente nuestro planteamiento inicial.

A partir de ese momento, estaremos en condiciones de redactar el informe de la investigación.

2C.8 - Muestra

Cuando se recaba información a todas las personas que están involucradas en el problema en estudio este diseño adopta el nombre de “censo”. Los censos son casi siempre trabajos de envergadura, por las dificultades que implica su realización, que sólo pueden ser acometidos por organizaciones con grandes recursos. Son muy útiles pues obtenemos una información general de referencia, indispensable para casi cualquier trabajo de indagación social posterior. Pero, por la gran cantidad de personas a consultar, no es factible en ellos obtener información muy detallada, pues se convertirían en trabajos desproporcionadamente difíciles de ejecutar y analizar.

Si el tamaño del colectivo es demasiado grande, el investigador toma sólo una parte del mismo, de acuerdo con ciertas reglas de procedimiento, que se basan en la teoría de las probabilidades. Se emplean las “encuestas por muestreo”, donde escogemos, mediante procedimientos estadísticos, una parte significativa de la población, que se toma como objeto a investigar. Las conclusiones que se obtienen para este grupo se proyectan luego a la totalidad del universo con características similares, teniendo en cuenta los errores muestrales que se calculen para el caso. De esta forma las conclusiones obtenidas a partir de la muestra pueden generalizarse a toda la población en cuestión, con un margen de error conocido y limitado previamente por el investigador.

Para una mejor comprensión de los términos que vamos a utilizar, vamos a comenzar con cuatro definiciones básicas: Población o universo, muestra, fracción de muestreo y representatividad de la muestra.

a) Población o universo. Es el conjunto de individuos que componen el colectivo sobre el que se estudiará el fenómeno expuesto en el proyecto de investigación. Así, en nuestro caso, la población estará formada por todos los estudiantes (hombres y mujeres) de determinadas Escuelas y/o Facultades, de diferentes cursos. La delimitación exacta de la población es condición necesaria para el cumplimiento de los objetivos de la investigación. De manera convencional, la población se denomina con la letra N.

b) Muestra. Es el conjunto de individuos incluidos en la muestra mediante algún procedimiento de selección. Habitualmente se la designa con la letra n (unidad de muestreo). Es la unidad del universo que será incluida en la muestra.

c) Fracción de muestreo. Es la fracción (f) que relaciona el tamaño de la muestra con el tamaño de la población. En general: $f = n/N$.

d) Representatividad de la muestra. Grado en el cual la muestra reproduce las características de la población de la cual proviene. La mayor representatividad se logra, en términos generales, cuando las unidades de muestreo tienen igual posibilidad de formar parte de la muestra.

Cuando la muestra tiene más de 100 observaciones, se puede aplicar el teorema central del límite, según el cual los valores de las características observadas en la muestra siguen una curva de distribución normal (campana de Gauss). Esto permite hacer análisis de inferencia estadística en cuanto a la distribución de los valores de dicha variable en la población. James Stevens afirma que al menos son necesarios 15 casos por cada variable del modelo (Stevens, 2009), y Bentler (2006) dice que son necesarios al menos 5 casos por parámetro a estimar, siempre y cuando el comportamiento de las variables sea “bueno” (distribución normal, sin casos perdidos o aislados, etc.).

En nuestra investigación utilizaremos el tipo de muestra no probabilística (muestreo por conveniencia) entre estudiantes universitarios, pero que tiene la aleatoriedad de ser los alumnos de los grupos a los que se tiene mejor acceso, por lo que interviene un cálculo de probabilidades que hace posible la investigación. (Malhotra, 2004)

Este tipo de muestra conformará una estratificación en la que se conformarán grupos homogéneos internamente pero heterogéneos entre sí. El tamaño de la muestra vendrá dado por la fórmula:

$$n = \frac{k^2 \cdot p \cdot q \cdot N}{(\epsilon^2 \cdot (N-1)) + k^2 \cdot p \cdot q}, \text{donde:}$$

k: constante para definir el nivel de confianza de la muestra. Su valor dependerá del nivel que se pretenda dar, de acuerdo al cuadro que se detalla más abajo.

p: es la proporción de individuos que poseen las características de estudio. En este caso será de 0,5 por no saber fehacientemente y generar el caso más adverso.

q: es la proporción de individuos que no tienen la característica de estudio, es decir $1-p$.

N: es el número total de la población.

e: es el error muestral deseado, que se mide en porcentaje

Los valores más utilizados para relacionar el coeficiente **K** con la confianza pueden verse en la tabla 29.

Tabla 29 Valores de K más usados

Nivel de confianza (porcentaje)	80	85	90	95	95,5	99
Valor de K	1,28	1,44	1,64	1,96	2	2,58

Fuente: EP

2D - Fundamentos Estadísticos para nuestro estudio

Para facilitar la comprensión de los parámetros utilizados en los modelos de ecuaciones estructurales propuestos hemos observado que muchas investigaciones incluyen una descripción básica de los mismos, su formulación y tolerancias.

Se trata de una aclaración que, a modo de ayuda, colabora en la interpretación de las conclusiones que indican los resultados obtenidos, puramente matemáticos.

Hemos decidido seguir el ejemplo de esas publicaciones y, si ya hemos definido en apartados anteriores algunos conceptos sobre los parámetros que vamos a medir (tipos de variables, constructos, causalidad, etc.), a continuación vamos a describir las herramientas matemáticas sobre estadísticas básicas sobre las que pivota la presente tesis, comentando sucintamente los conceptos, las definiciones y márgenes de los indicadores estadísticos que conforman la teoría que sustenta el estudio.

A modo de ejemplo algunas de estas definiciones sobre conceptos generales pueden encontrarse incluidas en los manuales de teoría estadística de diferentes autores, algunos de los cuales ya han sido referenciados en otros apartados, tales como:

Peña y Romo (1997), Briones (2002), Díez (1992), Batista y Gallart (2000 y 2005), y Malhotra (2004), Alaminos (2005), Andrade y Coba (2006), Fernández (2006).

Lo mismo también en diversas tesis, como las de:

Conchado (2011), Fernández (2004), García (2011), González (2001), Gutiérrez (2008), Guzmán (2013), Hernández (2001), Llamas (2005), y Mejía (2005).

2D.1 - Medidas de tendencia central, dispersión y concentración

Las medidas de tendencia central son números calculados con fórmulas que representan a una serie de valores de una variable cuantitativa. Las medidas de desviación expresan la heterogeneidad u homogeneidad de esos valores. En esos casos, ambas medidas, como variables colectivas que son, caracterizan al colectivo en el cual se dan los correspondientes valores individuales. Por ejemplo, si un grupo tiene un promedio de edad de 15,5 años y otro, de 18,6, el primero se caracteriza por su menor edad respecto al segundo.

El modo (o moda) es el valor de una serie que se da con mayor frecuencia entre los miembros de un colectivo. Puede ser utilizado con variables nominales ya que basta contar los números de sujetos que hay en cada categoría de una variable, de ese tipo (por ejemplo, el número de hombres y el número de mujeres). Obviamente es muy fácil de determinar y por ello se le emplea como una primera medida de tendencia central.

La mediana es el valor que ocupa el lugar central de una distribución ordenada de valores, habitualmente en orden ascendente. Si el número de valores es impar, la mediana es el valor central. Si ese número es par, la mediana es la semisuma de los dos valores centrales. La mediana es una medida de tendencia central que está especialmente indicada para datos ordinales, como medición de actitudes. A diferencia de la media aritmética, que presentamos a continuación, no está influida por valores extremos muy altos o muy bajos que se pueden dar en una serie de valores.

La media aritmética es una de las medidas de tendencia central más usada para caracterizar a un colectivo mediante un sólo valor. Ese valor es la suma de los valores de una variable cuantitativa continua, de carácter intervalo o proporcional, dividida por el número de valores sumados.

La varianza y la desviación típica son medidas de dispersión o de variabilidad de los datos de una serie de valores. Indican su homogeneidad o heterogeneidad y, por tanto, la semejanza o diferencia que existe entre los individuos de un colectivo con relación a una cierta variable cuantitativa (la edad, el sexo, etc.). El índice de dispersión se aplica a variables ordinales y nominales.

La varianza es el promedio de las desviaciones elevadas al cuadrado de cada uno de los valores de una serie respecto de la media aritmética de ella. La desviación típica, a su vez, es la raíz cuadrada de la varianza.

Para determinar la concentración que puede tener una variable cuantitativa en un cierto colectivo se utiliza la diferencia de la variable entre quintiles extremos de la distribución. Consiste en dividir en quintiles el total de la población (grupos de 20% de ella), y con los valores de la variable que determinan esa división se calculan los totales de la variable que queda en cada grupo. El nivel de concentración se comprueba con la comparación de los valores que quedan en los quintiles extremos.

La forma más simple para determinar si existe asociación entre dos variables consiste en cruzar ambas variables con lo cual se obtiene un cuadro de $m \times n$ celdas o de $n \times n$ si las dos variables tienen el mismo número de categorías.

2D.2 - Análisis descriptivo inferencial: comparaciones en muestras

La comparación de valores en dos o más subgrupos de una población total es una tarea muy fácil. Por ejemplo, si en cada uno de esos subgrupos hemos calculado las medias aritméticas de una cierta variable, la comparación de los valores obtenidos se hace de manera directa. El mismo procedimiento se aplicaría si se tratara de proporciones, porcentajes, etc. La situación cambia cuando la comparación se hace en una muestra probabilística. En ese caso, hay que realizar pruebas especiales que permitan pronunciarnos sobre la significación estadística que pueda tener la diferencia encontrada entre los valores comparados. Así, si un grupo tiene un promedio de 26,4 y el otro un promedio de 25,1, debemos preguntarnos si esa diferencia también se da en la población de la cual extrajimos la muestra, pues la diferencia podría deberse al error de muestreo al cual están sometidas, probabilísticamente, todas las muestras que se toman de una población o universo.

Problemas como el anterior se resuelven con el uso de pruebas de significación estadística, que son propias para cada medida que se va a comparar. La secuencia del cálculo se expone a continuación:

1. Formulación de una hipótesis nula y de una hipótesis alternativa.

Como lo sugiere su nombre, la hipótesis nula plantea que en la población de la cual se extrajo la muestra no existe diferencia entre los valores de los subgrupos que se desean comparar (proporción, media aritmética, etc.). En este caso aceptar la hipótesis nula significa que NO rechazamos el modelo. Compararemos el valor de χ^2 (chi cuadrado)⁴⁸ que nos calcula el programa con el de la tabla chi cuadrado, teniendo en cuenta el nivel de confianza y los grados de libertad. Si la χ^2 que calcula el programa es menor que el valor que da la tabla, estamos en la región de aceptación y por ello aceptamos H_0 , lo que significa que no hay diferencias significativas (al nivel prefijado) entre nuestra teoría (el modelo) y los datos de la muestra. Sin embargo, como se supone que existe una diferencia (y pudimos haberlo expresado así en una de las hipótesis del estudio), formulamos una hipótesis alternativa que exprese que existe tal diferencia, que es estadísticamente significativa, y que se da en la población de la cual se extrajo.

⁴⁸ Chi cuadrado indica el parecido de las covarianzas observadas con las del modelo hipotético

2. Elección de una distribución de muestreo.

La mayoría de las medidas estadísticas utilizadas en el análisis de datos cuantitativos tienen distribuciones de probabilidad conocida, como también algunas de ellas tienen ese tipo de distribuciones para diferencias entre dos medidas. En cada caso, esas distribuciones indican la probabilidad de que un cierto valor encontrado en una muestra se pueda dar en su correspondiente población, o la probabilidad que una diferencia de una cierta magnitud pueda darse entre subgrupos tomados muestralmente en la misma población.

Para avanzar en el mismo tema, digamos que si se toman muchas muestras y en cada una de ellas se calcula una misma proporción, entonces, el total de las proporciones de esas muestras se distribuye en la forma de la curva normal. Por esta propiedad de la distribución de frecuencias, que también la tienen otras distribuciones muestrales como la que corresponde a la diferencia entre proporciones, sabemos que sólo un 5% de todas las proporciones, convertidas a puntajes sigmas queda más allá de 1,96 unidades sigmas: 2,5% son mayores y 2,5 % son menores. Es decir, la probabilidad de encontrar en una muestra una proporción cuyo valor sigma sea superior o inferior a 1,96 sigmas es del 0,05. En otras palabras, existe una probabilidad del 0,95 (o un nivel de confianza del 95%) que la proporción encontrada se aleje menos de 1,96 sigmas del medio de la distribución, que es el verdadero medio aritmético de la población. Dicho en forma aproximada, que la diferencia encontrada sea la que corresponda, probabilísticamente, al error de muestreo. Esta situación se representa en la figura 41, a continuación:

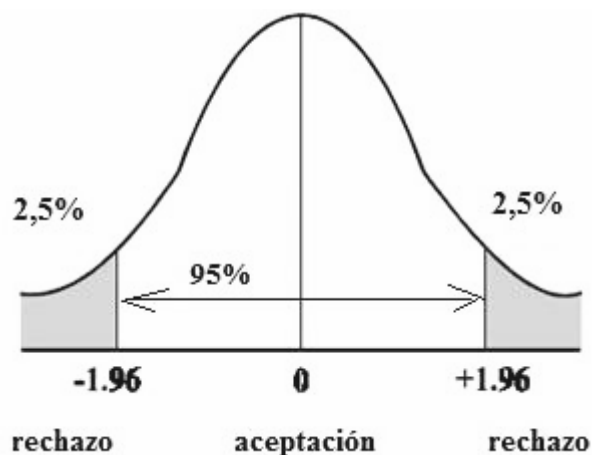


Fig. 41: Distribución normal, para el 95% de confianza - (EP)

No todas las medidas de las muestras de una población se distribuyen según la curva normal. Algunas de ellas lo hacen según la distribución de Student (t), la de chi cuadrado, etc.

3. Elección de un nivel de significación.

Las pruebas de significación estadística se basan en la teoría de las probabilidades. Cuando el investigador realiza una de estas pruebas se pregunta: ¿Cuál es la probabilidad que un valor encontrado en mi estudio sea por azar? Frente a esa pregunta hace una elección que define el riesgo probabilístico que tiene el aceptar su resultado. Podremos decir, por ejemplo, que ese valor, transformado a valores k puede darse al azar en un 5% de las veces. Tal porcentaje recibe el nombre de nivel de significación que, convencionalmente, se designa con la letra α (alfa).

Los siguientes valores de k en la tabla 30 definen áreas de la curva normal que comprenden proporciones o porcentajes de casos (valores de muestras) en ambos o en uno u otro lado de la curva normal, a partir de su media aritmética:

Tabla 30. Casos en ambos lados del área de la curva a partir de la media aritmética

Nivel de confianza (porcentaje)	90	95	99
Valor de K	1,64	1,96	2,58
Casos en los extremos	El 10% restante queda en los dos extremos, o zona de rechazo	El 5%...	El 1%...

Fuente: EP

Las terminaciones de la curva normal se denominan colas de la distribución. Cuando tenemos base para suponer que una de las medidas de las muestras por comparar es mayor o menor que la otra, entonces, esta situación se plantea en la hipótesis alternativa $X_1 > X_2$; o $X_1 < X_2$. En casos como éste, la prueba se denomina prueba de significación de una cola. Si no existe esa base, se utiliza una prueba de significación de dos colas, lo cual quiere decir que la diferencia en el universo puede ser mayor o menor, en términos probabilísticos, que la encontrada en el estudio. Tabla 31 y figura 42.

Tabla 31. Casos en uno de los extremos del área de la curva

Nivel de confianza (porcentaje)	95
Casos en los extremos (incluyendo “colas”)	En todo el resto del área de la curva normal queda el 95% de los casos

Fuente: EP

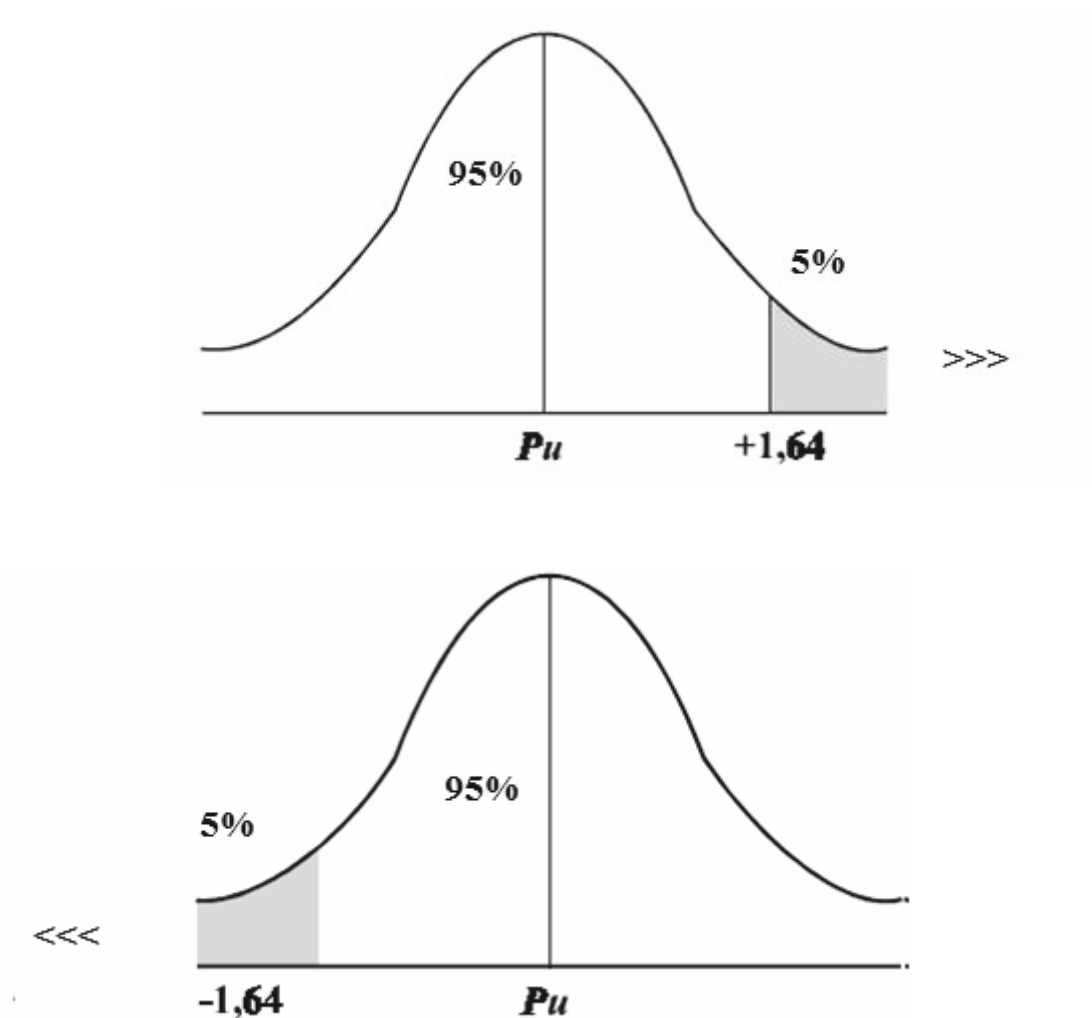


Fig. 42: Casos en uno de los extremos del área de la curva - (EP)

Respecto al nivel de significación, queremos recordar que un valor de z igual o inferior a 1,64 unidades sigma puede darse al azar un 5%; a la inversa, un valor superior a 1,64 significa que la probabilidad de darse al azar en las muestras de un universo es menor de 5%. Ese valor calculado decide la aceptación o rechazo de la hipótesis nula.

Como se trabaja con base en probabilidades, existe el riesgo de rechazar la hipótesis nula cuando es correcta, con lo cual se comete un error de tipo I. Este error se reduce cuando se baja el nivel de significación (por ejemplo, si elegimos un nivel del 1%, según el cual existe una probabilidad de 100 en que pueda cometerse ese tipo de error). Pero al hacer esto, se corre el riesgo de cometer el error de tipo II, es decir, aceptar la hipótesis nula cuando en efecto existe diferencia entre los grupos comparados.

4. Cálculo de la estadística de la prueba.

Para calcular el valor de z , de t o la estadística que corresponda a la distribución de muestreo existen fórmulas especiales. Ellas consisten en divisiones de la diferencia encontrada entre las muestras por el error estándar de esa distribución utilizando los datos del problema.

5. Aceptación o rechazo de la hipótesis nula.

Los valores de z , o t que puedan encontrarse en los cálculos anteriores se comparan con valores que están en tablas de los textos de estadística con las correspondientes probabilidades para el nivel de significación elegido. Cuando el valor calculado es mayor que el valor de la tabla, se rechaza la hipótesis nula y se acepta la hipótesis alternativa. Es decir, se acepta en términos probabilísticos, que existe una diferencia estadísticamente significativa (que no es la diferencia real que se da en el universo, pues las muestras tienen errores de muestreo). Si el valor calculado es menor que el valor de la tabla, para el nivel de significación elegido, entonces, se acepta la hipótesis nula, pues el valor encontrado puede darse al azar más veces que lo que nos permite el nivel de significación elegido: en otras palabras, no existe significación estadística entre los grupos comparados.

2D.3 - Análisis simple de la varianza

El análisis simple de la varianza con una sola variable de clasificación permite comparar dos, tres o más medias aritméticas de otras tantas submuestras definidas por las categorías de una cierta variable independiente elegida por el investigador en su estudio.

En el análisis de la varianza (llamado ANOVA, por las sigla en inglés: Analysis of Variance) se considera que la suma total de los cuadrados de las desviaciones de las medidas de su media aritmética correspondientes a varias submuestras tomadas de un cierto universo puede ser considerada como formada por dos partes: una suma de cuadrados correspondiente a las diferencias entre las medidas de cada grupo con su media aritmética, llamada suma de cuadrados dentro; y otra suma de cuadrados formada por las diferencias entre las medias aritméticas de los grupos y la media aritmética del total de las medidas, llamada suma de cuadrados entre.

Con esas sumas de cuadrados se hacen estimaciones de la varianza de todos los valores que se dan en el universo del cual provienen los grupos o submuestras utilizando los grados de libertad de las sumas de cuadrados mencionadas. Con esas estimaciones, a su vez, se determina el valor de la estadística F^{49} .

Muchos de los objetivos que se formulan en la investigación social suponen la relación entre dos o más variables, de naturaleza nominal u ordinal, o la correlación que se da entre dos variables de naturaleza intervalo o proporcional. En las relaciones entre variables ordinales, intervalos y proporcionales una de ellas es tomada como variable independiente y la otra como variable dependiente.

En la relación (sea una asociación o una correlación) de dos variables, relación bivariada, se consideran cuatro aspectos importantes:

1. La existencia o no de relación entre ellas, es decir, si al cambiar los valores de una de esas variables también hay cambios en la otra variable.

⁴⁹ La razón F, en ANOVA, es una relación de la variación entre muestras (por diferentes tratamientos) y la variación dentro de las muestras (por factores aleatorios).

2. El grado de la relación, su magnitud que, en general, se referencia con el valor máximo que puede tomar el coeficiente que mide la relación, (1).

3. Dirección de la relación, aspecto que se refiere a la forma de variar los valores de las dos variables. Si todas las veces que una de ellas aumenta de valor la otra también aumenta, se tiene una relación positiva. Si todas las veces que una de las variables aumenta de valor la otra disminuye, entonces se tiene una relación negativa.

4. Naturaleza de la relación. Se refiere a la forma que toma la representación de los valores de las dos variables. Si se da un aumento de los valores de una de las dos variables cuando también aumentan o disminuyen, de manera más bien uniforme los valores de la otra, tenemos relación lineal. Si el aumento o disminución de ambos valores se produce en los extremos (más con más y menos con menos) tenemos una relación curvilínea.

En la mayoría de las investigaciones cuantitativas, la determinación de relaciones cae dentro del análisis descriptivo. En otros casos, esa determinación puede ser la base de un análisis explicativo que plantea problemas particulares cuando se trabaja con datos no experimentales. En ese análisis, entre otras exigencias, el investigador debe mostrar no sólo la covariación de las variables implicadas en la relación, sino que una de ellas (la variable independiente) antecede a la otra en el tiempo y que esa relación no es espúrea, es decir, que la covariación no se debe a la influencia de otra variable que influye tanto en la variable que se ha tomado como independiente como en la variable tomada como dependiente.

2D.4 - Coeficiente de correlación de Pearson

Es uno de los coeficientes más utilizados para medir la correlación que pueda existir entre dos variables, cuando hay patrón de normalidad. Si no hay patrón normal se usa el coeficiente de Spearman, válido en ambos casos. Además del nombre de Pearson, recibe también el de momento producto y, en cuanto a la naturaleza de la covariación que mide, es un coeficiente de orden cero en cuanto que no controla el efecto que podrían producir otras variables en la correlación.

El coeficiente puede tomar valores entre + 1 y - 1. El primero se da cuando existe correlación positiva perfecta; el segundo, cuando hay correlación negativa perfecta (a mayor valor de una de las variables, menor valor proporcional de la otra).

2D.5 - Análisis de regresión simple

Supongamos que queremos saber si existe correlación entre variables (proporcionales) como también saber la magnitud de los efectos de la variable independiente sobre la variable dependiente y conocer un procedimiento para calcular el valor de esta última cuando se conocen los valores de la primera. La respuesta a la primera pregunta la obtenemos mediante la elaboración de un diagrama de dispersión en un eje cartesiano en el que, en el eje horizontal, se representan los valores de X y en el eje vertical los valores de Y. Las respuestas a las otras dos preguntas se verán a continuación de esta primera. De manera general, la correlación se puede expresar mediante una función matemática, que aquí recibe el nombre de ecuación de regresión, con la siguiente fórmula: $Y = a + bX$

Cuando la relación entre dos variables es total, a cada valor de X le corresponde un solo valor de Y. Sabemos, sin embargo, que en la realidad social se está muy lejos de darse esa situación. La ecuación de regresión que representa datos reales contiene un llamado término de error que suele indicarse con la letra “e”: $Y = a + bX + e$

En la ecuación el término a se denomina intercepto e indica el punto en el cual la recta de regresión corta el eje de las Y. En tal punto el valor de X es cero. El término b se denomina pendiente de la recta que indica, por su lado, el número de unidades de cambio que se produce en Y cada vez que X varía en una unidad. Cuando b es negativo, la pendiente es decreciente ya que al aumentar el valor de X disminuye el correspondiente valor de Y, y viceversa. En otras palabras, la correlación entre ambas variables es negativa.

La regresión se usa como técnica predictiva, esperando que la recta de regresión explique al máximo la relación entre la variable dependiente o explicada y las independientes o explicativas.

El análisis de regresión trabaja con ciertos supuestos o condiciones de las cuales se destacan las siguientes:

1. Las variables independientes y las variables dependientes deben estar medidas en escalas de intervalo o de razón (variables cuantitativas continuas).

2. Los valores de la variable dependiente deben estar normalmente distribuidos en la población de la cual proceden.
3. Los valores del término de error tienen una distribución normal.
4. Los valores del término de error no están correlacionados con los valores de la variable independiente.
5. Las desviaciones estándar de los valores de la variable dependiente que corresponden a cada valor de la variable independiente son iguales entre sí. Esta condición recibe el nombre de supuesto de homocedasticidad.

Cuando se cumplen los supuestos anteriores es posible obtener buenos estimadores de los parámetros a y b en la población a partir de sus correspondientes valores en la muestra. En particular, el supuesto de la distribución normal del término de error apoya la posibilidad de efectuar pruebas de significación con relación a los parámetros mencionados.

Por su lado, el supuesto de homocedasticidad también se relaciona con las pruebas de significación: su violación puede significar que tales pruebas no sean válidas. Si se tuviera constancia que existe esa violación, es decir, que se produce una condición de heterocedasticidad, debería utilizarse un procedimiento de ajuste de menores cuadrados ponderados.

Con toda la importancia que se debe dar a los supuestos señalados, se ha demostrado empíricamente que las estadísticas F y t que se utilizan en las pruebas de significación dentro del análisis de regresión son suficientemente fuertes para soportar desviaciones a algunos de ellos.

2D.6 - Análisis multivariado

Hemos visto diversas técnicas de análisis para tratar datos obtenidos de una o de dos propiedades (variables) que se dan en un colectivo de personas. Con todo el valor que tienen esos tipos de análisis, en muchas ocasiones debido a la complejidad de los fenómenos sociales, es indispensable considerar las relaciones simultáneas que se dan entre tres o más variables mediante uno o más de los procedimientos que constituyen el análisis multivariado. Algunas de sus técnicas determinan el efecto de una serie de variables independientes sobre una variable dependiente.

Es importante destacar que, en algunas investigaciones, el análisis multivariado da una explicación del fenómeno que se estudia, al tener en cuenta un mayor número de variables que en el análisis descriptivo y haciendo la distinción necesaria entre las causas y los efectos que se dan en el conjunto de los datos tomados de la realidad en sus expresiones cuantitativas. Por esta razón, el análisis que pueda cumplir esta función se denomina análisis explicativo. Debería tenerse muy en cuenta que la explicación no resulta de meras cifras obtenidas con el tratamiento de los datos, sino que deben estar comprendidas en algún marco teórico que les dé el adecuado sentido conceptual.

Veremos varias técnicas multivariadas, para tener una primera aproximación a un área de la metodología cuantitativa de especial importancia en la investigación social, dentro de las consideraciones hechas en el párrafo anterior. En particular, nos referiremos a las siguientes técnicas: regresión múltiple y análisis de senderos.

2D.7 - Regresión múltiple

La regresión múltiple es la extensión de la regresión bivariada por la incorporación de más de una variable independiente. El modelo se expresa con la siguiente fórmula en la cual los términos contenidos en ella tienen las mismas significaciones que en la fórmula simple:

$$Y = a_0 + b_1 x_1 + b_2 x_2 + b_3 x_3 + \dots + b_n x_n$$

Los coeficientes beta en la regresión múltiple están constituidos por coeficientes parciales lo cual significa que el coeficiente de una variable particular indica su efecto en la variable dependiente una vez que se han controlado los efectos de las otras variables sobre esa misma variable dependiente. Desde luego, el valor de cada coeficiente indica la importancia que tiene en la variación de Y y, por lo tanto, en la predicción que se haga de esta variable para distintos valores de X.

Cuando las distintas variables independientes están medidas en escalas diferentes, los coeficientes betas deben transformarse en ponderaciones betas mediante su estandarización.

2D.8 - Análisis de trayectorias

En un ámbito más estadístico, pero que igualmente involucra un conjunto de ecuaciones lineales de varias variables, podemos plantear relaciones entre variables de interés, dotarlas de direcciones lógicas y evaluar la fuerza de tales asociaciones, lo que caracteriza al método conocido como “path analysis”. En estos modelos las variables observables son equiparadas con las latentes y solo existe el modelo de relaciones estructurales. El análisis de senderos es, por ahora, el modelo más utilizado para probar conjuntos de supuestos causales entre variables que se dan en un estudio (Kline, 2005).

Si el modelo constituido por el investigador se ajusta a los datos recogidos, el modelo se mantiene para ser sometido a nuevas pruebas o, en caso contrario, modificarlo o cambiarlo por otro nuevo. Pero en todo caso, el análisis de senderos no es un procedimiento para demostrar la existencia de causalidad, en forma definitiva.

El análisis de senderos fue desarrollado por el genetista Wright (1921). Posteriormente fue introducido en las Ciencias Sociales por Blalock (1967), Boudon (1965) y Duncan (1966). En general, es una aplicación del análisis de regresión múltiple que agrega, a los supuestos básicos de éste, otros tres nuevos:

- a) Las variables que se incluyen en el modelo causal deben tener un orden derivado de una cierta teoría,
- b) El modelo debe ser considerado como un sistema cerrado en cuanto contiene explícitamente todas las variables importantes en la determinación causal.
- c) El modelo debe ser recursivo, es decir, la influencia de una variable en otra es asimétrica, o sea, se ejercita en una sola dirección causal.

El análisis de senderos se inicia con un diagrama, basado en una teoría, en el cual se señalan, por medio de flechas, las relaciones de influencias sobre las variables. Las correlaciones de orden cero entre variables no influidas por otras se indican con líneas de doble flecha o con líneas cortadas. En las terminales de una o más flechas se señalan, con otras flechas, influencias residuales que, como en el análisis de regresión, no están correlacionadas, por definición, con las variables a las que apuntan. Cuando se han

hecho cálculos, en los senderos o flechas se indica la contribución que cada variable hace en la otra, cuando los efectos de las otras han sido controlados, mediante coeficientes de senderos (path coefficients) y correlaciones de orden cero para variables no relacionadas con otras.

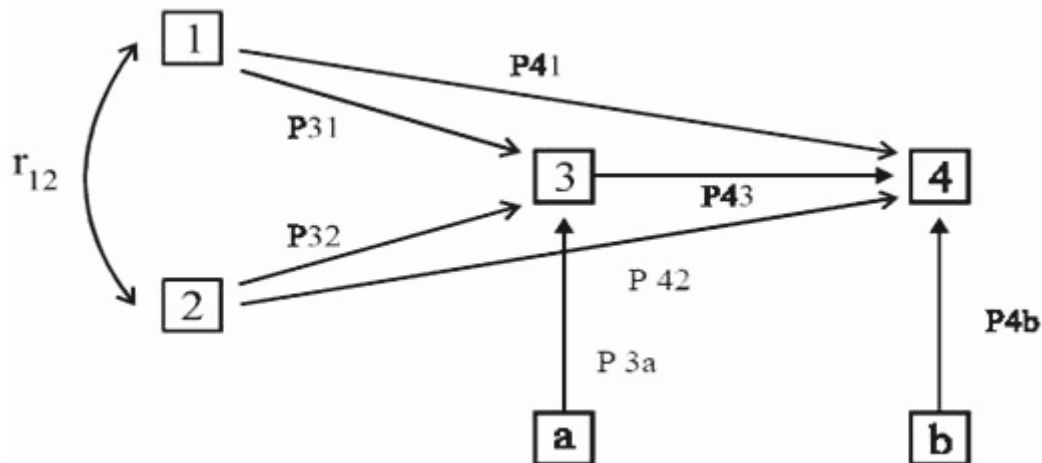


Fig. 43: Diagrama de senderos

Fuente: Briones (2002)

Las variables 1 y 2 son exógenas. La correlación entre ellas se anota en la figura 43 con una línea curva, con flechas en ambos extremos, con la cual se indica que ninguna de ellas es la causa de la otra. La correlación r_{12} no se analiza en el sistema.

Las variables 3 y 4 son endógenas. Como puede verse, estas variables pueden ser tomadas como dependientes de otra u otras y como independientes respecto de otra. Es el caso de la variable 3.

Las variables a y b son residuales. Indican el efecto de variables no incluidas en el modelo. O sea, se reconoce que el conjunto de variables que componen el modelo no da cuenta de toda la variación de las variables (3 y 4 en la figura 43). Se supone que las variables residuales no están relacionadas entre sí ni con las variables exógenas.

En el análisis de senderos se distinguen efectos directos e indirectos de unas variables sobre otras. Así, en la figura 43, vemos que, por ejemplo, la variable 1 tiene un efecto

directo sobre las variables 3 y 4. Pero también un efecto indirecto sobre la 3 y la 4 a través de su correlación con la 2 y de ésta por sus efectos sobre ambas variables (3 y 4).

Sobre la variable 4 se dan efectos indirectos a partir de la 1 y pasando por 2 y por 3. Las variables 1 y 2 son tomadas como causa de la 3, pero esta variable no puede ser tomada como causa de la 4. Los modelos no recursivos admiten causación recíproca.

Los programas de ordenador para análisis de senderos permiten calcular tanto los coeficientes de senderos y los efectos directos como los efectos indirectos totales sobre una determinada variable. Puede suceder que tales efectos indirectos sean mayores que los directos, lo cual quiere decir que el efecto de una variable sobre otra se ejercita a través de correlaciones con otras.

El análisis de senderos trabaja con los siguientes supuestos:

- 1) No existe correlación entre las variables residuales con las variables exógenas.
- 2) La causalidad es recursiva.
- 3) Las correlaciones entre las variables son lineales y aditivas. Es decir, se excluyen relaciones curvilíneas y de interacción (multiplicativas).
- 4) Las varianzas de las distribuciones de las variables endógenas del modelo son iguales (supuesto de homocedasticidad).
- 5) Existe baja multicolinealidad entre las variables.
- 6) El nivel de medición debe ser intervalo. Sobre este supuesto puede decirse que la introducción de datos ordinales no plantea problemas en la mayoría de los casos.
- 7) Las variables independientes están medidas sin error.

2D.9 - Coeficientes de senderos (path coefficients)

El coeficiente de sendero indica el efecto directo de una variable tomada como causa sobre otra variable tomada como dependiente. Se representa con la letra P, con dos subíndices: el primero representando el efecto a la variable dependiente y el segundo, la causa o variable independiente (P_{ji}, efecto directo de la variable *i* sobre la variable *j*).

Los coeficientes de senderos son iguales a las ponderaciones o pesos betas (b*) o coeficientes estandarizados de las ecuaciones de regresión. Así, como ejemplo, el coeficiente:

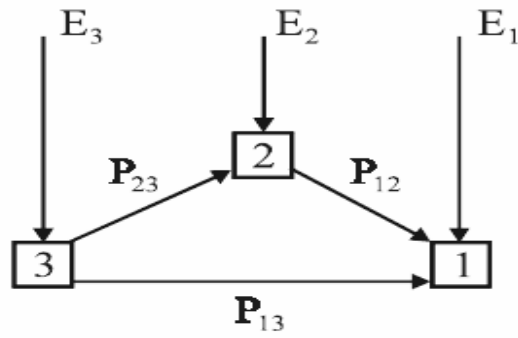
$$P_{31} = \frac{r_{13} - r_{12} \cdot r_{23}}{1 - r_{12}^2} = b_{31.2}^*$$

Los coeficientes residuales indican la variación no explicada sobre una determinada variable dependiente. En el diagrama P_{3a} sería:

$$P_{3a} = \sqrt{1 - R_{3.12}^2}$$

donde R² es el cuadrado del coeficiente de correlación múltiple de las variables involucradas.

Para cierto modelo, hay unas ecuaciones por resolver con los datos del problema que se llama sistema de ecuaciones estructurales (sistema de ecuaciones de regresión). En la figura 44, el sistema sería el que se indica más abajo, de tal modo que las E son las variables residuales:



$$\begin{aligned}
 x_3 &= E_3 \\
 x_2 &= P_{23}x_3 + E_2 \\
 x_1 &= P_{13}x_3 + P_{12}x_2 + E_1
 \end{aligned}$$

Fig. 44: Ecuaciones de regresión 1
 Fuente: Briones (2002)

En general, con n variables, la estimación de los correspondientes coeficientes de senderos requiere (n-1) ecuaciones estructurales.

Cuando por alguna razón considerada por el investigador, una relación se omite en un modelo recursivo, equivale a darle el valor cero al respectivo coeficiente.

2D.10 - Criterio de los mínimos cuadrados

Conocido como OLS, por sus siglas en inglés (Ordinary Least Squares). Cuando se tiene un conjunto de puntos en un diagrama de dispersión es posible hacer pasar por ellos varias rectas. Sin embargo, debemos elegir aquella que mejor se ajusta a los datos. Para hacer esta elección se utiliza el criterio general denominado de los mínimos cuadrados según el cual la suma de los cuadrados de las desviaciones de los valores reales de Y a la línea es mínima. Según esto, si se trazan líneas verticales de cada uno de los puntos a la línea de los mínimos cuadrados y si se elevan al cuadrado esas distancias y se las suma, la suma resultante será menor que otra suma de cuadrados posible de trazar, por lo que minimizamos el error y será mayor la varianza explicada de la variable dependiente. Figura 45.

Para trazar la línea de los mínimos cuadrados, se necesita computar los coeficientes a y b de la ecuación de regresión, valores que determinan la línea con la propiedad señalada

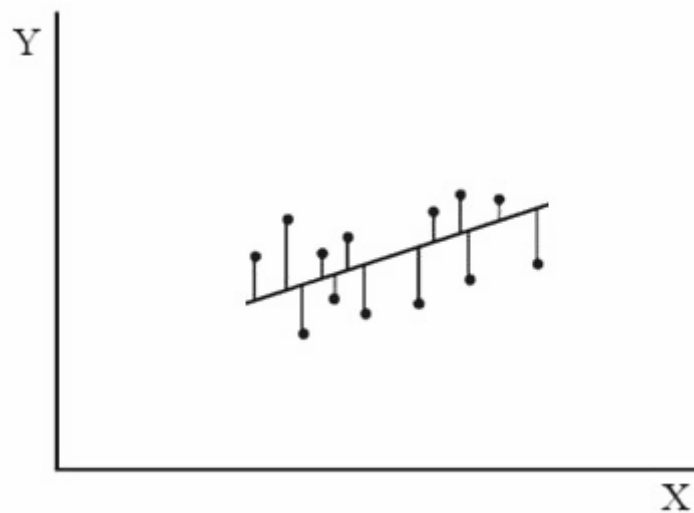


Fig. 45: Ajuste de regresión - (EP)

2D.11 - Análisis factorial

En muchas situaciones podemos estudiar relaciones entre dos tipos de variables:

- a) Aquellas observables que son medibles de modo objetivo (edad, sexo, salario...) o subjetivo (actitudes, percepciones, etc.), y
- b) Aquellas no-observables (latentes o factoriales) que corresponden a conceptos teóricos cuantificables sólo como constructo a partir de algunas variables observables (inteligencia, por ejemplo).

Con el análisis factorial exploratorio extraemos los factores que, a partir de correlaciones significativas entre variables, decimos que en teoría miden el mismo constructo (Kim y Mueller, 1978). Se asume que las correlaciones indican la presencia de la variable latente que explica esas correlaciones entre las variables medidas (Carroll, 1985; Gorsuch, 1988).

Los modelos de análisis factorial confirmatorio solo contienen el modelo de medida y las relaciones entre las variables latentes solo pueden ser de tipo correlacional. Se presupone la existencia de una teoría que trata de probarse contrastándola con los datos.

En los resultados del análisis factorial realizado con SPSS debemos tener en cuenta la importancia de la información aportada por los dos conceptos siguientes:

- Comunalidades, que indica que, aunque cada variable dé el 100% de información, cada factor nos dice lo que cada variable representa en ese factor. Es el porcentaje en el que cada variable representa a sus variables originales. Es una prueba de la calidad de los factores que utilizamos para representar a las variables. Las de valor inferior a 0,5 son candidatas a eliminarse.
- Componentes principales, con las que salen los factores y seleccionamos los que explican un porcentaje alto. Cada uno incluye todas las variables. La matriz de componentes da una combinación de las variables de sus componentes. Cada variable es una combinación lineal de los factores, aunque ninguna esté representada al 100%. Indica qué variables pertenecen “más” a cada factor

En algunas ocasiones nos podemos encontrar con variables observables que tienen altas correlaciones con más de un constructo, lo que dificulta conocer su influencia. Esta situación se corrige aplicando los métodos de rotación que tanto Gorsuch (1988) como Kim y Mueller (1978) explican al considerar que la rotación coloca, desde una perspectiva geométrica, a las variables medidas más cercanas a los factores que las explican, facilitando la comprensión de las relaciones entre observadas y latentes.

2E - Características de los modelos de ecuaciones estructurales

Los modelos de ecuaciones estructurales se caracterizan por dos elementos:

1. Estimación de relaciones de dependencias múltiples y cruzadas, y
2. La capacidad de representar conceptos no observados en estas relaciones, teniendo en cuenta el error de medida en el proceso de estimación.

La diferencia más observable entre los sistemas de ecuaciones estructurales y las otras técnicas de análisis multivariante es la capacidad de analizar relaciones para cada subconjunto de variables. Además de permitir interrelaciones entre algunas variables de estos subconjuntos.

Los sistemas de ecuaciones estructurales permiten, además de estimar relaciones múltiples que fortalecen las correlaciones utilizadas, introducir conceptos o variables independientes al análisis. De esta manera se pueden realizar estimaciones más precisas de los coeficientes estructurales.

Los modelos estructurales proponen una relación causal entre variables observadas y latentes, y después miden la covarianza de tales mediciones para observar:

- a) si el modelo observado ajusta con el modelo propuesto, y
- b) la fuerza y dirección de las variables resultantes. (Huerta, 2010)

2E.1 - Estrategias de modelización

La flexibilidad de los sistemas de ecuaciones estructurales permite utilizar la técnica de múltiples formas, en función de los objetivos a conseguir. Sin embargo, hay que seleccionar al inicio de la investigación la estrategia a seguir para alcanzar nuestro propósito.

En ese sentido, hay tres estrategias para adoptar en la utilización de sistemas de ecuaciones estructurales:

1. La estrategia de modelización confirmatoria, donde el investigador especifica un modelo aislado y el modelo de ecuaciones estructurales se utiliza para evaluar su significación estadística.
2. La estrategia de modelos rivales, permite evaluar el modelo estimado con modelos alternativos. En muchas ocasiones el investigador se encuentra con modelos alternativos para representar una misma situación sin conocer cuál proporciona un nivel de ajuste mejor. Esta estrategia proporciona las líneas básicas para realizar esta comparación y seleccionar el más idóneo; y
3. La estrategia de desarrollo del modelo, que difiere de las dos anteriores estrategias en que aunque se propone un modelo, el propósito del esfuerzo de modelización es mejorarlo a través de modificaciones de los modelos de medida y/o estructurales. Seguir esta estrategia es para re especificar el modelo básico de teoría para encontrar uno nuevo.

En nuestro caso, utilizaremos el primer modelo para asegurar la validez y coherencia de los constructos establecidos para las distintas fases de nuestro análisis pero profundizaremos en su posible desarrollo. Lo que nos ayudará a descubrir la posible existencia de constructos latentes (factores de primer orden) vinculados con un constructo común a dichos factores, obteniéndolo a través de un Análisis Factorial Confirmatorio de segundo orden (Mikulic, Muiños, 2005).

2E.2 - Fases de un modelo de ecuaciones estructurales

En la figura 46 se resumen las distintas fases en la obtención de un modelo de ecuaciones estructurales. Comienza con la definición de un modelo teórico que se intentará contrastar estadísticamente y acaba verificando parcial o totalmente el modelo.

La falta de confirmación de una o varias hipótesis establecidas en la elaboración del modelo de ecuación estructural nos hace modificarlo, manteniendo un significado lógico además de una significación estadística. Esa modificación implica repetir todo el análisis estadístico. El proceso de análisis acaba cuando se consigue un modelo con un nivel de ajuste, global o parcial, igual o superior al establecido por el investigador.

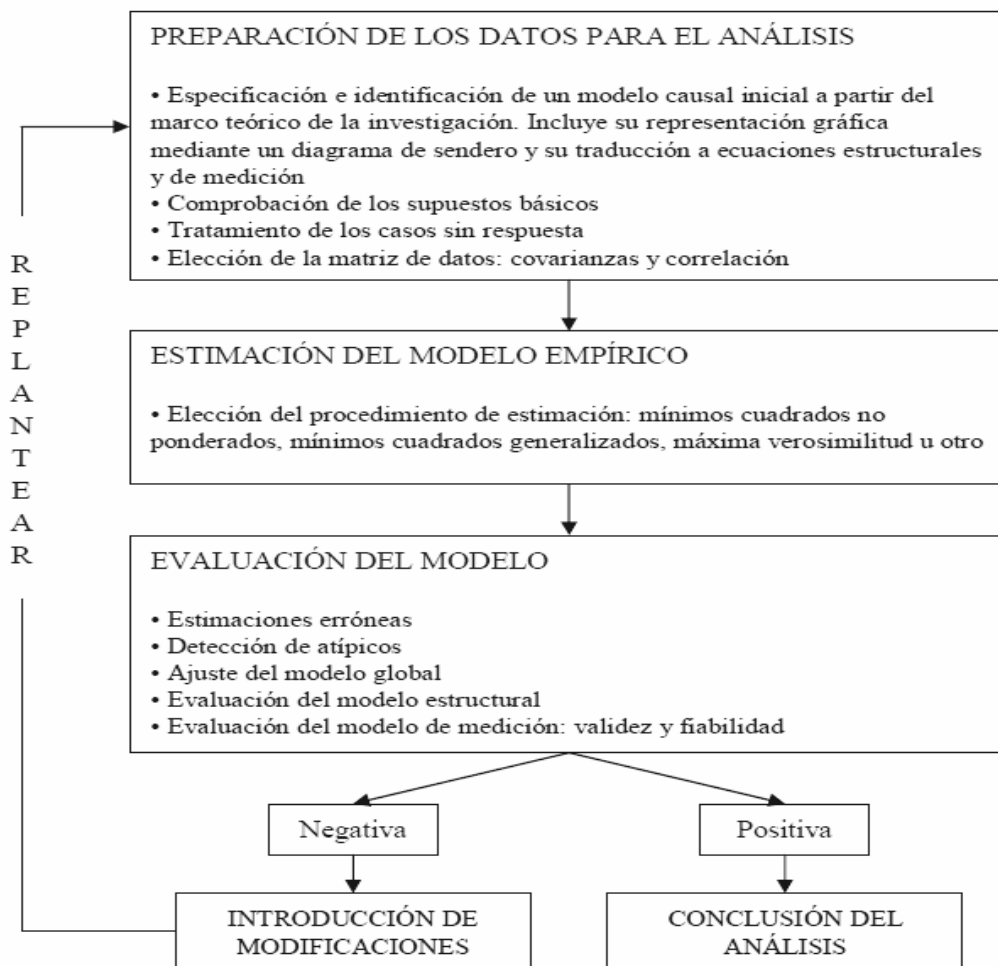


Fig. 46: Fases de obtención de un modelo de ecuaciones estructurales

Fuente: Fernández (2004)

La modelización de ecuaciones estructurales se fundamenta en relaciones causales, en las que el cambio en una variable se supone que produce un cambio en otra variable. Se encuentra este tipo de enunciado cuando se define una relación de dependencia, tal y como se encuentra en el análisis de regresión. Las relaciones causales pueden tomar muchas formas y significados, desde la estricta causación encontrada en los procesos físicos, tales como una reacción química, a las relaciones menos definidas encontradas en la investigación del comportamiento. La seguridad y la convicción con la que asumimos la causación entre dos variables no descansan en los métodos analíticos escogidos sino en la justificación teórica ofrecida por los análisis.

El problema de error de especificación, caracterizado por la omisión de una o más variables predictivas claves, es el más crítico en el desarrollo de modelos de fundamentación teórica. La consecuencia de omitir una variable significativa consiste en sesgar la evaluación de la importancia de otras variables.

2E.3 -Resumen y conclusiones de utilización de Ecs. Estructurales

La utilidad de los modelos de ecuaciones estructurales para el investigador social radica en la aportación de una visión global de los aspectos del fenómeno estudiado, en contraposición a otro tipo de herramientas estadísticas que se centran en el análisis individual de cada factor. Asimismo, reducen la cantidad de información que debe ser analizada, ya que su fundamento es agrupar las relaciones entre un gran número de variables en unos pocos factores, manifestando los aspectos esenciales de la situación explicada. En el caso del estudio de constructos o variables no medibles directamente, estos modelos tienen el inconveniente de que el investigador debe proceder a la explicación objetiva de relaciones causales entre variables que se caracterizan por su abstracción y subjetividad.

En lo que respecta al estudio de la causalidad, la función de los modelos de ecuaciones estructurales no es corroborar las relaciones causales entre las distintas variables, sino facilitar su análisis y toma de decisiones, para lo cual es necesario un análisis exploratorio de los datos y que el proceso de modelización sea seguido con rigor. En ocasiones la confirmación de un modelo de este tipo se ha considerado como una prueba de validez, sin tener en cuenta que podrían ser igualmente válidos otros modelos alternativos, puesto que las pruebas de significación sólo son efectivas cuando se cumplen las condiciones especificadas.

Los modelos de ecuaciones estructurales surgieron como necesarios para conseguir mayor flexibilidad en los modelos de regresión. Según Bollen,; *“Podemos mirar estos modelos de diversos modos. Son ecuaciones de regresión con supuestos menos restrictivos, que permiten errores de medida tanto en las variables criterio (independientes) como en las variables dependientes. Consisten en análisis factoriales que permiten efectos directos e indirectos entre los factores. Habitualmente incluyen múltiples indicadores y variables latentes. Resumiendo, engloban y extienden los procedimientos de regresión, el análisis econométrico y el análisis factorial.”* (Chamorro, 2005: 378)

Para conocer mejor estos términos y verificar la necesidad de los modelos de ecuaciones estructurales, debemos revisar los conceptos sobre las relaciones entre variables y las metodologías para establecerlas.

Las relaciones causales entre variables pueden establecerse con una metodología experimental o no experimental. La primera se desarrolla en las ciencias físicas o químicas, puesto que existe un conocimiento de los fenómenos que permite demostrar que toda variación en la variable causa produce un cambio en la variable efecto.

En las Ciencias Sociales y del comportamiento el conocimiento teórico es escaso, no existe la experimentación y de lo único que se dispone es de información estadística.

Esto es, en los estudios no experimentales las relaciones causales se inducen a partir de las relaciones estadísticas observadas entre las variables, y la variación entre variables se mide, como es sabido, con la covarianza o la correlación. Pero la covariación entre dos variables significa que los valores de una se dan a menudo asociados a valores de la otra, sin embargo para que exista relación causal, además de existir correlación, los cambios en la variable causa implicarán variaciones en la variable efecto.

La correlación entre variables es una relación simétrica. Si "x" tiene un tipo de correlación, positiva o negativa, con "y", entonces "y" tiene el mismo tipo de correlación con "x".

Sin embargo, la causalidad es asimétrica, pues si "x" es causa de "y", no se deduce que "y" sea causa de "x". La causalidad implica una dirección del efecto.

Si representamos la relación causal de "x" en "y" mediante una ecuación de regresión lineal de la forma $y = bx + \varepsilon$, el término ε expresa la variación de "y" por causas distintas de "x", es decir por causas de perturbación aleatorias. Entonces para inducir que "x" sea causa de "y" se exige además de correlación, que se dé la dirección del efecto y el aislamiento de otras posibles causas.

En la investigación no experimental (Ciencias Sociales y del comportamiento), se descartan situaciones en las que la causalidad se dé en las dos direcciones. En cuanto al aislamiento, en los casos no experimentales, se usa el control estadístico, exigiendo la incorrelación entre el término de perturbación aleatoria y las variables explicativas. Mateos-Aparicio (2011).

Una vez recordados estos términos aclaratorios, podemos decir que los modelos de ecuaciones estructurales constituyen una de las herramientas más potentes para el estudio de las relaciones causales sobre datos no experimentales cuando estas relaciones son lineales. Sin embargo, hay que tener en cuenta que estos modelos no prueban de una forma definitiva la causalidad, aunque desechen las relaciones co soportadas em píricamente hablando; es decir, pueden negar una causalidad pero no afirmarla. Podemos rechazar las teorías causales si se contradicen con los datos pero no se pueden confirmar estadísticamente. (Batista y Gallart, 2000).

El Análisis de la Varianza pensado inicialmente para el análisis de datos experimentales, trata de explicar el efecto de una variable independiente (explicativa) sobre otra variable dependiente (explicada), y establece hasta qué punto la variación de la variable dependiente se debe a las variaciones de la variable independiente. Entre los diversos modelos estadísticos diseñados para explicar la variación de una o varias variables dependientes, esto es, para el análisis de relaciones de dependencia, está el modelo de regresión, que tiene en común con el Análisis de la Varianza el analizar la variación de las variables explicadas por otras.

En Ciencias Sociales, los econometras han sido los pioneros en el uso de modelos de análisis de dependencia para estudiar la causalidad con datos no experimentales, el concepto de modelo de estructura fue definido por Koopman (1949). El término estructural supone que los parámetros no son simplemente medidas descriptivas de asociación sino que revelan una relación causal.

En las ciencias del comportamiento, los primeros psicómetras de principios del siglo XX desarrollaron modelos para estudiar variables abstractas, no observables, llamadas constructos, variables latentes o factores, cuyos valores se obtienen a partir de las variables observables.

Por otro lado, sociómetras y biómetras sentaron las bases del Análisis Path (análisis de rutas) que describe relaciones de dependencia que, en algún sentido son causales, entre variables latentes. El análisis de rutas es un método para buscar relaciones causa efecto, en las que los coeficientes path miden el grado de relación causal entre las variables, es decir, el grado de variación producida en la variable dependiente por cada una de las variables independientes, permaneciendo las otras constantes.

El Análisis Path es el antecedente de los modelos de ecuaciones estructurales, es una técnica útil para estimar los parámetros desconocidos de un sistema de ecuaciones simultáneas.

De la conjunción de planteamientos, del Análisis Factorial, que dio lugar a lo que llamamos modelo de medida, que relaciona variables latentes con variables observadas en las de ecuaciones estructurales, y el Análisis Path, con el que se establecen las relaciones entre variables latentes, que ahora llamamos modelo de estructura, se dedujo la base de los modelos de ecuaciones estructurales, en los que se incorpora el error de medida y las relaciones entre variables latentes.

Los modelos de ecuaciones estructurales, como marco general permiten afirmar una dirección en las relaciones entre las variables, y también incorporan las variables no observables, es decir, los factores.

2E.4 - Prueba de chi cuadrado

La prueba de chi cuadrado (χ^2) se utiliza para determinar si existe asociación o no, en términos probabilísticos, en un cuadro de contingencia (el cruce de dos variables) obtenido con datos de una muestra. La magnitud de la asociación se calcula con el coeficiente de contingencia que evalúa el ajuste general del modelo de medición.

El valor de χ^2 representa una medida preliminar de la diferencia registrada por el procedimiento entre el modelo de medición y la estructura de covarianza observada en los datos. Para este valor, se espera obtener un mínimo de diferencia, que no resulte estadísticamente significativo. Esto implica que no hay diferencia apreciable entre el modelo propuesto y los datos empíricos. Si la diferencia resulta estadísticamente significativa, el resultado se toma como base para el cálculo de otros índices de ajuste.

2E.5 - Coeficiente de ajuste comparativo (CFI)

Este índice compara los valores de discrepancia de χ^2 para dos casos: la discrepancia del modelo hipotetizado, y la discrepancia de un modelo teóricamente posible (llamado modelo de independencia), en el que todas las relaciones entre variables son nulas. Es decir, este índice compara la estructura de covarianzas del modelo de medición con una situación hipotética donde no existe relación alguna entre las variables observadas.

Los valores del CFI oscilan entre 0 y 1. Cuando el CFI toma valores que exceden 0.90 se considera que existe ajuste razonable entre el modelo y los datos (Bentler, 1990)

$$CFI = 1 - \left[\frac{(\chi^2_{Model} - df_{Model})}{\chi^2_{Indep} - df_{Indep}} \right]$$

2E.6 - Error Medio Cuadrático de Aproximación (RMSEA)

El índice de bondad de ajuste más robusto es el *Error Medio Cuadrático de Aproximación* (RMSEA, por sus siglas en inglés). Este índice ha sido desarrollado como una medida absoluta de la diferencia de la estructura de relaciones entre el modelo propuesto y los valores de covarianza en la población medida (Steiger, 1990).

Su cálculo es como sigue:

$$RMSEA = \sqrt{\frac{\bar{\delta}_M}{df_M (N - 1)}}$$

En este caso el término proviene de la medida inicial de diferencia entre los datos y el modelo:

$$\bar{\delta}_M = \max(\chi_M^2 - df_M, 0)$$

Lo anterior significa que el valor mayor de discrepancia entre el modelo y los datos observados se obtiene a partir del término con mayor valor, ya sea χ^2 , menos los grados de libertad del modelo, o bien cero. La importancia de este índice radica en que refleja una diferencia absoluta entre el modelo propuesto y los datos observados, tomando en cuenta el número de estimaciones y el tamaño de la muestra implicada por el modelo bajo prueba. Es muy importante notar que este índice, debido a su origen y propiedades estadísticas, compara el modelo con la estructura de relaciones entre las variables en la población. Por debajo de 0.1 indican un error aceptable y alrededor de 0.06 un muy buen ajuste entre datos y modelo (Hu y Bentler, 1999).

2E.7 - Coeficiente de ajuste normalizado (NFI)

El índice NFI (Normed fit index) de Bentler-Bonett se define mediante:

$$\text{NFI} = \Delta_1 = 1 - \frac{\hat{C}}{\hat{C}_0} = 1 - \frac{\hat{F}}{\hat{F}_0}$$

Donde $\hat{C} = n\hat{F}$ es la discrepancia mínima del modelo evaluado y $\hat{C}_0 = n\hat{F}_0$ es la mínima discrepancia del modelo base, de referencia.

Toma valores entre 0 y 1. Por encima de 0,90 indican muy buen ajuste entre los datos y el modelo teórico. Bentler & Bonett (1980).

ANEXO A – Codificación x pregunta

Variables explicativas:

Perfil usuario

Variables latentes:

(actitudinales)

Actuación

Interés

Confianza

Ansiedad

Utilidad

(aptitudinales)

Conocimientos

*** La variable Actuación sobre seguridad se forma desde los siguientes ítems:

back ups:

- frecuencia
- Localización

accesos:

- protección
- wi fi

mails:

- recepción
- envío

info:

- vulnerabilidades
- virus
- privacidad

redes sociales:

- registro
- perfil
- uso

ANEXO A1 - Primer cuestionario piloto, con comentarios resaltados

Cuestionario global de la encuesta:

Edad:

Sexo (hombre = H, mujer = M): **Modificar alternativa. Difícil discernir si escribieron H o M**

A continuación, marcar lo que proceda:

Vas a curso por año	
o arrastras alguna asignatura de cursos anteriores	
o arrastras varias asignaturas de otros cursos	

El ordenador que utilizo habitualmente es un sobremesa	
El ordenador que utilizo habitualmente es un portátil	

Algunos utilizan los dos

5. Me conecto a internet:

todos los días , casi continuamente (Iphone, tablet PC...)	
o cada día , en varias ocasiones a lo largo del día (puesto de trabajo, en casa...)	
o varios días a la semana (3, 4 ó 5 días)	
o una o dos veces a la semana	
u ocasionalmente	

6. Respecto a contraseñas:

uso diferentes contraseñas para cada acceso (PC, ficheros, aplicaciones ...)	
o bien tengo una password común para la mayoría de esos accesos	
o no establezco contraseñas	

7., siguiendo con contraseñas, si las establezco:

suelo mantener fijas las contraseñas	
o bien cambio las contraseñas anualmente	
o cambio las contraseñas cada 2 ó 3 meses	
o con mayor frecuencia	

dejo que el navegador grabe la contraseña, (por facilidad vs) para ir más rápido	
uso contraseñas fáciles de recordar (nombres o iniciales, matrículas, DNI, fechas de aniversario, teléfonos,...)	
uso reglas mnemotécnicas	
uso contraseñas con mezcla de letras, números, signos de puntuación...	

Algunos marcan varias opciones

9. Respecto la frecuencia de copias de seguridad de mis datos

No las he hecho nunca	
Las hago cuando cambio de ordenador	
Las hago cada año	
Las hago cada 6 meses	
Las hago con una frecuencia programada (semanal, quincenal o mensual)	

10. Respecto donde guardo las copias de seguridad de mis datos

Algunos marcan varias opciones

Ya he dicho que no las suelo hacer	
Las almaceno en otra carpeta del disco interno del sistema	
Las guardo en CD's o DVD's o pendrives	
Las guardo en un disco externo	
Las almaceno en la propia red (apls. de Cloud Computing)	

11. Mientras hago mis trabajos...

Algunos marcan varias opciones

No hago copias de seguridad, tengo confianza en el sistema	
Hago una copia cuando lo he terminado	
Hago una copia cada vez que me paso varias horas, actualizándolo	
Hago una copia tras cada actualización, por breve que sea	
Tengo un sistema automático de actualización	

12. Protejo el acceso a mi PC y/o a ficheros del mismo a través de:

Algunos marcan varias opciones

No necesito esas protecciones, se trata de mi PC	
Utilizo una password para acceder a la sesión	
Utilizo la ocultación de ficheros	
Utilizo claves para acceder a los ficheros	
Utilizo sistemas biométricos	

13. Cuando recibo un mail de remitente desconocido...

Lo abro para enterarme de lo que pretenden	
Abro los posibles archivos para examinar su contenido	
Guardo los posibles archivos para examinarlos más tarde	
Lo marco como spam	
Lo elimino directamente	

14. Me entero de las últimas vulnerabilidades en seguridad a través de: Algunos marcan varias opciones

No suelo mostrar interés	
Webs personalizadas (compañías de sw, inteco, ministerios...), revistas técnicas	
Avisos de la Universidad	
Correo electrónico	
Compañeros, amigos	

(*) En relación con el uso de internet, dirías que usas internet para...

15	Información sobre noticias de actualidad	
16	Formación	
17	Comunicarme (correo, foros, chats...)	
18	Compra-venta	
19	Transacciones bancarias	
20	Información de ofertas comerciales	
21	Entretenimiento: multimedia (vídeos, música online, con Youtube, Spotify..)	
22	Entretenimiento: lectura (descarga de libros)	
23	Entretenimiento: juegos on-line	
24	Intercambio de archivos	
25	Tengo un blog y lo actualizo ocasionalmente	
26	Tengo un blog y lo actualizo con frecuencia	
27	Otras formas de entretenimiento (<i>especificar</i>)	

(*) Has hecho, o sueles hacer, compras a través de internet de...

28	Viajes (billetes, hoteles, alquiler de coches...)	
29	Entradas de espectáculos (cine, teatro, conciertos....)	
30	Adquisición de libros, ropa, electrónica...	
31	Adquisiciones domésticas (alimentación, hogar...)	
32	Otros tipos de compra	

(*) se pueden marcar varias casillas en cada tabla

Seguridad en las TICs: Separar en bloques /Algunas se quedan en blanco, NS/NC

		Si	No
33	Me gusta hablar con otros de seguridad		
34	Si tuviera oportunidad me inscribiría en cursos de seguridad		
35	Siento curiosidad por las noticias sobre seguridad		
36	Saber seguridad incrementa mis posibilidades de navegar tranquilo		
37	Me da una gran satisfacción poder resolver dificultades de seguridad		
38	Si me lo propongo llego a dominar bien la seguridad		
39	Estudiar sobre seguridad me resulta difícil		
40	Estoy preocupado por los riesgos de seguridad		
41	Me altero cuando tengo que resolver un problema de seguridad		
42	Me siento incapaz de comprender algunas cuestiones sobre seguridad		
43	Es complicado seguir las instrucciones sobre seguridad		
44	Pienso que la seguridad es muy necesaria para mi actividad personal		
45	Pienso que la seguridad es muy necesaria para mi actividad profesional		
46	Pienso que saber de seguridad es de lo más importante de la informática		
47	Creo que los conocimientos sobre seguridad deben ser previos al uso de PC's		
48	Pienso que debo saber utilizar los recursos de protección de mi PC		
49	Creo que debo saber utilizar los recursos de protección al acceder a internet		
50	Usando Wi-fi en casa uso clave para el acceso		
51	Usando Wi-fi en casa noto que, a ratos, varía la velocidad		
52	Cada vez que inicio sesión con mi PC debo introducir mi password		
53	En alguna ocasión he tenido problemas con algún virus		
54	Tengo activo un antivirus actualizado con regularidad		
55	Tengo activo un firewall actualizado con regularidad		
56	Elimino periódicamente los archivos temporales y cookies almacenados en mi PC tras navegar por internet		
57	Borro el Histórico de páginas visitadas o he determinado que almacene las correspondientes el mínimo tiempo posible		
58	Cuando envío un mail a varios destinatarios, utilizo la copia oculta		
59	Cuando envío un mail a varios destinatarios, direcciono a todos directamente para que sepan a quien se lo he enviado		
60	Un usuario con conexión ADSL debe preocuparse por la seguridad		
61	Es seguro hacer compras en línea		
62	Cuando accedo a mi correo y navego por la red a través de un enlace inalámbrico en sitio público (hotel, cafetería, aeropuerto...), estoy en riesgo		
63	Cuando uso Wi-fi en la conexión en mi domicilio, estoy en riesgo		
64	Al usar Wi-fi en la conexión en el centro de trabajo/estudio, estoy en riesgo		
65	El símbolo del candado que se ve en los sitios más serios de e-commerce cuando doy los datos de mi tarjeta, me permiten hacer pagos seguros		
66	Algunos programas informáticos de malware son inofensivos		
67	La mayoría de los virus se diseñan para eliminar archivos y/o perjudicar nuestro sistema operativo y/o acceder a información confidencial		
68	Los virus solo se propagan por determinadas actuaciones de los usuarios		
69	Un virus puede mutar y recombinarse con otros originando nuevos virus		
70	Casi todos los usuarios pueden formar parte de redes zombi		
71	Los troyanos y el phishing persiguen resultados similares		
72	Algunos programas de adware (ejecución inmediata de publicidad) hacen un seguimiento de las prácticas del usuario y acaban siendo spyware		

Respecto las Redes sociales...

73. Con referencia a la dedicación:

estoy conectado todos los días , casi continuamente	
o me conecto cada día , en varias ocasiones a lo largo del día,	
o me conecto varios días a la semana (3, 4 ó 5 días)	
o una o dos veces a la semana	
u ocasionalmente	
o no soy usuario (<i>finalizas la encuesta</i>)	

74., si soy usuario, me di de alta impulsado por: **Algunos marcan varias opciones**

novedad, estar “a la última”	
recomendado por algunos amigos, para comunicarnos	
encontrar nuevas relaciones	
observar, ver lo que se dice	
otras razones (<i>especificar</i>)	

75. Con referencia a las condiciones de registro

Me las leí en su totalidad y las acepté	
Acepté sin leerlas, entendiendo que son estándar	
Las acepté sin leerme la totalidad de los extremos incluidos	
Las leí con posterioridad	
Tras haberme dado de alta, al leerlas, cancelé la cuenta	
No me di de alta porque no me gustaron	

76. Respecto a la privacidad del usuario

Las acepté tal cual vienen, pues son las más usadas	
Las acepté previamente y, cuando me familiaricé, las adapté	
Como no se adaptaban a lo que quería, no me di de alta	
Las investigué y los aspectos más relevantes los adapté a mis gustos	
Las investigué y adapté a mis gustos en su totalidad	

(*) Respecto tu actividad

77	Suelo subir imágenes (fotos , vídeos)	
78	Suelo subir composiciones personales (dibujos, música, textos)	
79	Suelo expresarme libremente manifestando mis aficiones (deportes, cine, música , lecturas ...)	
80	Suelo expresarme libremente manifestando mis puntos de vista (políticos, religiosos, sexuales...)	

(*) **En este tipo de foro, no tengo inconveniente en**

81	Usar mi verdadero nombre	
82	Incluir mis datos (fotografía, dirección, teléfono, profesión, curriculum, hobbies, edad, lista de amigos...) en mi perfil	
83	Suelo compartir (vs Comparto) fotos/vídeos de acontecimientos (fiestas, viajes, bodas, cumpleaños...)	
84	Suelo invitar (vs Invito) a conocidos nuevos a que se den de alta y así seguir la relación	
85	Los suelo usar tanto para el ámbito familiar como el laboral o de amistad	
86	Tengo identidades diferentes para según qué tipo de relación	
87	No participo activamente, simplemente observo	

Finalmente, para contestar al último grupo de preguntas, se utilizará la escala de A a E para responder a cada línea propuesta, donde:

A=no estoy dado de alta,

B=me di de alta pero no accedo,

C=accedo alguna vez, (1 – 2 días /semana)

D=accedo con frecuencia, (de 3 a 5 días /semana) y

E=me conecto continuamente, (a diario)

88	Facebook	
89	Flickr	
90	Linkedin	
91	Tuenti	
92	MySpace	
93	Twitter	
94	Messenger	
95	Otras (especificar)	

Algunos ponen cruces, acostumbrados a los tipos de respuesta anteriores

ANEXO A1.1 - Resultados análisis primer cuestionario piloto

A. factorial

Comunalidades^a

	Inicial	Extracción
Int1	1,000	,813
Int2	1,000	,623
Int3	1,000	,824

Método de extracción: Análisis de Componentes principales.

Varianza total explicada^a

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción
	Total	% de la varianza	% acumulado	Total
1	2,260	75,347	75,347	2,260
2	,520	17,350	92,697	
3	,219	7,303	100,000	

Matriz de componentes^{a,b}

	Componente
	1
Int1	,902
Int2	,789
Int3	,908

Análisis de fiabilidad

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,835	3

A. factorial

Comunalidades^a

	Inicial	Extracción
Ans1	1,000	,732
Ans2	1,000	,684
Ans3	1,000	,751
Ans4	1,000	,461
Ans5	1,000	,320

Método de extracción: Análisis de Componentes principales.

Varianza total explicada^a

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción
	Total	% de la varianza	% acumulado	Total
1	1,815	36,295	36,295	1,815
2	1,134	22,678	58,974	1,134
3	,944	18,876	77,849	
4	,563	11,267	89,116	
5	,544	10,884	100,000	

Matriz de componentes^{a,b}

	Componente	
	1	2
Ans1	,585	,624
Ans2	,731	-,387
Ans3	,579	-,645
Ans4	,648	,205
Ans5	,428	,370

Análisis de fiabilidad

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,552	5

A. factorial

Comunalidades^a

	Inicial	Extracción
Ans2	1,000	,670
Ans3	1,000	,575
Ans4	1,000	,349

Varianza total explicada^a

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción
	Total	% de la varianza	% acumulado	Total
1	1,594	53,122	53,122	1,594
2	,851	28,367	81,489	
3	,555	18,511	100,000	

Matriz de componentes^{a,b}

	Componente
	1
Ans2	,818
Ans3	,758
Ans4	,591

Análisis de fiabilidad

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,559	3

A. factorial

Comunalidades^a

	Inicial	Extracción
Ut1	1,000	,852
Ut6	1,000	,944
Ut2	1,000	,547
Ut4	1,000	,626

Método de extracción: Análisis de Componentes principales.

Varianza total explicada^a

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción
	Total	% de la varianza	% acumulado	Total
	1	1,925	48,114	48,114
2	1,045	26,115	74,229	1,045
3	,701	17,523	91,753	
4	,330	8,247	100,000	

Matriz de componentes^{a,b}

	Componente	
	1	2
Ut1	,766	-,514
Ut6	,410	,881
Ut2	,740	-,019
Ut4	,789	,060

Análisis de fiabilidad

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,626	4

ANEXO A2 - Segundo cuestionario piloto

Cuestionario global de la encuesta:

1. Edad:

(A continuación, marcar lo que proceda)

2.	Hombre	Mujer
Sexo:	<input type="checkbox"/>	<input type="checkbox"/>

3.

Vas a curso por año	<input type="checkbox"/>
o arrastras alguna asignatura (1 ó 2) de cursos anteriores	<input type="checkbox"/>
o arrastras varias asignaturas (3 ó más) de cursos anteriores	<input type="checkbox"/>

4. Me conecto a internet:

Todos los días, casi continuamente (Iphone, Tablet PC, Ipad...)	<input type="checkbox"/>
o en varias ocasiones a lo largo del día (puesto de trabajo, en casa...)	<input type="checkbox"/>
o varios días a la semana (3, 4 ó 5 días)	<input type="checkbox"/>
o una o dos veces a la semana	<input type="checkbox"/>
o ocasionalmente	<input type="checkbox"/>

5. Respecto a contraseñas:

No establezco contraseñas	<input type="checkbox"/>
o bien tengo una password común para la mayoría de accesos	<input type="checkbox"/>
o uso diferentes contraseñas para cada acceso (PC, ficheros, aplicaciones ...)	<input type="checkbox"/>

6., siguiendo con contraseñas, si las establezco:

suelo mantener fijas las contraseñas	<input type="checkbox"/>
o bien cambio las contraseñas anualmente, aproximadamente	<input type="checkbox"/>
o con mayor frecuencia (periodos inferiores a 6 meses)	<input type="checkbox"/>

7.

dejo que el navegador grabe la contraseña	<input type="checkbox"/>
uso contraseñas fáciles de recordar (nombres o iniciales, matrículas, DNI, fechas de aniversario, teléfonos, direcciones...)	<input type="checkbox"/>
uso contraseñas con mezcla de letras, números, signos de puntuación.....no descriptivos de la opción anterior	<input type="checkbox"/>

8. Respecto la frecuencia de copias de seguridad de mis datos

No las he hecho nunca	
Las hago cuando cambio de ordenador	
Las hago cada año, seleccionando manualmente los ficheros	
Las hago cada 6 meses aproximadamente, seleccionando manualmente los ficheros	
Las hago de forma programada con un sistema automático	

9. Respecto donde guardo las copias de seguridad de mis datos

Ya he dicho que no las suelo hacer	
Las almaceno en otra carpeta del disco interno del sistema	
Las guardo en CD's o DVD's, pendrives o discos externos	
Las almaceno en la propia red (apls. de Cloud Computing)	

10. Mientras hago mis trabajos...

No hago copias de seguridad, tengo confianza en el sistema	
Hago una copia cuando lo he terminado	
Hago una copia tras cada actualización	
Tengo un sistema automático de actualización	

11. Protejo el acceso a mi PC y/o a ficheros del mismo a través de:

No necesito esas protecciones, se trata de mi PC	
Utilizo una password para acceder a la sesión	
Utilizo claves para los distintos accesos (PC, ficheros...)	

12. Cuando recibo un mail de remitente desconocido...

Lo abro para enterarme de lo que pretenden	
Abro los posibles archivos para examinar su contenido	
Guardo los posibles archivos para examinarlos más tarde	
Lo marco como spam	
Lo elimino directamente	

13. Me entero de las últimas vulnerabilidades en seguridad a través de:

No suelo mostrar interés	
Compañeros, amigos	
Webs personalizadas (compañías de sw, inteco, ministerios...), revistas técnicas	
Avisos de la Universidad	

14. En relación con el uso de internet, dirías que usas internet para Información sobre noticias de actualidad, Formación, Comunicarme (correo, foros, chats...), Compra-venta, Transacciones bancarias, Información de ofertas comerciales, Entretenimientos multimedia (escuchar / ver vídeos, música online, películas, descarga de libros...)...

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

15. En relación con el uso de internet, dirías que usas internet para Entretenimiento multimedia (subir vídeos, música), participar en juegos on-line, tengo un blog actualizado, soy usuario de wikis....

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

16. Has hecho, o sueles hacer, compras a través de internet de viajes (billetes, hoteles, alquiler de coches...), entradas de espectáculos (cine, teatro, concierto....), adquisición de libros, ropa, electrónica, alimentación, hogar....

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

Respecto las Redes sociales...

17. Con referencia a la dedicación:

estoy conectado casi continuamente	
o me conecto en varias ocasiones a lo largo del día	
o me conecto varios días a la semana (3,4 ó 5)	
o una o dos veces a la semana	
u ocasionalmente	
o no soy usuario (<i>finalizas la encuesta</i>)	

18., si soy usuario, me di de alta impulsado por:

novedad, estar “a la última”	
recomendado por algunos amigos, para comunicarnos	
encontrar nuevas relaciones	
observar, ver lo que se dice	
otras razones (<i>especificar</i>)	

19. Con referencia a las condiciones de registro

Acepté sin leerlas, entendiendo que son estándar	
Las acepté previamente y, cuando me familiaricé, las adapté a mi perfil	
Estudí los aspectos más relevantes y, tras adaptarlos a mis gustos, las acepté	
Me las leí y, tras adaptarlas a mis gustos en su totalidad, las acepté	
No me di de alta porque no me gustaron	

En este tipo de foro,

		Si	No
20	Soy usuario de Facebook, Twitter, Tuenti...en ámbitos familiar y de amistad		
21	Soy usuario de LinkedIn, Facebook, ...en ámbito profesional		
22	Limito determinados accesos a mi información		
23	Tengo identidades diferentes para según qué tipo de relación		
24	No participo activamente, simplemente observo		

25. Respecto tu actividad, usas tu verdadero nombre e incluyes tus datos (fotografía, dirección, teléfono, profesión, curriculum, edad, lista de amigos...) en tu perfil, y te expresas libremente manifestando tus aficiones (deportes, cine, música, lectura....)

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

26. Compartes fotos/vídeos de acontecimientos personales (fiestas, viajes, bodas, cumpleaños...) así como composiciones propias (dibujos, música, textos, diseños...)

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

27. Te expresas libremente manifestando tus puntos de vista sobre asuntos políticos, religiosos, relaciones familiares, de amistad, laborales, sexuales...

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

Seguridad en las TICs:

		Si	No
28	Me gusta hablar con otros de seguridad		
29	Si tuviera oportunidad me inscribiría en cursos de seguridad		
30	Siento curiosidad por las noticias sobre seguridad		
31	Saber seguridad incrementa mis posibilidades de navegar tranquilo		
32	Me alegra poder resolver dificultades de seguridad		
33	Adopto suficientes medidas de seguridad		
34	Estoy preocupado por los riesgos de seguridad		
35	Me altero cuando tengo que resolver un problema de seguridad		
36	Me siento incapaz de comprender algunas cuestiones sobre seguridad		
37	Pienso que la seguridad es muy necesaria para mi actividad personal		
38	Pienso que la seguridad es muy necesaria para mi actividad profesional		
39	Creo que los conocimientos sobre seguridad deben ser previos al uso de PC's		
40	Creo que debo saber utilizar los recursos de protección al acceder a internet		
41	Usando Wi-fi en casa uso clave para el acceso		
42	Cada vez que inicio sesión con mi PC debo introducir mi password		
43	Tengo activo un antivirus actualizado con regularidad		
44	Tengo activo un firewall actualizado con regularidad		
45	Elimino periódicamente los archivos temporales y cookies almacenados en mi PC tras navegar por internet		
46	Borro el Histórico de páginas visitadas o he determinado que almacene las correspondientes el mínimo tiempo posible		
47	Cuando envío un mail a varios destinatarios, algunas veces utilizo la copia oculta		
48	Cuando envío un mail a varios destinatarios, algunas veces direcciono a todos de forma abierta para que sepan a quien se lo he enviado		

49	Un usuario con conexión ADSL debe preocuparse por la seguridad		
50	Una conexión inalámbrica con cifrado WEP tiene la misma seguridad que una conexión a través de cable		
51	Cuando uso Wi-fi en la conexión en mi domicilio, estoy en riesgo		
52	Al usar Wi-fi en la conexión en el centro de trabajo/estudio, estoy en riesgo		
53	El símbolo del candado que se ve en los sitios más serios de e-commerce cuando doy los datos de mi tarjeta, me permiten hacer pagos seguros		
54	Algunos programas informáticos de malware son inofensivos		
55	La mayoría de los virus se diseñan para eliminar archivos y/o perjudicar nuestro sistema operativo y/o acceder a información confidencial		
56	Un virus puede mutar y recombinarse con otros originando nuevos virus		
57	Casi todos los usuarios pueden formar parte de redes zombi		
58	Los troyanos y el phishing persiguen resultados similares		
59	Algunos programas de adware (ejecución inmediata de publicidad) hacen un seguimiento de las prácticas del usuario y acaban siendo spyware		

ANEXO A2.1 - Resultados análisis segundo cuestionario piloto

Constructo “Atracción”, observado a través de las preguntas 28, 29 y 30, y que en el primer ejercicio piloto nos daba una alfa de 0,835, por lo que no cambiamos nada, obtenemos ahora:

Correlaciones

		At1	At2	At3
At1	Correlación de Pearson	1	,744**	,302
	Sig. (bilateral)		,000	,112
	N	29	29	29
At2	Correlación de Pearson	,744**	1	,318
	Sig. (bilateral)	,000		,092
	N	29	29	29
At3	Correlación de Pearson	,302	,318	1
	Sig. (bilateral)	,112	,092	
	N	29	29	29

** . La correlación es significativa al nivel 0,01 (bilateral).

Con una fiabilidad:

Estadísticos de fiabilidad

	Alfa de Cronbach basada en los elementos tipificados	N de elementos
Alfa de Cronbach	,721	3

Mejorable hasta:

Estadísticos total-elemento

	Media de la escala si se elimina el elemento	Varianza de la escala si se elimina el elemento	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
At1	1,45	,542	,654	,559	,482
At2	1,31	,579	,677	,564	,460
At3	1,24	,833	,332	,111	,852

Con el análisis factorial obtengo:

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,577
Prueba de esfericidad de Chi-cuadrado aproximado		24,190
Bartlett	gl	3
	Sig.	,000

Donde vemos que la variable At3 es menos significativa, pero válida:

	Inicial	Extracción
At1	1,000	,797
At2	1,000	,807
At3	1,000	,344

Método de extracción: Análisis de Componentes principales.

Y con las otras dos variables se explica el 91% de la varianza.

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,947	64,906	64,906	1,947	64,906	64,906
2	,797	26,575	91,481			
3	,256	8,519	100,000			

Método de extracción: Análisis de Componentes principales.

De hecho, ya vimos que la correlación de At3 con las otras dos es menor y que, incluso eliminándola, subía el alfa de Cronbach hasta 0,852.

En resumen, definitivamente hay que dar por buena la redacción de las preguntas que nos llevan a esos resultados.

Constructo “Confianza”,

Tras los primeros análisis descubrimos que la redacción de la pregunta 33 podía sugerir las mismas respuestas para alumnos tanto “celosos” como “pasotas” respecto la variable latente “Confianza” en la seguridad.

De hecho, excepto uno, los demás entre los que consideraban que no adoptaban suficientes medidas de seguridad se manifestaban preocupados por ese constructo.

Y, por otra parte, también había una mayoría que consideraba que si adoptaba suficientes medidas entre el resto de los que también se preocupaban.

Para mantener la coherencia habrá que redactarla como “prefiero”, o “me gusta”, adoptar las máximas medidas de seguridad.

Tabla de contingencia Conf1 * Conf2 * Conf3

Recuento

			Conf2		Total
			0	1	
Conf3 0	Conf1	0	1	0	1
		1	0	10	10
	Total		1	10	11
1	Conf1	0	2	2	4
		1	3	11	14
	Total		5	13	18
Total	Conf1	0	3	2	5
		1	3	21	24
	Total		6	23	29

Las correlaciones entre las respuestas a las tres preguntas nos dan:

Matriz de correlaciones inter-elementos

	Conf1	Conf2	Conf3
Conf1	1,000	,443	-,169
Conf2	,443	1,000	-,224
Conf3	-,169	-,224	1,000

donde observamos que las respuestas a la pregunta 3ª van con signo diferente a las otras.

La fiabilidad obtenida, eliminando esa variable:

Estadísticos total-elemento

	Media de la escala si se elimina el elemento	Varianza de la escala si se elimina el elemento	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
Conf1	1,41	,323	,175	,201	-,565 ^a
Conf2	1,45	,328	,104	,219	-,391 ^a
Conf3	1,62	,458	-,232	,056	,613

a. El valor es negativo debido a una covarianza promedio entre los elementos negativos, lo cual viola los supuestos del modelo de fiabilidad. Puede que desee comprobar las codificaciones de los elementos.

El análisis factorial nos confirma el diferente signo que aporta la variable:

Matriz de componentes^a

	Componente
	1
Conf1	,785
Conf2	,814
Conf3	-,546

Si modificamos las respuestas de la 3ª variable, cambiándoles el signo, obtenemos:

Correlaciones

		Conf1	Conf2	Conf3
Conf1	Correlación de Pearson	1	,443 [*]	,169
	Sig. (bilateral)		,016	,382
	N	29	29	29
Conf2	Correlación de Pearson	,443 [*]	1	,224
	Sig. (bilateral)	,016		,243
	N	29	29	29
Conf3	Correlación de Pearson	,169	,224	1
	Sig. (bilateral)	,382	,243	
	N	29	29	29

*. La correlación es significativa al nivel 0,05 (bilateral).

Con una fiabilidad:

Estadísticos de fiabilidad

	Alfa de Cronbach basada en los elementos tipificados	N de elementos
Alfa de Cronbach	,517	3

En este caso, con el análisis factorial obtenemos:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,564
Prueba de esfericidad de Chi-cuadrado aproximado		7,226
Bartlett	gl	3
	Sig.	,065

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,577	52,561	52,561	1,577	52,561	52,561
2	,870	29,011	81,572			
3	,553	18,428	100,000			

Método de extracción: Análisis de Componentes principales.

**Matriz de
componentes^a**

	Componente
	1
Conf1	,785
Conf2	,814
Conf3	,546

Y si eliminamos esa 3ª variable entonces:

Estadísticos total-elemento

	Media de la escala si se elimina el elemento	Varianza de la escala si se elimina el elemento	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
Conf1	1,17	,505	,374	,201	,361
Conf2	1,21	,456	,416	,219	,281
Conf3	1,62	,458	,232	,056	,613

En el primer piloto nos habíamos quedado en un alfa de 0,234, así que cambiaremos la forma de la redacción de esa tercera variable observable en la encuesta definitiva y, en el resto del análisis del piloto, vamos a utilizarla con el “signo” cambiado.

Constructo “Estrés”, medido por las respuestas a las preguntas 34, 35 y 36 da los siguientes valores:

Estadísticos de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en los elementos tipificados	N de elementos
,552	,558	3

Similar al obtenido en el primer piloto (0,559) y en el que no hemos modificado ninguna redacción. Mejorable hasta:

Estadísticos total-elemento

	Media de la escala si se elimina el elemento	Varianza de la escala si se elimina el elemento	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
St1	,66	,734	,155	,028	,758
St2	,93	,567	,466	,373	,287
St3	,90	,525	,513	,384	,197

Correlaciones

		St1	St2	St3
St1	Correlación de Pearson	1	,110	,168
	Sig. (bilateral)		,571	,385
	N	29	29	29
St2	Correlación de Pearson	,110	1	,611**
	Sig. (bilateral)	,571		,000
	N	29	29	29
St3	Correlación de Pearson	,168	,611**	1
	Sig. (bilateral)	,385	,000	
	N	29	29	29

** . La correlación es significativa al nivel 0,01 (bilateral).

Con el análisis factorial, encontramos los siguientes valores:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,520
Prueba de esfericidad de Chi-cuadrado aproximado		12,978
Bartlett	gl	3
	Sig.	,005

Matriz de componentes^a

	Componente
	1
St1	,364
St2	,868
St3	,885

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,669	55,620	55,620	1,669	55,620	55,620
2	,945	31,510	87,131			
3	,386	12,869	100,000			

Así que la dejaremos tal cual está.

Constructo “Utilidad”:

Matriz de correlaciones inter-elementos

	Ut1	Ut2	Ut3	Ut4
Ut1	1,000	-,096	-,207	,462
Ut2	-,096	1,000	,224	-,096
Ut3	-,207	,224	1,000	,083
Ut4	,462	-,096	,083	1,000

La correlación entre Ut1 y Ut2 y Ut3 es negativa, y donde hay más alta correlación es entre Ut1 y Ut4

Por otra parte, el análisis factorial de las cuatro variables nos indica 2 factores:

**Matriz de componentes
rotados^a**

	Componente	
	1	2
Ut1	,817	-,239
Ut2	-,108	,701
Ut3	,022	,837
Ut4	,883	,110

Pero, eliminando Ut3 nos quedamos con un factor con los siguientes parámetros:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.	,518	
Prueba de esfericidad de Chi-cuadrado aproximado	6,349	
Bartlett	gl	3
	Sig.	,096

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,499	49,952	49,952	1,499	49,952	49,952
2	,963	32,099	82,051			
3	,538	17,949	100,000			

Método de extracción: Análisis de Componentes principales.

Matriz de componentes^a

	Componente
	1
Ut1	,835
Ut2	-,322
Ut4	,835

Como vemos que el signo de la aportación de Ut2 es negativo, cambiamos la codificación de las respuestas por la complementaria, y lo tenemos en cuenta para dar la redacción correspondiente, y obtenemos:

Estadísticos de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en los elementos tipificados	N de elementos
,430	,455	3

Con una muy baja correlación de Ut2:

Matriz de correlaciones inter-elementos

	Ut1	Ut2	Ut4
Ut1	1,000	,096	,462
Ut2	,096	1,000	,096
Ut4	,462	,096	1,000

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,518
Prueba de esfericidad de	Chi-cuadrado aproximado	6,349
Bartlett	gl	3
	Sig.	,096

Matriz de componentes^a

	Componente
	1
Ut1	,835
Ut2	,322
Ut4	,835

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
	1	1,499	49,952	49,952	1,499	49,952
2	,963	32,099	82,051			
3	,538	17,949	100,000			

Método de extracción: Análisis de Componentes principales.

Que si la eliminamos, tendríamos:

Estadísticos total-elemento

	Media de la escala si se elimina el elemento	Varianza de la escala si se elimina el elemento	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
Ut1	1,04	,184	,353	,216	,173
Ut2	1,86	,201	,112	,013	,632
Ut4	1,04	,184	,353	,216	,173

Correlaciones

		Ut1	Ut4
Ut1	Correlación de Pearson	1	,354
	Sig. (bilateral)		,059
	N	29	29
Ut4	Correlación de Pearson	,354	1
	Sig. (bilateral)	,059	
	N	29	29

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,500
Prueba de esfericidad de Chi-cuadrado aproximado		3,557
Bartlett	gl	1
	Sig.	,059

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,354	67,720	67,720	1,354	67,720	67,720
2	,646	32,280	100,000			

Método de extracción: Análisis de Componentes principales.

Matriz de componentes^a

	Componente
	1
Ut1	,823
Ut4	,823

Para el resto del análisis de nuestro piloto utilizaremos estas dos variables.

ANEXO A3 - Cuestionario definitivo

Cuestionario global de la encuesta:

1. Edad:

(A continuación, marcar lo que proceda)

2.

Hombre Mujer

Sexo:	<input type="checkbox"/>	<input type="checkbox"/>
--------------	--------------------------	--------------------------

3. **RA**

Vas a curso por año	<input type="checkbox"/>
o arrastras alguna asignatura (1 ó 2) de cursos anteriores	<input type="checkbox"/>
o arrastras varias asignaturas (3 ó más) de cursos anteriores	<input type="checkbox"/>

4. Me conecto a internet: **UI**

Casi de continuo
(Iphone, tablet, Ipad)

Ocasionalmente	1-2 veces / semana	3-5 días/semana	todos los días	<input type="checkbox"/>
----------------	--------------------	-----------------	----------------	--------------------------

5. Respecto a contraseñas: **AUP1**

No establezco contraseñas Tengo una password común para la mayoría de accesos Uso diferentes contraseñas para cada acceso (PC, ficheros, aplics.)

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

6., siguiendo con contraseñas, si las establezco: **AUP2**

suelo mantenerlas fijas las cambio anualmente, más o menos las cambio cada semestre o menos

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

7. y, habitualmente..... AUP3

Dejo que el navegador grabe la contraseña, para ir más rápido	
Suelo usar contraseñas fáciles de recordar (nombres o iniciales, matrículas, DNI, fechas de aniversario, teléfonos,...)	
Prefiero usar contraseñas con mezcla de letras, números, signos de puntuación..., no descriptivos de la opción anterior	

8. Hago copias de seguridad de mis datos ABU1

No he hecho nunca	Al cambiar el PC	Cada año, seleccionando ficheros	Cada seis meses, seleccionando ficheros	De forma programada, automáticamente

9. Respecto donde guardo las copias de seguridad de mis datos ABU2

No las suelo hacer	En otras carpetas del disco del sistema	En CD, DVD, pendrive	En disco externo	En la propia red (Cloud computing)

10. Mientras hago mis trabajos... ABU3

No hago copias de seguridad, tengo confianza en el sistema	
Hago una copia cuando lo he terminado	
Hago una copia tras cada actualización a la que he dedicado gran esfuerzo	
Hago una copia tras cada actualización, aunque haya sido sencilla	
Tengo un sistema automático de actualización	

11. Protejo el acceso a mi PC y/o a ficheros del mismo a través de: A1

No necesito protecciones, se trata de mi PC	
Utilizo una password para acceder a la sesión	
Utilizo claves para los distintos accesos (PC, ficheros...)	

12. Cuando recibo un mail de remitente desconocido... A2

Lo abro para enterarme de lo que pretenden	
Abro los posibles archivos para examinar su contenido	
Guardo los posibles archivos para examinarlos más tarde	
Lo marco como spam	
Lo elimino directamente	

13. En general, me entero de las últimas vulnerabilidades en seguridad a través de:

A3

No suelo mostrar interés	
Compañeros, amigos	
Medios de comunicación	
Webs personalizadas (compañías de sw, inteco, ministerios...), revistas técnicas	
Avisos de la Universidad	

14. En relación con el uso de internet, dirías que usas internet para Información sobre noticias de actualidad, Formación, Comunicarme (correo, foros, chats...), Compra-venta, Transacciones bancarias, Información de ofertas comerciales, Entretenimientos multimedia (escuchar / ver vídeos, música online, películas, descarga de libros...)... **AW1**

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

15. En relación con el uso de internet, dirías que usas internet para Entretenimiento multimedia (subir vídeos, música), participar en juegos on-line, tengo un blog actualizado, soy usuario de wikis.... **AW2**

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

16. Has hecho, o sueles hacer, compras a través de internet de viajes (billetes, hoteles, alquiler de coches...), entradas de espectáculos (cine, teatro, concierto...), adquisición de libros, ropa, electrónica, alimentación, hogar.... **AW3**

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

Dinos tu opinión sobre estos conceptos: P1 – P11

		Si no	
17	Un usuario con conexión ADSL debe preocuparse por la seguridad		
18	Una conexión inalámbrica con cifrado WEP tiene la misma seguridad que una conexión a través de cable		
19	Cuando uso Wi-fi en la conexión en mi domicilio, estoy en riesgo		
20	Al usar Wi-fi en la conexión en el centro de trabajo/estudio, estoy en riesgo		
21	El símbolo del candado que se ve en los sitios más serios de e-commerce cuando doy los datos de mi tarjeta, me permiten hacer pagos seguros		
22	Algunos programas informáticos de malware son inofensivos		
23	La mayoría de los virus se diseñan para eliminar archivos y/o perjudicar nuestro sistema operativo y/o acceder a información confidencial		
24	Un virus puede mutar y recombinarse con otros originando nuevos virus		
25	Casi todos los usuarios pueden formar parte de redes zombi		
26	Los troyanos y el phishing persiguen resultados similares		
27	Algunos programas de adware (ejecución inmediata de publicidad) hacen un seguimiento de las prácticas del usuario y acaban siendo spyware		

Respecto las Redes sociales...(si no eres usuario de ninguna, pasa a la pregunta 39)

28. Con referencia a la dedicación, me conecto: URS1

Ocasionalmente 1-2 veces / semana 3-5 días/semana todos los días casi continuamente

--	--	--	--	--

29. el motivo de darme de alta, inicialmente, fue por: URS2

novedad, estar “a la última”	
recomendado por algunos amigos, para comunicarnos	
encontrar nuevas relaciones	
observar, ver lo que se dice	
otras razones (<i>especificar</i>)	

30. Con referencia a las condiciones de registro AURS3

Acepté sin leerlas, entendiendo que son estándar	
Las acepté previamente y, cuando me familiaricé, las adapté a mi perfil	
Estudí los aspectos más relevantes y, tras adaptarlos a mis gustos, las acepté	
Me las leí y, tras adaptarlas a mis gustos en su totalidad, las acepté	
No me di de alta porque no me gustaron	

En este tipo de foro, URS4 – URS8

		Si	No
31	Soy usuario de Facebook, Twitter, Tuenti...en ámbitos familiar y de amistad		
32	Soy usuario de LinkedIn, Facebook, ...en ámbito profesional		
33	Limito determinados accesos a mi información		
34	Tengo identidades diferentes para según qué tipo de relación		
35	Participo activamente, no me limito a observar		

36. Respecto tu actividad, usas tu verdadero nombre e incluyes tus datos (fotografía, dirección, teléfono, profesión, curriculum, edad, lista de amigos...) en tu perfil, y te expresas libremente manifestando tus aficiones (deportes, cine, música, lectura....) AURS9

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

37. Compartes fotos/vídeos de acontecimientos personales (fiestas, viajes, bodas, cumpleaños...) así como composiciones propias (dibujos, música, textos, diseños...) AURS10

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

38. Te expresas libremente manifestando tus puntos de vista sobre asuntos políticos, religiosos, relaciones familiares, de amistad, laborales, sexuales... AURS11

no, nunca	alguna vez	suelo hacerlo	frecuentemente	siempre

Seguridad en las TICs:

Indique valoración en escala de 1 a 5, de forma que:

1=Totalmente en desacuerdo 2=Más bien, en desacuerdo 3=Indiferente

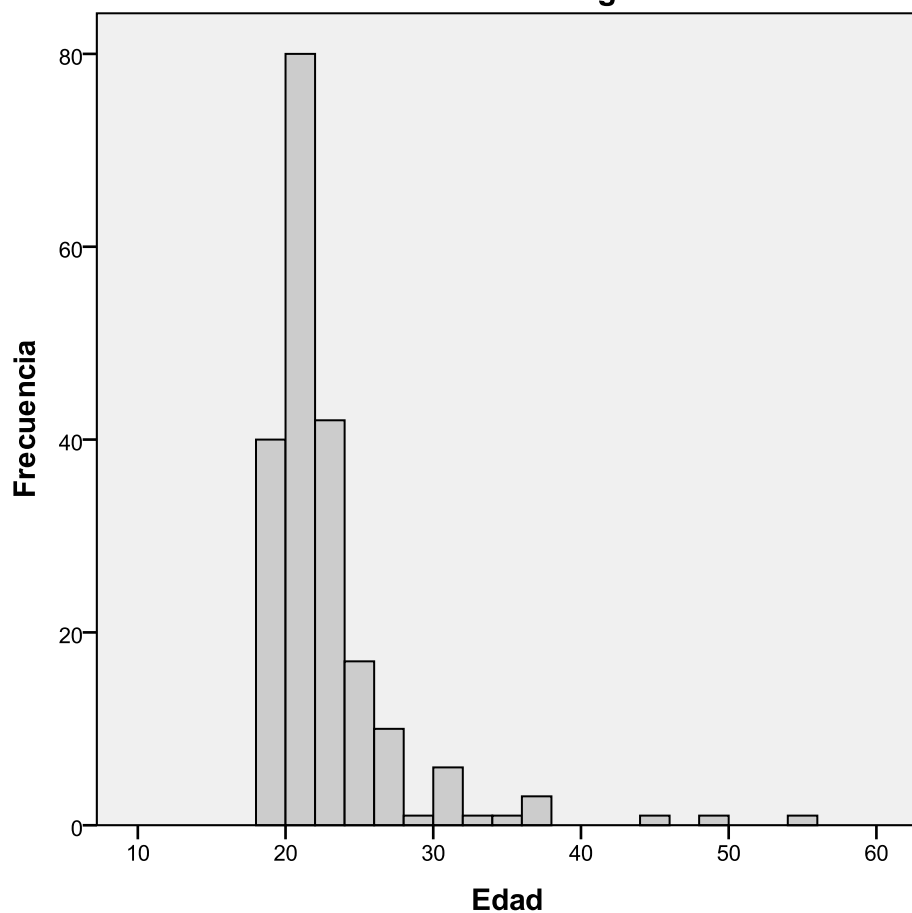
4=Más bien de acuerdo 5=Totalmente de acuerdo

39	Me gusta hablar con otros de seguridad	At1	
40	Si tuviera oportunidad me inscribiría en cursos de seguridad		
41	Siento curiosidad por las noticias sobre seguridad		
42	Estudiar sobre seguridad es entretenido		
43	Me gustaría dedicar más tiempo a aprender temas de seguridad	A15	
44	Saber seguridad incrementa mis posibilidades de navegar tranquilo	C1	
45	Me alegra poder resolver dificultades de seguridad		
46	Soy capaz de ayudar a otros a resolver muchos de sus problemas de seguridad		
47	Me gusta adoptar suficientes medidas de seguridad		
48	Si me lo propongo puedo dominar bien los aspectos sobre seguridad	C5	
49	Estoy preocupado por los riesgos de seguridad	E1	
50	Me altero cuando tengo que resolver un problema de seguridad		
51	Me siento incapaz de comprender algunas cuestiones sobre seguridad		
52	Tengo que encontrar más tiempo para implementar temas de seguridad		
53	Si me surge un problema de seguridad debo buscar ayuda	E5	
54	La seguridad es muy necesaria para mi actividad personal	U1	
55	La seguridad es muy necesaria para mi actividad profesional		
56	Los conocimientos sobre seguridad deben ser previos al uso de PC's		
57	Debo saber utilizar los recursos de protección al navegar por internet		
58	Debo saber utilizar los recursos de seguridad al navegar por redes sociales	U5	
59	Usando Wi-fi en casa uso clave para el acceso	A4	
60	Cada vez que inicio sesión con mi PC introduzco mi password	A5	
61	Tengo activo un antivirus actualizado con regularidad	A6	
62	Tengo activo un firewall actualizado con regularidad	A7	
63	Elimino periódicamente los archivos temporales y cookies almacenados en mi PC tras navegar por internet	A8	
64	Borro el Histórico de páginas visitadas o he determinado que almacene las correspondientes el mínimo tiempo posible	A9	
65	Cuando envío un mail a varios destinatarios, la mayor parte de las veces utilizo la copia oculta	A10	
66	Cuando envío un mail a varios destinatarios, casi siempre direcciono a todos de forma abierta para que sepan a quien se lo he enviado	A11	

ANEXO A3.1 - Resultados cuestionario definitivo (curso 2011-12)

		Edad			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	19	40	19,6	19,6	19,6
	20	52	25,5	25,5	45,1
	21	28	13,7	13,7	58,8
	22	19	9,3	9,3	68,1
	23	23	11,3	11,3	79,4
	24	11	5,4	5,4	84,8
	25	6	2,9	2,9	87,7
	26	8	3,9	3,9	91,7
	27	2	1,0	1,0	92,6
	29	1	,5	,5	93,1
	30	4	2,0	2,0	95,1
	31	2	1,0	1,0	96,1
	32	1	,5	,5	96,6
	34	1	,5	,5	97,1
	36	1	,5	,5	97,5
	37	2	1,0	1,0	98,5
	44	1	,5	,5	99,0
	48	1	,5	,5	99,5
	55	1	,5	,5	100,0
	Total	204	100,0	100,0	

Histograma



Sexo

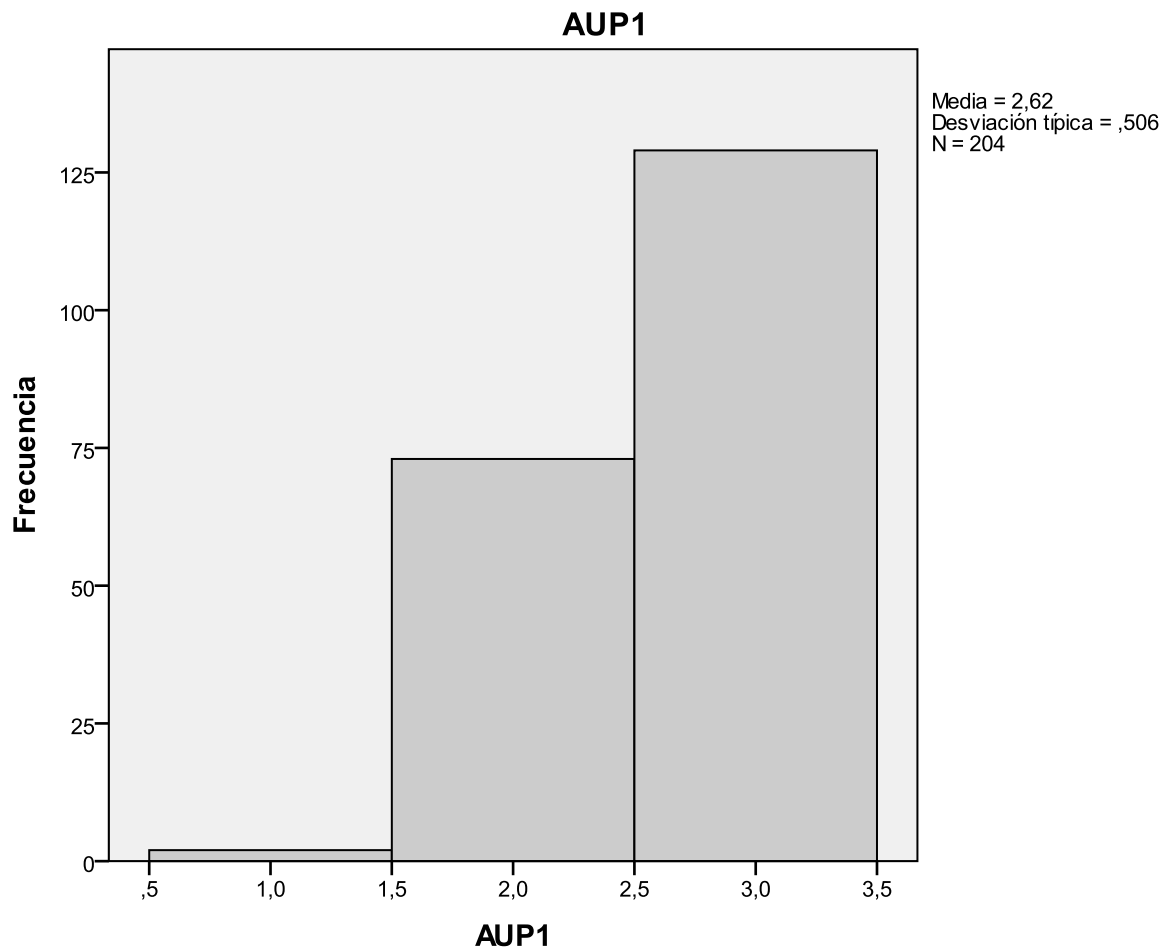
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	180	88,2	88,2	88,2
	2	24	11,8	11,8	100,0
	Total	204	100,0	100,0	

RA

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	117	57,4	57,6	57,6
	2	58	28,4	28,6	86,2
	3	28	13,7	13,8	100,0
	Total	203	99,5	100,0	
Perdidos	Sistema	1	,5		
	Total	204	100,0		

Contraseñas:

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	2	1,0	1,0	1,0
	2	73	35,8	35,8	36,8
	3	129	63,2	63,2	100,0
	Total	204	100,0	100,0	

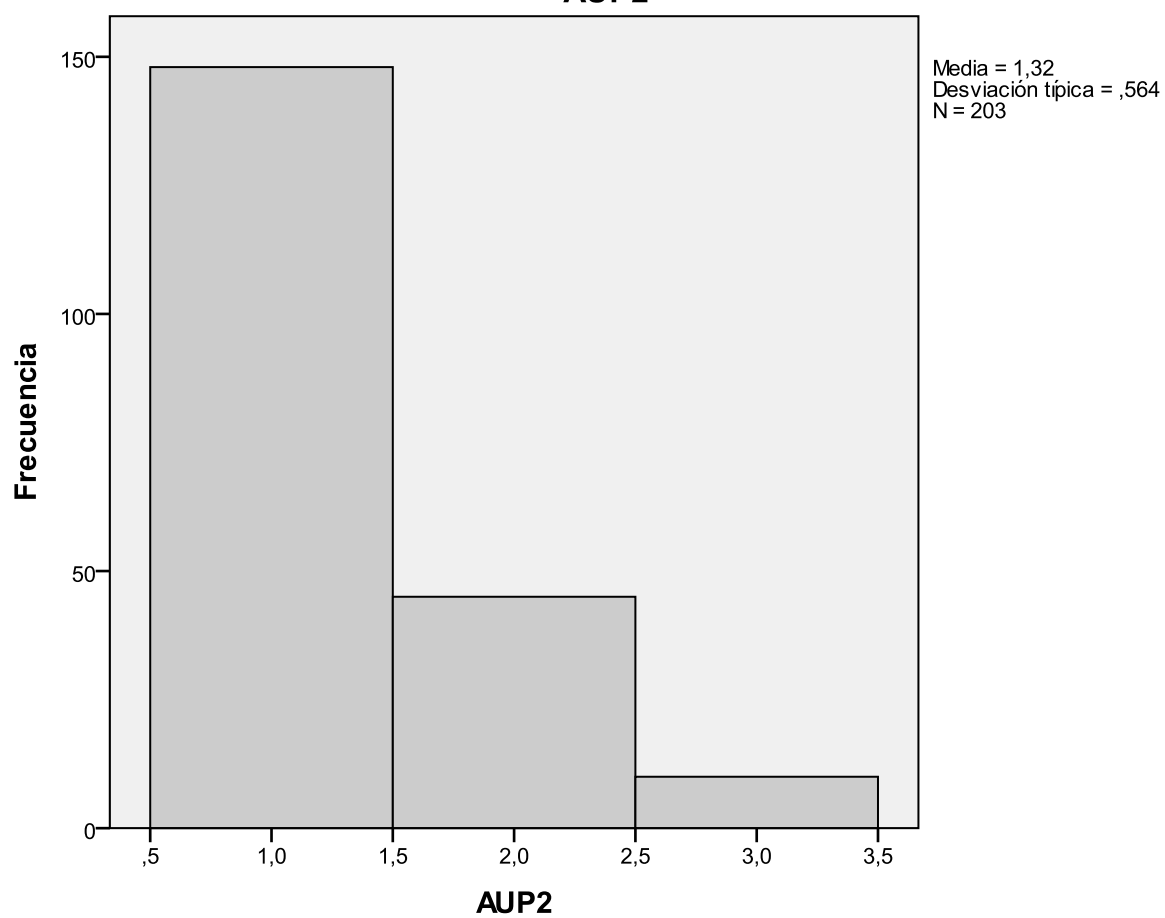


Salvo dos “temerarios”, la mayoría usa diferentes contraseñas, aunque muchos usan la misma

AUP2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	148	72,5	72,9	72,9
	2	45	22,1	22,2	95,1
	3	10	4,9	4,9	100,0
	Total	203	99,5	100,0	
Perdidos	Sistema	1	,5		
	Total	204	100,0		

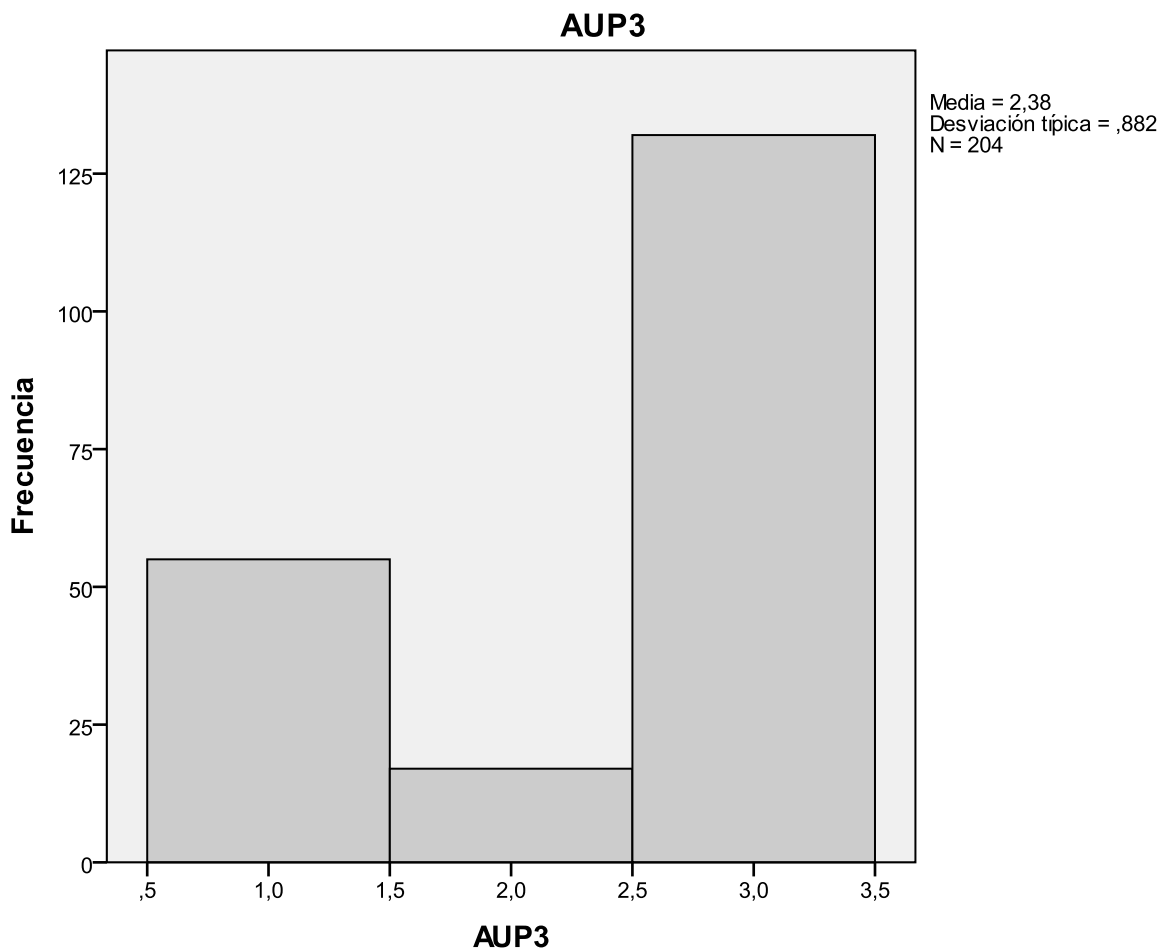
AUP2



La inmensa mayoría las mantiene fijas en el tiempo

AUP3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	55	27,0	27,0	27,0
	2	17	8,3	8,3	35,3
	3	132	64,7	64,7	100,0
	Total	204	100,0	100,0	



Y, aunque no usan combinaciones fáciles de identificar, un porcentaje alto (27,3%) deja que las grabe el navegador. Queda un 64% de más precavidos.

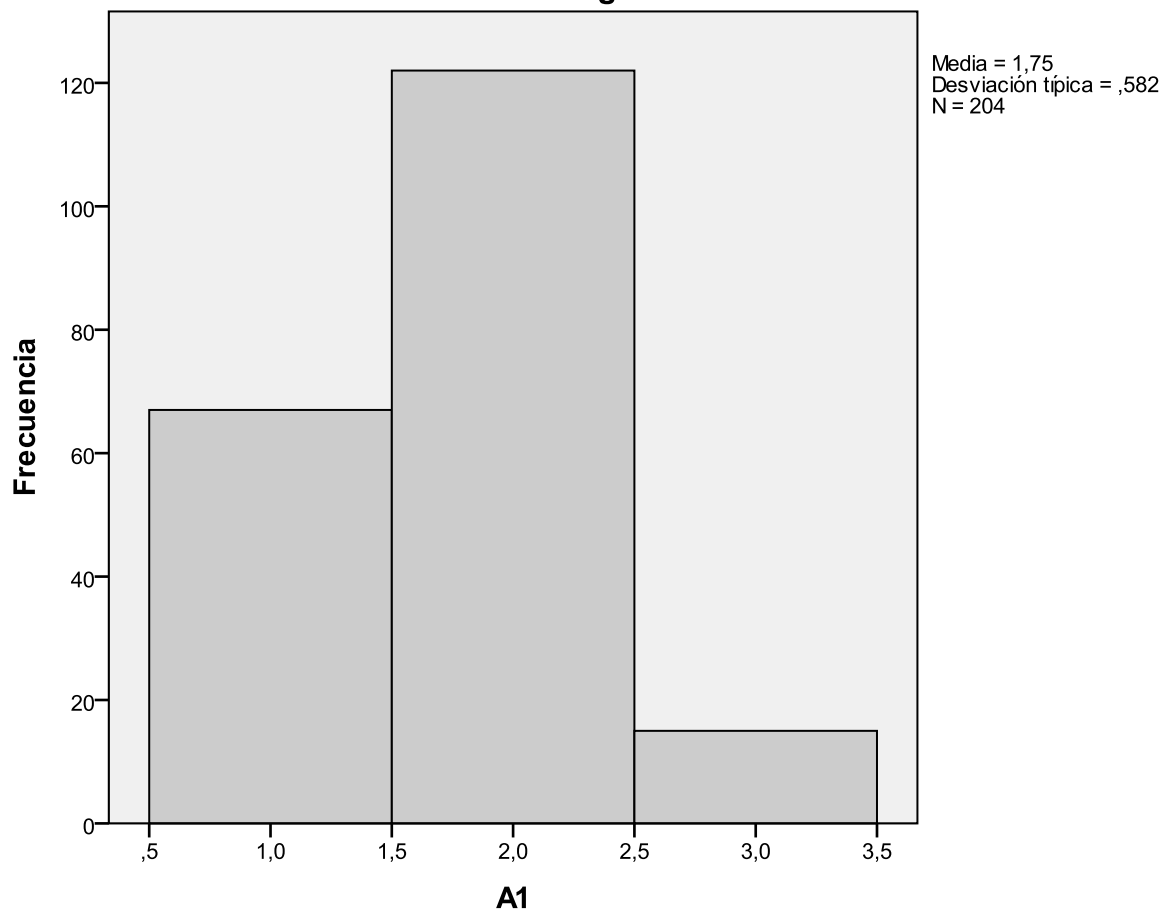
Tabla de contingencia AUP1 * AUP2 * AUP3

Recuento

AUP3			AUP2			Total
			1	2	3	
1	AUP1	2	21	7		28
		3	18	9		27
	Total		39	16		55
2	AUP1	2	8	0	0	8
		3	6	2	1	9
	Total		14	2	1	17
3	AUP1	1	1	0	0	1
		2	31	6	0	37
		3	63	21	9	93
	Total		95	27	9	131
Total	AUP1	1	1	0	0	1
		2	60	13	0	73
		3	87	32	10	129
	Total		148	45	10	203

A1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	67	32,8	32,8	32,8
	2	122	59,8	59,8	92,6
	3	15	7,4	7,4	100,0
	Total	204	100,0	100,0	

Histograma

Tampoco son cuidadosos con la necesidad de usar claves para acceder al PC. Solo el 7% utilizan diversas claves para distintos accesos y el 60% usa una clave general. El 33% no utiliza ninguna protección.

A2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	39	19,1	19,1	19,1
	2	4	2,0	2,0	21,1
	3	5	2,5	2,5	23,5
	4	33	16,2	16,2	39,7
	5	123	60,3	60,3	100,0
	Total	204	100,0	100,0	

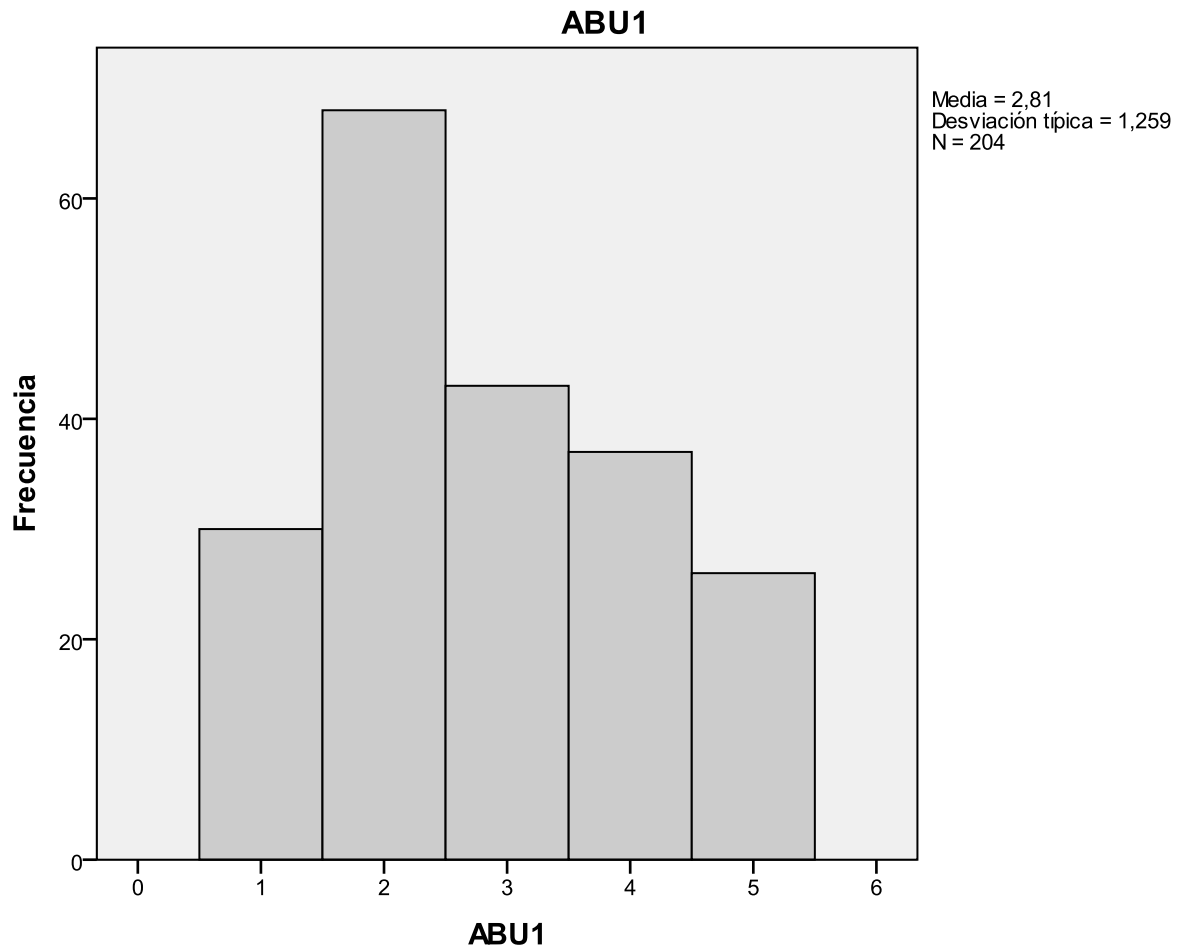
A3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	33	16,2	16,2	16,2
	2	52	25,5	25,5	41,7
	3	58	28,4	28,4	70,1
	4	59	28,9	28,9	99,0
	5	2	1,0	1,0	100,0
	Total	204	100,0	100,0	

Sin embargo, hay correlaciones significativas entre las siguientes variables con cinco alternativas de respuesta:

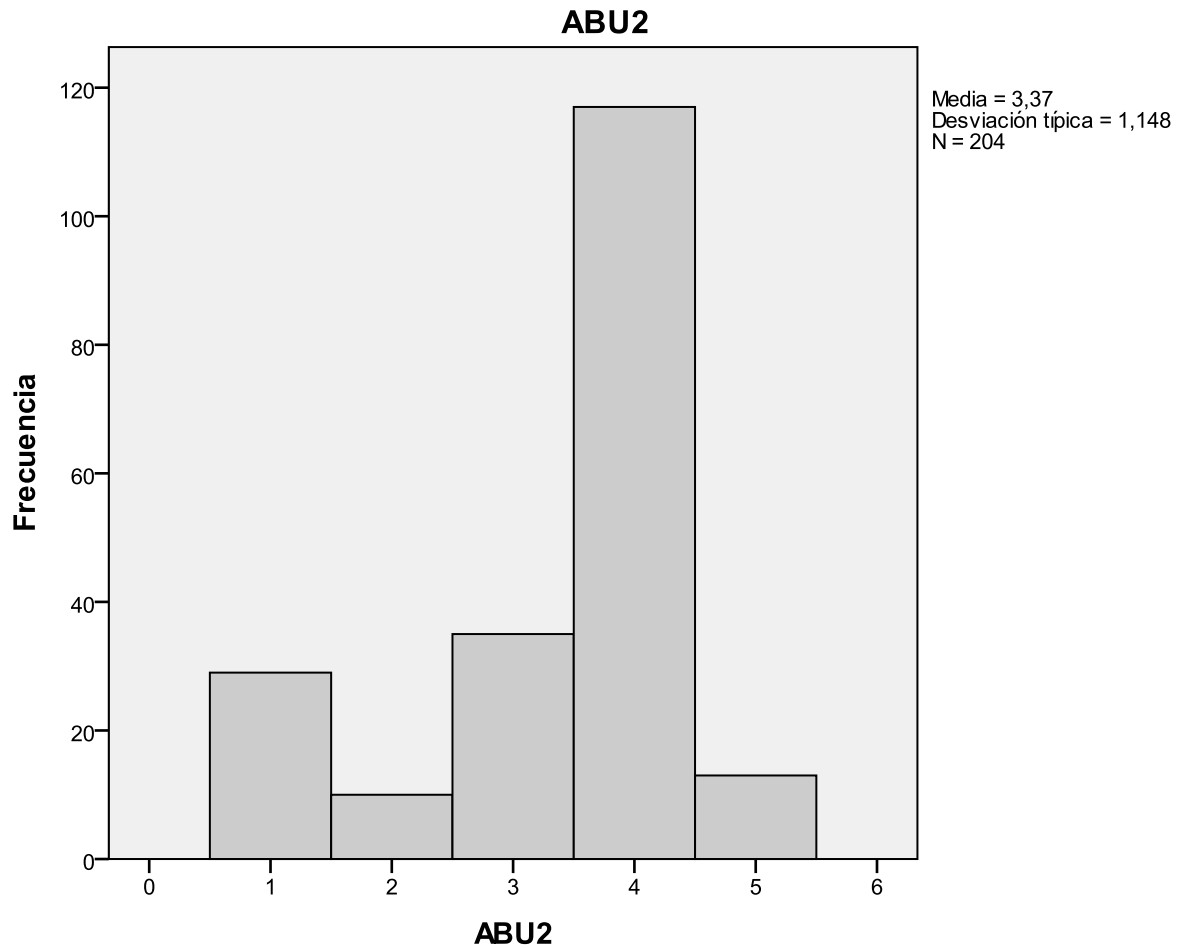
ABU1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	30	14,7	14,7	14,7
	2	68	33,3	33,3	48,0
	3	43	21,1	21,1	69,1
	4	37	18,1	18,1	87,3
	5	26	12,7	12,7	100,0
	Total	204	100,0	100,0	



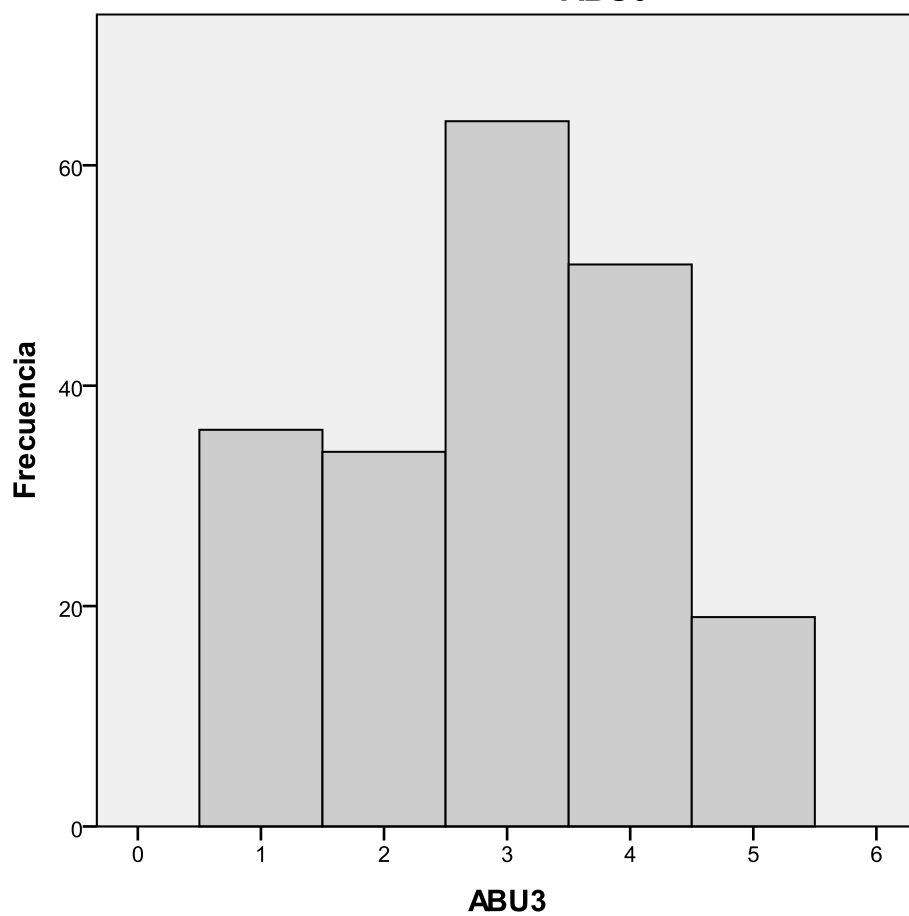
ABU2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	29	14,2	14,2	14,2
	2	10	4,9	4,9	19,1
	3	35	17,2	17,2	36,3
	4	117	57,4	57,4	93,6
	5	13	6,4	6,4	100,0
	Total	204	100,0	100,0	



ABU3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	36	17,6	17,6	17,6
	2	34	16,7	16,7	34,3
	3	64	31,4	31,4	65,7
	4	51	25,0	25,0	90,7
	5	19	9,3	9,3	100,0
	Total	204	100,0	100,0	

ABU3

Media = 2,92
Desviación típica = 1,223
N = 204

ABU1 con ABU2 (copias de seguridad)

		ABU1	ABU2
ABU1	Correlación de Pearson	1	,554**
	Sig. (bilateral)		,000
	N	204	204
ABU2	Correlación de Pearson	,554**	1
	Sig. (bilateral)	,000	
	N	204	204

** . La correlación es significativa al nivel 0,01 (bilateral).

			ABU2					Total
			1	2	3	4	5	
ABU1	1	Recuento	25	1	1	3	0	30
		% dentro de ABU1	83,3%	3,3%	3,3%	10,0%	,0%	100,0%
	2	Recuento	3	4	19	40	2	68
		% dentro de ABU1	4,4%	5,9%	27,9%	58,8%	2,9%	100,0%
	3	Recuento	1	3	8	28	3	43
		% dentro de ABU1	2,3%	7,0%	18,6%	65,1%	7,0%	100,0%
	4	Recuento	0	0	5	30	2	37
		% dentro de ABU1	,0%	,0%	13,5%	81,1%	5,4%	100,0%
	5	Recuento	0	2	2	16	6	26
		% dentro de ABU1	,0%	7,7%	7,7%	61,5%	23,1%	100,0%
Total		Recuento	29	10	35	117	13	204
		% dentro de ABU1	14,2%	4,9%	17,2%	57,4%	6,4%	100,0%

Nada menos que un 15% de los alumnos de “Informática” no hecho nunca copias de seguridad de sus datos. Y otro 5% que si lo hacen lo almacenan en el mismo disco del sistema.

Con alta significatividad:

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	161,732 ^a	16	,000
Razón de verosimilitudes	127,264	16	,000
Asociación lineal por lineal	62,215	1	,000
N de casos válidos	204		

a. 13 casillas (52,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,27.

Gráfico de barras

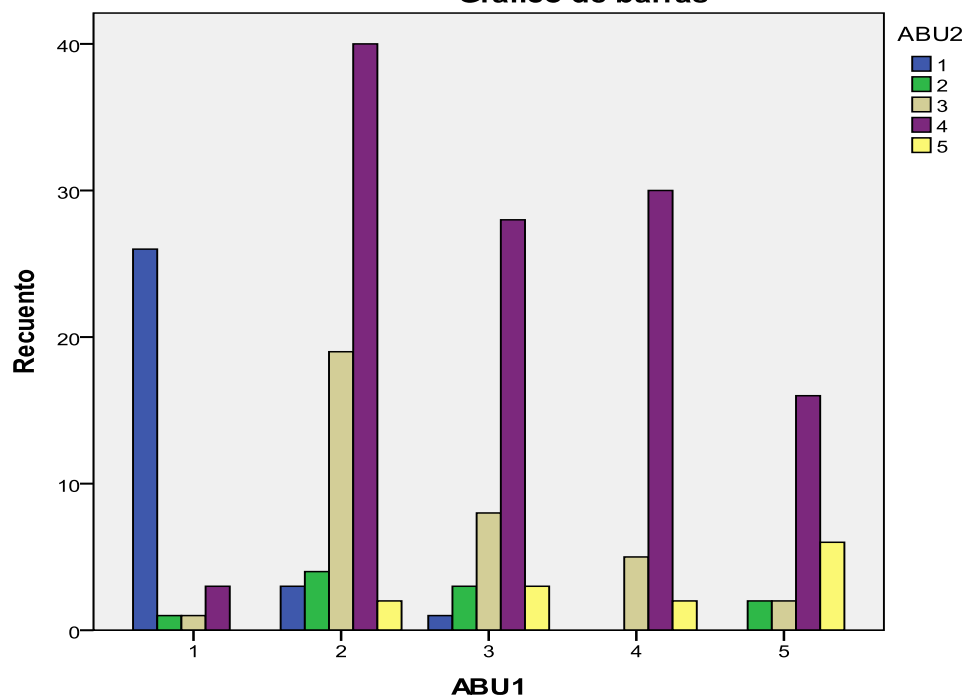


Tabla de contingencia ABU3 * ABU2 * ABU1

Recuento

ABU1			ABU2					Total
			1	2	3	4	5	
1	ABU3	1	9	0	1	0		10
		2	3	0	0	1		4
		3	7	1	0	2		10
		4	3	0	0	0		3
		5	3	0	0	0		3
	Total		25	1	1	3		30
2	ABU3	1	1	0	3	7	1	12
		2	0	1	1	11	0	13
		3	2	2	7	8	0	19
		4	0	1	7	12	1	21
		5	0	0	1	2	0	3
	Total		3	4	19	40	2	68
3	ABU3	1	1	0	1	3	0	5
		2	0	1	1	7	0	9
		3	0	0	6	8	1	15
		4	0	1	0	10	0	11
		5	0	1	0	0	2	3
	Total		1	3	8	28	3	43
4	ABU3	1			2	4	0	6
		2			0	6	0	6
		3			2	11	1	14
		4			1	7	1	9
		5			0	2	0	2
	Total				5	30	2	37
5	ABU3	1		0	0	3	0	3
		2		0	0	1	1	2
		3		1	1	3	1	6
		4		1	1	4	1	7
		5		0	0	5	3	8
	Total			2	2	16	6	26
Total	ABU3	1	11	0	7	17	1	36
		2	3	2	2	26	1	34
		3	9	4	16	32	3	64
		4	3	3	9	33	3	51
		5	3	1	1	9	5	19
	Total		29	10	35	117	13	204

AW1 con AW2 y AW3 (tipo de actividad en internet)

Correlaciones

			AW1	AW2	AW3
Rho de Spearman	AW1	Coeficiente de correlación	1,000	,298**	,310**
		Sig. (bilateral)	.	,000	,000
		N	204	204	204
	AW2	Coeficiente de correlación	,298**	1,000	,317**
		Sig. (bilateral)	,000	.	,000
		N	204	205	205
	AW3	Coeficiente de correlación	,310**	,317**	1,000
		Sig. (bilateral)	,000	,000	.
		N	204	204	204

** . La correlación es significativa al nivel 0,01 (bilateral).

AW1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	2	1,0	1,0	1,0
	2	14	6,9	6,9	7,9
	3	15	7,4	7,4	15,3
	4	82	40,2	40,4	55,7
	5	90	44,1	44,3	100,0
	Total	203	99,5	100,0	
Perdidos	Sistema	1	,5		
Total		204	100,0		

AW2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	9	4,4	4,4	4,4
	2	39	19,1	19,1	23,5
	3	31	15,2	15,2	38,7
	4	66	32,4	32,4	71,1
	5	59	28,9	28,9	100,0
	Total	204	100,0	100,0	

AW3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	28	13,7	13,7	13,7
	2	101	49,5	49,5	63,2
	3	47	23,0	23,0	86,3
	4	20	9,8	9,8	96,1
	5	8	3,9	3,9	100,0
	Total	204	100,0	100,0	

URS1, con AURS9, con AURS10 y AURS11 (tipo de actividad en redes sociales)

Con respecto a la **actividad en redes sociales**, tenemos:

AURS9

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	25	12,3	12,3	12,3
	2	78	38,2	38,2	50,5
	3	52	25,5	25,5	76,0
	4	33	16,2	16,2	92,2
	5	16	7,8	7,8	100,0
	Total	204	100,0	100,0	

AURS10

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	34	16,7	16,7	16,7
	2	78	38,2	38,4	55,2
	3	51	25,0	25,1	80,3
	4	30	14,7	14,8	95,1
	5	10	4,9	4,9	100,0
	Total	203	99,5	100,0	
Perdidos	Sistema	1	,5		
	Total	204	100,0		

AURS11

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	51	25,0	25,0	25,0
	2	61	29,9	29,9	54,9
	3	44	21,6	21,6	76,5
	4	22	10,8	10,8	87,3
	5	26	12,7	12,7	100,0
	Total		204	100,0	100,0

Correlaciones

		AURS9	AURS10	AURS11
AURS9	Correlación de Pearson	1	,560**	,422**
	Sig. (bilateral)		,000	,000
	N	204	203	204
AURS10	Correlación de Pearson	,560**	1	,369**
	Sig. (bilateral)	,000		,000
	N	203	203	203
AURS11	Correlación de Pearson	,422**	,369**	1
	Sig. (bilateral)	,000	,000	
	N	204	203	204

** . La correlación es significativa al nivel 0,01 (bilateral).

Las correlaciones son altas.

Tabla de contingencia AURS9 * AURS10

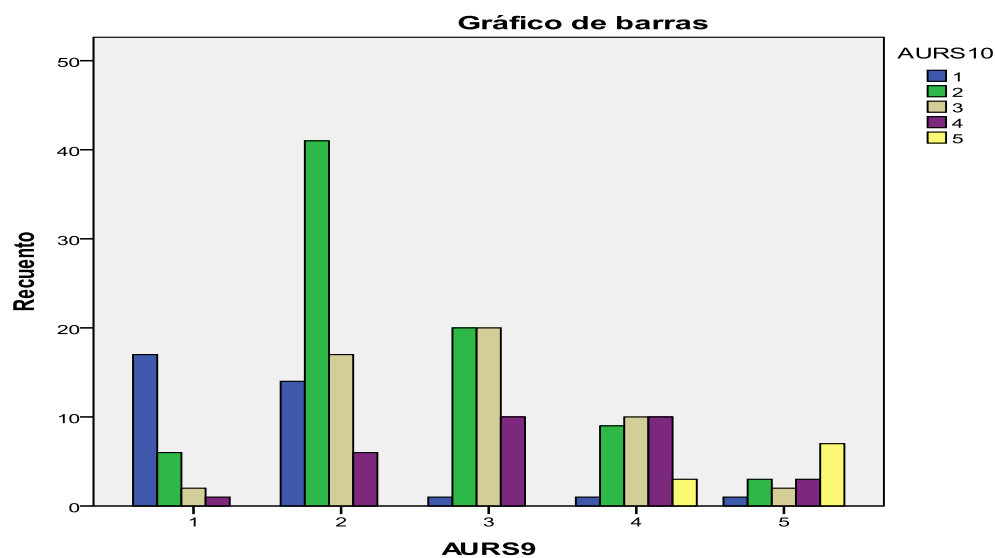
			AURS10					Total
			1	2	3	4	5	
AURS9	1	Recuento	17	5	2	1	0	25
		% dentro de AURS9	68,0%	20,0%	8,0%	4,0%	,0%	100,0%
	2	Recuento	14	41	17	6	0	78
		% dentro de AURS9	17,9%	52,6%	21,8%	7,7%	,0%	100,0%
	3	Recuento	1	20	20	10	0	51
		% dentro de AURS9	2,0%	39,2%	39,2%	19,6%	,0%	100,0%
	4	Recuento	1	9	10	10	3	33
		% dentro de AURS9	3,0%	27,3%	30,3%	30,3%	9,1%	100,0%
	5	Recuento	1	3	2	3	7	16
		% dentro de AURS9	6,3%	18,8%	12,5%	18,8%	43,8%	100,0%
Total		Recuento	34	78	51	30	10	203
		% dentro de AURS9	16,7%	38,4%	25,1%	14,8%	4,9%	100,0%

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	136,988 ^a	16	,000
Razón de verosimilitudes	104,011	16	,000
Asociación lineal por lineal	63,305	1	,000
N de casos válidos	203		

a. 11 casillas (44,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,79.

Claro que, más de un 20%, deja “al libre albedrío” el uso de sus trabajos personales.



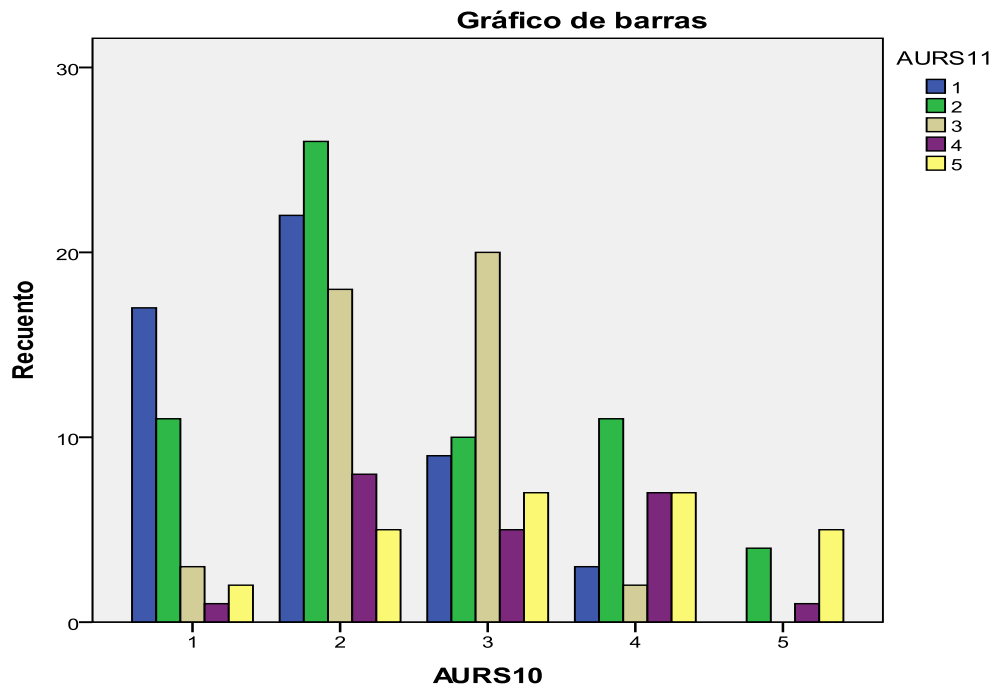
Todo con una alta correspondencia.

Pasa lo mismo cuando comparamos con la actividad más peligrosa:

Tabla de contingencia AURS10 * AURS11

			AURS11					Total
			1	2	3	4	5	
AURS10	1	Recuento	17	11	3	1	2	34
		% dentro de AURS10	50,0%	32,4%	8,8%	2,9%	5,9%	100,0%
	2	Recuento	22	26	18	8	5	79
		% dentro de AURS10	27,8%	32,9%	22,8%	10,1%	6,3%	100,0%
	3	Recuento	9	10	20	5	7	51
		% dentro de AURS10	17,6%	19,6%	39,2%	9,8%	13,7%	100,0%
	4	Recuento	3	11	2	7	7	30
		% dentro de AURS10	10,0%	36,7%	6,7%	23,3%	23,3%	100,0%
	5	Recuento	0	4	0	1	5	10
		% dentro de AURS10	,0%	40,0%	,0%	10,0%	50,0%	100,0%
Total		Recuento	51	62	43	22	26	204
		% dentro de AURS10	25,0%	30,4%	21,1%	10,8%	12,7%	100,0%

Donde vemos que un 45% de los alumnos no tienen perjuicios en contar sus “intimidades” a través de las redes sociales.



Con una significatividad alta entre ambas medidas de actividad:

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	57,244 ^a	16	,000
Razón de verosimilitudes	56,606	16	,000
Asociación lineal por lineal	27,724	1	,000
N de casos válidos	204		

AURS3

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos 1	126	61,8	61,8	61,8
2	40	19,6	19,6	81,4
3	22	10,8	10,8	92,2
4	10	4,9	4,9	97,1
5	6	2,9	2,9	100,0
Total	204	100,0	100,0	

Y, para Correlaciones en **temas más generales de seguridad**

Correlaciones

	A3	A4	A5	A6	A7	A8	A9
A3 Correlación de Pearson	1	,272**	,166*	,164*	,199**	,310**	,229**
Sig. (bilateral)		,000	,018	,019	,004	,000	,001
N	204	203	204	204	204	204	204
A4 Correlación de Pearson	,272**	1	,212**	,264**	,305**	,287**	,233**
Sig. (bilateral)	,000		,002	,000	,000	,000	,001
N	203	203	203	203	203	203	203
A5 Correlación de Pearson	,166*	,212**	1	,162*	,236**	,164*	,141*
Sig. (bilateral)	,018	,002		,020	,001	,019	,044
N	204	203	204	204	204	204	204
A6 Correlación de Pearson	,164*	,264**	,162*	1	,637**	,365**	,378**
Sig. (bilateral)	,019	,000	,020		,000	,000	,000
N	204	203	204	204	204	204	204
A7 Correlación de Pearson	,199**	,305**	,236**	,637**	1	,337**	,259**
Sig. (bilateral)	,004	,000	,001	,000		,000	,000
N	204	203	204	204	204	204	204
A8 Correlación de Pearson	,310**	,287**	,164*	,365**	,337**	1	,754**
Sig. (bilateral)	,000	,000	,019	,000	,000		,000
N	204	203	204	204	204	204	204

A9	Correlación de Pearson	,229**	,233**	,141*	,378**	,259**	,754**	1
	Sig. (bilateral)	,001	,001	,044	,000	,000	,000	
	N	204	203	204	204	204	204	204

** . La correlación es significativa al nivel 0,01 (bilateral).

*. La correlación es significativa al nivel 0,05 (bilateral).

Así pues, tenemos los posibles factoriales siguientes:

ABU1 con ABU2

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,500
Prueba de esfericidad de Chi-cuadrado aproximado		73,743
Bartlett	gl	1
	Sig.	,000

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,554	77,680	77,680	1,554	77,680	77,680
2	,446	22,320	100,000			

Método de extracción: Análisis de Componentes principales.

Matriz de componentes^a

	Componente
	1
ABU1	,881
ABU2	,881

Método de extracción:

Análisis de componentes principales.

a. 1 componentes extraídos

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,711	2

AW1 con AW2 y AW3

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,625
Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	53,367
	gl	3
	Sig.	,000

Comunalidades

	Inicial	Extracción
AW1	1,000	,517
AW2	1,000	,514
AW3	1,000	,591

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,621	54,049	54,049	1,621	54,049	54,049
2	,735	24,492	78,541			
3	,644	21,459	100,000			

Matriz de componentes^a

	Componente
	1
AW1	,719
AW2	,717
AW3	,769

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,565	3

Escasa de porcentaje de explicación de varianza y bajo Cronbach. De hecho, las propias correlaciones eran muy “justitas”.

URS1, con AURS9, con AURS10 y AURS11

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,712
Prueba de esfericidad de Chi-cuadrado aproximado		172,269
Bartlett	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
URS1	1,000	,452
AURS9	1,000	,621
AURS10	1,000	,669
AURS11	1,000	,478

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la	% acumulado	Total	% de la	% acumulado
		varianza			varianza	
1	2,221	55,516	55,516	2,221	55,516	55,516
2	,726	18,158	73,673			
3	,651	16,267	89,940			
4	,402	10,060	100,000			

Quitando URS1

Matriz de componentes^a

	Componente
	1
AURS9	,843
AURS10	,817
AURS11	,726

Método de extracción:

Análisis de componentes principales.

a. 1 componentes extraídos

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,905	63,508	63,508	1,905	63,508	63,508
2	,659	21,980	85,488			
3	,435	14,512	100,000			

Método de extracción: Análisis de Componentes principales.

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,649
Prueba de esfericidad de Chi-cuadrado aproximado		120,776
Bartlett	gl	3
	Sig.	,000

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,701	3

Con A3, 4, 5, 6, 7, 8, 9

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,684
Prueba de esfericidad de Chi-cuadrado aproximado		389,994
Bartlett	gl	21
	Sig.	,000

Comunalidades

	Inicial	Extracción
A3	1,000	,239
A4	1,000	,387
A5	1,000	,354
A6	1,000	,569
A7	1,000	,662
A8	1,000	,851
A9	1,000	,845

Varianza total explicada							
Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	2,826	40,373	40,373	2,826	40,373	40,373	
2	1,080	15,428	55,801	1,080	15,428	55,801	
3	,994	14,202	70,003				
4	,827	11,816	81,819				
5	,685	9,785	91,603				
6	,361	5,160	96,764				
7	,227	3,236	100,000				

Quitando, inicialmente, A3 por su escasa contribución:

KMO y prueba de Bartlett		
Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,659
Prueba de esfericidad de Chi-cuadrado aproximado		358,305
Bartlett	gl	15
	Sig.	,000

Comunalidades		
	Inicial	Extracción
A4	1,000	,368
A5	1,000	,352
A6	1,000	,611
A7	1,000	,688
A8	1,000	,852
A9	1,000	,868

Varianza total explicada							
Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	2,658	44,306	44,306	2,658	44,306	44,306	
2	1,080	18,000	62,305	1,080	18,000	62,305	
3	,905	15,079	77,384				
4	,764	12,729	90,113				
5	,364	6,069	96,183				
6	,229	3,817	100,000				

Está claro que sobran también A4 y 5. Entonces:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,600
Prueba de esfericidad de	Chi-cuadrado aproximado	313,145
Bartlett	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
A6	1,000	,807
A7	1,000	,837
A8	1,000	,870
A9	1,000	,885

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	2,375	59,380	59,380	2,375	59,380	59,380	
2	1,023	25,582	84,962	1,023	25,582	84,962	
3	,373	9,335	94,297				
4	,228	5,703	100,000				

Método de extracción: Análisis de Componentes principales.

Matriz de componentes rotados^a

	Componente	
	1	2
A6	,244	,864
A7	,129	,906
A8	,907	,218
A9	,927	,160

Método de rotación:

Normalización Varimax con Kaiser.

a. La rotación ha convergido en 3 iteraciones.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,769	4

Se forman dos factores, agrupándose A6 con A7 y A8 con A9, explicando el 85% de la varianza, y con KMO de 0,7 y Alfa de 0,77.

En resumen, tras ver las correlaciones, podemos factorizar entre:

ABU1 y ABU2

AURS9, 10 y 11

A6 con A7

A8 con A9

De hecho, si los agrupamos, obtenemos los siguientes resultados:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,612
Prueba de esfericidad de Chi-cuadrado aproximado		533,070
Bartlett	gl	36
	Sig.	,000

Comunalidades

	Inicial	Extracción
ABU1	1,000	,785
ABU2	1,000	,772
AURS9	1,000	,718
AURS10	1,000	,668
AURS11	1,000	,531
A6	1,000	,827
A7	1,000	,842
A8	1,000	,867
A9	1,000	,892

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	2,574	28,602	28,602	2,574	28,602	28,602	
2	1,924	21,382	49,984	1,924	21,382	49,984	
3	1,381	15,343	65,326	1,381	15,343	65,326	
4	1,021	11,345	76,671	1,021	11,345	76,671	
5	,655	7,273	83,944				
6	,463	5,147	89,091				
7	,427	4,746	93,837				
8	,331	3,679	97,515				
9	,224	2,485	100,000				

Matriz de componentes rotados^a

	Componente			
	1	2	3	4
ABU1	-,020	,101	,031	,880
ABU2	,009	,062	,106	,870
AURS9	,847	,016	-,007	-,006
AURS10	,816	-,030	-,007	-,019
AURS11	,725	,065	,009	,014
A6	-,082	,253	,869	,003
A7	,073	,117	,895	,145
A8	,047	,891	,210	,165
A9	,015	,930	,159	,028

Que se asocian tal y como habíamos establecido.

Con un alfa de Cronbach aceptable

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,648	9

Todos juntos:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,611
Prueba de esfericidad de Chi-cuadrado aproximado		528,869
Bartlett	gl	36
	Sig.	,000

Comunalidades

	Inicial	Extracción
ABU1	1,000	,782
ABU2	1,000	,769
AURS9	1,000	,718
AURS10	1,000	,667
AURS11	1,000	,530
A6	1,000	,827
A7	1,000	,842
A8	1,000	,868
A9	1,000	,892

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	2,567	28,522	28,522	2,567	28,522	28,522	
2	1,927	21,416	49,938	1,927	21,416	49,938	
3	1,380	15,333	65,272	1,380	15,333	65,272	
4	1,020	11,332	76,604	1,020	11,332	76,604	
5	,655	7,279	83,883				
6	,469	5,211	89,094				
7	,427	4,746	93,839				
8	,332	3,690	97,530				
9	,222	2,470	100,000				

Método de extracción: Análisis de Componentes principales.

Matriz de componentes rotados^a

	Componente			
	1	2	3	4
ABU1	-,022	,101	,029	,878
ABU2	,003	,063	,102	,869
AURS9	,847	,018	-,012	-,020
AURS10	,816	-,030	-,007	-,019
AURS11	,725	,063	,010	,016
A6	-,086	,254	,869	-,002
A7	,072	,117	,896	,144
A8	,044	,892	,209	,161
A9	,017	,930	,161	,032

Método de rotación: Normalización Varimax con Kaiser.

a. La rotación ha convergido en 5 iteraciones.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,644	9

Quedan, pues, correlacionadas actuaciones sobre: copias de seguridad, **actividad en redes sociales**, disponibilidad de protecciones (antivirus-firewall), y “rastros” de actividad en el PC (archivos temporales, cookies, histórico), que definen el constructo “actividad” real que llevan a cabo los encuestados, incorporando cuatro nuevas variables (fac1, 2, 3 y 4) en la hoja excel que son el resumen de las otras 9 variables que fueron su origen. El valor que cada individuo, o sujeto de la muestra, toma en cada uno de los factores que representan a las variables originales, es la puntuación factorial, puesto que, en regresión trabajo con todas las variables o con los factores que las representan.

Tablas de frecuencia

A6

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	19	9,3	9,3	9,3
	2	13	6,4	6,4	15,7
	3	12	5,9	5,9	21,6
	4	47	23,0	23,0	44,6
	5	113	55,4	55,4	100,0
	Total	204	100,0	100,0	

A7

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	20	9,8	9,8	9,8
	2	12	5,9	5,9	15,7
	3	36	17,6	17,6	33,3
	4	50	24,5	24,5	57,8
	5	86	42,2	42,2	100,0
	Total	204	100,0	100,0	

A8

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	9	4,4	4,4	4,4
	2	28	13,7	13,7	18,1
	3	39	19,1	19,1	37,3
	4	58	28,4	28,4	65,7
	5	70	34,3	34,3	100,0
	Total	204	100,0	100,0	

A9

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	13	6,4	6,4	6,4
	2	22	10,8	10,8	17,2
	3	47	23,0	23,0	40,2
	4	65	31,9	31,9	72,1
	5	57	27,9	27,9	100,0
	Total	204	100,0	100,0	

ANEXO A3.2 - Resultados cuestionario definitivo (curso 2012-13)

Contraseñas:

AUP1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	4	2,1	2,1	2,1
	2	79	41,1	41,1	43,2
	3	109	56,8	56,8	100,0
	Total	192	100,0	100,0	

Estadísticos

AUP1

N	Válidos	192
	Perdidos	0
Media		2,55

El 2% no tiene passwords para sus accesos y el 41% tiene la misma. Media=2,55, debería →3

AUP2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	133	69,3	69,6	69,6
	2	47	24,5	24,6	94,2
	3	11	5,7	5,8	100,0
	Total	191	99,5	100,0	
Perdidos	Sistema	1	,5		
	Total	192	100,0		

Estadísticos

AUP2

N	Válidos	191
	Perdidos	1
Media		1,36

El 70% las mantiene fijas. Media= 1,36 cuando debería → 3

AUP3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	42	21,9	21,9	21,9
	2	19	9,9	9,9	31,8
	3	131	68,2	68,2	100,0
	Total	192	100,0	100,0	

Estadísticos

AUP3

N	Válidos	192
	Perdidos	0
Media		2,46

El 22% deja que el navegador grabe sus contraseñas. Media=2,46, debería → 3

A1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	65	33,9	34,0	34,0
	2	113	58,9	59,2	93,2
	3	13	6,8	6,8	100,0
	Total	191	99,5	100,0	
Perdidos	Sistema	1	,5		
Total		192	100,0		

Estadísticos

A1

N	Válidos	191
	Perdidos	1
Media		1,73

El 34% no usa password para acceder a la sesión de su PC. Solo el 6,8% usa diferentes claves para distintos accesos. Media=1,73, debería → 3

Tabla de contingencia AUP1 * AUP2 * AUP3

Recuento

AUP3			AUP2			Total
			1	2	3	
1	AUP1	1	2	0		2
		2	15	3		18
		3	18	4		22
		Total	35	7		42
2	AUP1	2	13		1	14
		3	5		0	5
		Total	18		1	19
3	AUP1	1	2	0	0	2
		2	32	13	2	47
		3	46	27	8	81
		Total	80	40	10	130
Total	AUP1	1	4	0	0	4
		2	60	16	3	79
		3	69	31	8	108
		Total	133	47	11	191

Con respecto a copias de seguridad:

ABU1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	24	12,5	12,5	12,5
	2	62	32,3	32,3	44,8
	3	35	18,2	18,2	63,0
	4	39	20,3	20,3	83,3
	5	32	16,7	16,7	100,0
Total		192	100,0	100,0	

El 13% no ha hecho nunca copias de seguridad de sus datos.

ABU2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	29	15,1	15,1	15,1
	2	7	3,6	3,6	18,8
	3	24	12,5	12,5	31,3
	4	108	56,3	56,3	87,5
	5	24	12,5	12,5	100,0
	Total	192	100,0	100,0	

Correlaciones

		ABU1	ABU2
ABU1	Correlación de Pearson	1	,581**
	Sig. (bilateral)		,000
	N	192	192
ABU2	Correlación de Pearson	,581**	1
	Sig. (bilateral)	,000	
	N	192	192

** . La correlación es significativa al nivel 0,01 (bilateral).

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,500
Prueba de esfericidad de Chi-cuadrado aproximado		77,947
Bartlett	gl	1
	Sig.	,000

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,581	79,036	79,036	1,581	79,036	79,036
2	,419	20,964	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,734	2

A2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	38	19,8	19,8	19,8
	2	7	3,6	3,6	23,4
	3	13	6,8	6,8	30,2
	4	46	24,0	24,0	54,2
	5	88	45,8	45,8	100,0
	Total	192	100,0	100,0	

Un 20% abre los correos de desconocidos para enterarse del contenido.

A3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	28	14,6	14,7	14,7
	2	59	30,7	30,9	45,5
	3	43	22,4	22,5	68,1
	4	57	29,7	29,8	97,9
	5	4	2,1	2,1	100,0
	Total	191	99,5	100,0	
Perdidos	Sistema	1	,5		
	Total	192	100,0		

A un 15% les importan poco las vulnerabilidades de seguridad.

Navegación por redes sociales:

AURS10

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	38	19,8	19,8	19,8
	2	88	45,8	45,8	65,6
	3	39	20,3	20,3	85,9
	4	17	8,9	8,9	94,8
	5	10	5,2	5,2	100,0
	Total	192	100,0	100,0	

AURS11

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	52	27,1	27,1	27,1
	2	62	32,3	32,3	59,4
	3	29	15,1	15,1	74,5
	4	29	15,1	15,1	89,6
	5	20	10,4	10,4	100,0
	Total	192	100,0	100,0	

El 41% suele contar, o lo hace siempre, sus “intimidades” por las redes sociales.

AURS3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	117	60,9	61,6	61,6
	2	30	15,6	15,8	77,4
	3	23	12,0	12,1	89,5
	4	10	5,2	5,3	94,7
	5	10	5,2	5,3	100,0
	Total	190	99,0	100,0	
Perdidos	Sistema	2	1,0		
	Total	192	100,0		

El 61% acepta las condiciones estándar para darse de alta en redes sociales, sin leerlas.

A(6-7):

Correlaciones

		A6	A7
A6	Correlación de Pearson	1	,741**
	Sig. (bilateral)		,000
	N	192	192
A7	Correlación de Pearson	,741**	1
	Sig. (bilateral)	,000	
	N	192	192

** . La correlación es significativa al nivel 0,01 (bilateral).

A(8-9):

		A8	A9
A8	Correlación de Pearson	1	,809**
	Sig. (bilateral)		,000
	N	192	192
A9	Correlación de Pearson	,809**	1
	Sig. (bilateral)	,000	
	N	192	192

** . La correlación es significativa al nivel 0,01 (bilateral).

Tablas de frecuencia

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	13	6,8	6,8	6,8
	2	6	3,1	3,1	9,9
	3	17	8,9	8,9	18,8
	4	48	25,0	25,0	43,8
	5	108	56,3	56,3	100,0
	Total	192	100,0	100,0	

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	12	6,3	6,3	6,3
	2	9	4,7	4,7	10,9
	3	24	12,5	12,5	23,4
	4	52	27,1	27,1	50,5
	5	95	49,5	49,5	100,0
	Total	192	100,0	100,0	

A8

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	16	8,3	8,3	8,3
	2	26	13,5	13,5	21,9
	3	35	18,2	18,2	40,1
	4	48	25,0	25,0	65,1
	5	67	34,9	34,9	100,0
	Total	192	100,0	100,0	

A9

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	21	10,9	10,9	10,9
	2	31	16,1	16,1	27,1
	3	37	19,3	19,3	46,4
	4	49	25,5	25,5	71,9
	5	54	28,1	28,1	100,0
	Total	192	100,0	100,0	

Conjunto factores A(6-9):

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,553
Prueba de esfericidad de	Chi-cuadrado aproximado	369,376
Bartlett	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
A6	1,000	,875
A7	1,000	,868
A8	1,000	,903
A9	1,000	,907

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	2,272	56,798	56,798	2,272	56,798	56,798	
2	1,281	32,037	88,835	1,281	32,037	88,835	
3	,259	6,482	95,317				
4	,187	4,683	100,000				

Método de extracción: Análisis de Componentes principales.

Matriz de componentes rotados^a

	Componente	
	1	2
A6	,100	,930
A7	,163	,917
A8	,938	,154
A9	,946	,113

Método de extracción: Análisis de componentes principales.

Método de rotación:

Normalización Varimax con Kaiser.

a. La rotación ha convergido en 3 iteraciones.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,746	4

Factores A(6-7):

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.	,500
Prueba de esfericidad de Chi-cuadrado aproximado	151,205
Bartlett	gl
	1
	Sig.
	,000

Comunalidades

	Inicial	Extracción
A6	1,000	,871
A7	1,000	,871

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,741	87,072	87,072	1,741	87,072	87,072
2	,259	12,928	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,852	2

Factores A(8-9):

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.	,500
Prueba de esfericidad de Chi-cuadrado aproximado	201,816
Bartlett	gl
	1
	Sig.
	,000

Comunalidades

	Inicial	Extracción
A8	1,000	,905
A9	1,000	,905

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,809	90,474	90,474	1,809	90,474	90,474
2	,191	9,526	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,895	2

Factores AURS (9-11):

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,628
Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	134,979
	gl	3
	Sig.	,000

Comunalidades

	Inicial	Extracción
AURS9	1,000	,720
AURS10	1,000	,747
AURS11	1,000	,473

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,940	64,668	64,668	1,940	64,668	64,668
2	,698	23,278	87,947			
3	,362	12,053	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,710	3

Factores AURS(9-10):

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,500
Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	98,567
	gl	1
	Sig.	,000

Comunalidades

	Inicial	Extracción
AURS9	1,000	,818
AURS10	1,000	,818

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,637	81,842	81,842	1,637	81,842	81,842
2	,363	18,158	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,772	2

ANEXO B – Preguntas sobre conocimientos (test)

Un usuario con conexión ADSL debe preocuparse por la seguridad

Una conexión inalámbrica con cifrado WEP tiene la misma seguridad que una conexión a través de cable

Cuando uso Wi-fi en la conexión en mi domicilio, estoy en riesgo

Al usar Wi-fi en la conexión en el centro de trabajo/estudio, estoy en riesgo

El símbolo del candado que se ve en los sitios más serios de e-commerce cuando doy los datos de mi tarjeta, me permiten hacer pagos seguros

Algunos programas informáticos de malware son inofensivos

La mayoría de los virus se diseñan para eliminar archivos y/o perjudicar nuestro sistema operativo y/o acceder a información confidencial

Un virus puede mutar y recombinarse con otros originando nuevos virus

Casi todos los usuarios pueden formar parte de redes zombi

Los troyanos y el phishing persiguen resultados similares

Algunos programas de adware (ejecución inmediata de publicidad) hacen un seguimiento de las prácticas del usuario y acaban siendo spyware

ANEXO B 1 – Respuestas a conocimientos (test)

Las respuestas correctas a las once preguntas formuladas, referidas en el Anexo B anterior, eran por orden:

Si – No – Si – No – No – No – Si – Si – Si – Si - Si

¿Un usuario medio con conexión DSL necesita preocuparse por la seguridad? - Si

Por supuesto. Si su computador está conectado a internet por largos períodos de tiempo, cualquier persona, en cualquier parte del mundo puede intentar en algún momento acceder a él.

Una de las más sencillas y efectivas medidas es asegurarse de instalar y configurar adecuadamente un cortafuegos que permita limitar las conexiones de entrada y de salida.

Sería un riesgo menos ante otros tipos de ataques como programas maliciosos o virus enviados vía e-mail o presentes por ejemplo, en soportes de almacenamiento.

¿Qué es WEP?

Wired Equivalent Privacy o "*Privacidad Equivalente a Cableado*", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Básicamente es un sistema de encriptación para redes inalámbricas ya sea con autenticación abierta o con clave compartida.

¿Estoy seguro si tengo un punto de acceso con WEP (Wired Equivalent Privacy), un algoritmo usado para proteger las comunicaciones inalámbricas de escuchas clandestinas? - No

¿Cómo puedo asegurar apropiadamente una conexión inalámbrica?

No, las sesiones WEP pueden ser descryptadas debido a un fallo en la implementación del protocolo.

Para poder atravesar esta seguridad se utilizan programas llamados Packet Sniffers y un crackeador WEP. Se captura una cantidad determinada de paquetes y luego mediante el crackeador se rompe el cifrado de la red. Un key cracker es un programa basado generalmente en matemáticas estadísticas que procesa los paquetes capturas para descifrar la clave WEP.

Hay que utilizar técnicas avanzadas de comunicaciones "tunelizadas" a través de SSH (Secure Shell, una aplicación de seguridad que permite la conexión entre computadoras de forma segura).

Accedo a mi correo y navego por la red a través de un enlace inalámbrico, ¿estoy en riesgo? Si-No

Eso depende de varios factores. La ubicación geográfica por ejemplo. Si estás en el medio del campo, es muy poco probable que puedan interceptar sus comunicaciones. *Si te encuentras en una ciudad o lugar muy poblado, rodeado de mucha tecnología, es probable que tengas vecinos que también utilicen redes inalámbricas, o existan aquellos que rastrean estas redes, pudiendo ambos visualizar todo el tráfico de datos que realices desde y hacia tu PC.*

¿Es seguro hacer compras en línea?

Sí y no, pero el consumidor final nunca está en posición de saberlo. En primer lugar, para mitigar riesgos, debería escanear asiduamente el sistema con uno (o más) antivirus al día, para asegurarse de no tener ningún programa del tipo "caballo de Troya" que permita a alguien tomar el control remoto de su PC, o que le de acceso a cualquier acción que el usuario pueda hacer en forma local.

Además, solo deberíamos hacer las compras en empresas razonablemente importantes, que cuidarán más sus datos una vez estén en su sistema, así como el flujo de estos en su red interna. Los problemas pueden ocurrir si ese vendedor usa contraseñas débiles, o el mismo no tiene el software actualizado, o es negligente en relación al manejo de los datos y procedimientos de backup de los mismos. Todo esto es menos probable que ocurra con empresas que son reconocidas o con más tiempo en el mercado.

¿El símbolo del candado que muestran los sitios de comercio electrónico más respetables cuando ingreso la información de mi tarjeta de crédito, me permiten hacer pagos seguros? No

No. El candado es solo un indicador de que el sitio utiliza SSL. Esta tecnología permite que el usuario confirme la identidad de los servidores, y que el servidor confirme la de los usuarios, además de cifrar todas las comunicaciones entre usuario y servidor.

Para ser eficaz el usuario debe ver el certificado que aparece al hacer doble clic sobre el candado, y confirmar que es de una autoridad certificadora de confianza, que la fecha es válida y que el nombre del certificado es idéntico al del sitio.

Esto es importante, debido a que es posible para cualquiera realizar un ataque del tipo "hombre-en-el-medio", situándose entre usuario y el servidor con el que se conecta para enviar la información, creando la ilusión de que todo es normal cuando de hecho se están interceptando todos sus datos.

Esto funciona porque se estableció (engañado) una conexión segura entre su computadora y el atacante, el cual a su vez, se conecta al servidor que deseabas conectarte. La comprobación del certificado puede prevenir esto. De cualquier modo hay otras maneras mucho más fáciles de conseguir la información de su tarjeta de crédito.

Malware

El malware suele ser representado con símbolos de peligro.

Malware (del inglés *malicious software*), también llamado badware, software malicioso o software malintencionado es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático es utilizado en muchas ocasiones de forma incorrecta para referirse a todos los tipos de malware, incluyendo los verdaderos virus.

El software es considerado malware en base a las intenciones del autor a la hora de crearlo. El término malware incluye virus, gusanos, troyanos, la mayoría de los rootkits, spyware, adware intrusivo, crimeware y otros software maliciosos e indeseables.

Malware no es lo mismo que software defectuoso, este último contiene bugs peligrosos pero no de forma intencionada.

En general, es fácil determinar si un programa es (o contiene) un malware: sus actividades son ocultas y no son anunciadas al usuario. Pero existen casos en que la distinción no es clara, provocando hasta demandas por parte de los desarrolladores de estos programas a los antivirus y anti espías que los detectan como malignos.

¿Qué es un virus informático?

Es un programa (código) dañino que pasa desapercibido hasta causar los daños, que se replica añadiendo una copia de sí mismo a otros programas. Se caracterizan por su capacidad de replicarse sin intervención o consentimiento del usuario y por su *capacidad de mutar y acomodarse en otros programas distintos al portador original*.

En informática, es un pequeño software que, al igual que un virus biológico, infecta a una computadora y se propaga en ella con diversos propósitos como daño, robo de información, molestia, etc. y por lo general intenta pasar desapercibido por el usuario el mayor tiempo posible. Los virus se incluyen dentro de los malwares (programas malignos).

El contagio por un virus suele producirlo el mismo usuario al ejecutar un programa que está infectado y toma los servicios básicos del sistema operativo para lograr sus objetivos. Suele quedar residente en memoria.

Lo más habitual es que los virus permanezcan ocultos en archivos del tipo ejecutable (.exe y .com), pero pueden existir en otros formatos.

Cada mes se crean cientos de nuevos virus. Algunos son relativamente inofensivos, pero la mayoría están diseñados para eliminar archivos, poner en peligro su información confidencial o dañar su sistema operativo. Tanto los PC como los Mac son vulnerables, y la última generación de virus hasta puede propagarse sin intervención humana. Para detenerlos, debe instalar software antivirus confiable y actualizarlo periódicamente.

¿Cómo se clasifican los virus informáticos?

Se clasifican por sus diferentes propósitos, comportamientos y consecuencias, así:
Genérico o de archivo: se aloja como una especie de parásito dentro de un archivo ejecutable y se replica a otros programas durante la ejecución.
Mutante: en lugar de copiarse genera copias modificadas de sí mismo.
Recombinable: se unen, recombinan códigos y crean nuevos virus.

Caza recompensas o BOUNTY HUNTER: porque atacan un producto antivirus.
Específico de redes: coleccionan contraseñas de acceso a la red para luego reproducirse e iniciar sus rutinas destructivas en los computadores conectados.
De sector de arranque: se alojan en la sección de disco o las instrucciones se cargan en memoria al iniciar el sistema.

Macro: infectan los macros que acompañan una aplicación específica, entendiendo por macro como el conjunto de instrucciones que ejecutan una tarea particular activada por una aplicación específica como Word o Excel.

De Internet: se alojan en el código subyacente de las páginas Web. Así cuando el usuario accede a esos sitios en internet el virus se descarga y ejecuta modificando o destruyendo la información almacenada.

Humanos: hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, falsificación, robo de contraseñas

Propósitos de los troyanos

Los troyanos están diseñados para permitir a un individuo el acceso remoto a un sistema. Una vez ejecutado el troyano, el individuo puede acceder al sistema de forma remota y realizar diferentes acciones sin necesitar permiso. Las acciones que el individuo puede realizar en el equipo remoto dependen de los privilegios que tenga el usuario en el ordenador remoto y de las características del troyano.

Algunas de las operaciones que se pueden llevar a cabo en el ordenador remoto son:

- Utilizar la máquina como parte de una botnet (por ejemplo para realizar ataques de denegación de servicio o envío de spam).
- Instalación de otros programas (incluyendo otros programas maliciosos).
- Robo de información personal: información bancaria, contraseñas, códigos de seguridad.
- Borrado, modificación o transferencia de archivos (descarga o subida).

- Ejecutar o terminar procesos.
- Apagar o reiniciar el equipo.
- Monitorizar las pulsaciones del teclado.
- Realizar capturas de pantalla.
- Ocupar el espacio libre del disco duro con archivos inútiles.
- Borra el disco duro

Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social *caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria)*. El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Dado el creciente número de denuncias de incidentes relacionados con el *phishing*, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica y campañas para prevenir a los usuarios con la aplicación de medidas técnicas a los programas.

Efectos del adware

Los anuncios emergentes aparecen durante la navegación web en el navegador como una ventana emergente o también durante el uso de programa del ordenador. Esta publicidad es molesta en algunos casos, pero lo que más molesta es que deteriora el rendimiento del sistema. *El adware también puede recopilar información del usuario, lo que provoca preocupación por la privacidad.*

ANEXO B2 – Calificaciones

En 1º de Teleco se elimina el elemento 31 por escasez de respuestas y, posteriormente, el 2, 4, 29, 30, 34 por falta de respuestas de variables necesarias y el 14 por falta de coherencia. Quedan 31 encuestados. Otros tres alumnos no proporcionan suficientes respuestas en las variables latentes.

nota media: 2,7
desv. típica 2,7
nº aprobados 12,0
% " 38,7

En 4º de Teleco eliminados los individuos 2, 3, 24, 37-40 del listado inicial por no contestar a la mayoría de preguntas y el 37 y 41 por falta de coherencia. Quedan 40. Un alumno deja sin responder a bastantes variables latentes

Nota media 2,7
Desv. Típica 2,0
nº aprobados 12,0
% aprobados 30

Eliminado el individuo 22 de la lista inicial de 5º de Teleco por no contestar a la mayoría de cuestiones. Y, posteriormente se elimina al 17 por falta de respuestas de variables necesarias, además del 2 y el 5 por falta de coherencia. Quedan 20.

nota media 4,2
Desv. Típica 2,3
nº aprobados 13,0
% aprobados 65

Eliminados los elementos 6,16,18,26,29,33,37,81,93,113,114,121,145,148,150-153 de Informática por escasez de respuestas. Datos del 110 por la media y/o mayoría (edad y sexo). Posteriormente, se eliminan el 2,4,11,17,22,25,31,49,57,74,82,90,91,105, 106, 109, 111, 112, 122, 130, 131, 135 por falta de respuestas de variables necesarias. Y los 22, 38, 42, 45, 80, 89, 95 por falta de coherencia. Quedan 106 encuestados. Otro alumno no proporciona respuestas suficientes a las variables latentes

nota media	3,7
desv. Típica	1,9
nº aprobados	52,0
% aprobados	49,1

En el curso anterior, entre los 204 alumnos de Informática encuestados:

Media	3,6
Desv Típica	2,26
aprobados	102
%	50

ANEXO C – Cálculo de regresiones, curso 2011-12

Tablas de contingencia

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
A6 * A7	202	99,0%	2	1,0%	204	100,0%

Tabla de contingencia A6 * A7

Recuento

		A7					Total
		1	2	3	4	5	
A6	1	13	1	0	2	3	19
	2	2	7	1	3	0	13
	3	0	0	12	0	0	12
	4	0	1	12	30	2	45
	5	5	3	11	13	81	113
Total		20	12	36	48	86	202

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	282,917 ^a	16	,000
Razón de verosimilitudes	212,881	16	,000
Asociación lineal por lineal	81,598	1	,000
N de casos válidos	202		

a. 14 casillas (56,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,71.

Luego, teniendo como ausentes dos valores (uno de A6 y otro de A7 - individuos 93 y 167), en los que el valor presente es 4, vamos a adjudicar valor también de 4 al perdido.

Por otra parte, con un valor perdido para AURS10 en el individuo 74, siendo 3 AURS9 y 11:

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
AURS9 * AURS10 * AURS11	203	99,5%	1	,5%	204	100,0%

Tabla de contingencia AURS9 * AURS10 * AURS11

Recuento

AURS11			AURS10					Total
			1	2	3	4	5	
1	AURS9	1	10	4	1	1		16
		2	7	12	5	1		25
		3	0	5	2	0		7
		4	0	1	0	1		2
		5	0	0	1	0		1
	Total		17	22	9	3		51
2	AURS9	1	5	0	0	0	0	5
		2	3	17	5	3	0	28
		3	1	4	2	5	0	12
		4	1	3	3	2	1	10
		5	1	1	0	1	3	6
	Total		11	25	10	11	4	61
3	AURS9	1	0	1	0	0		1
		2	3	8	4	0		15
		3	0	5	14	2		21
		4	0	4	2	0		6
	Total		3	18	20	2		43
4	AURS9	1	1	0	0	0	0	1
		2	0	4	1	1	0	6
		3	0	4	1	1	0	6
		4	0	0	2	5	1	8
		5	0	0	1	0	0	1
	Total		1	8	5	7	1	22
5	AURS9	1	1	0	1	0	0	2
		2	1	0	2	1	0	4
		3	0	2	1	2	0	5
		4	0	1	3	2	1	7
	5	0	2	0	2	4	8	

	Total		2	5	7	7	5	26
Total	AURS9	1	17	5	2	1	0	25
		2	14	41	17	6	0	78
		3	1	20	20	10	0	51
		4	1	9	10	10	3	33
		5	1	3	2	3	7	16
	Total		34	78	51	30	10	203

Comprobamos lo lógico de asignar el valor 3 al ausente, pues así han respondido en 14/21 casos

Regresión: Variable dependiente = $\beta_0 + \beta_1.V_1 + \beta_2.V_2 + \beta_3.V_3 + \beta_4.V_4 + \epsilon = Y$

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	At5, At1, At4, At2	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: At3

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación
1	,775 ^a	,600	,592	,589

a. Variables predictoras: (Constante), At5, At1, At4, At2

b. Variable dependiente: At3

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	101,494	4	25,373	73,100	,000 ^a
	Residual	67,686	195	,347		
	Total	169,180	199			

a. Variables predictoras: (Constante), At5, At1, At4, At2

b. Variable dependiente: At3

		Coeficientes ^a						
		Coeficientes no estandarizados		Coeficientes tipificados		Intervalo de confianza de 95,0% para B		
Modelo		B	Error típ.	Beta	t	Sig.	Límite inferior	Límite superior
1	(Constante)	,652	,185		3,528	,001	,287	1,016
	At1	,293	,053	,318	5,571	,000	,189	,396
	At2	,262	,068	,277	3,851	,000	,128	,396
	At4	,125	,061	,142	2,045	,042	,004	,246
	At5	,170	,070	,180	2,434	,016	,032	,307

a. Variable dependiente: At3

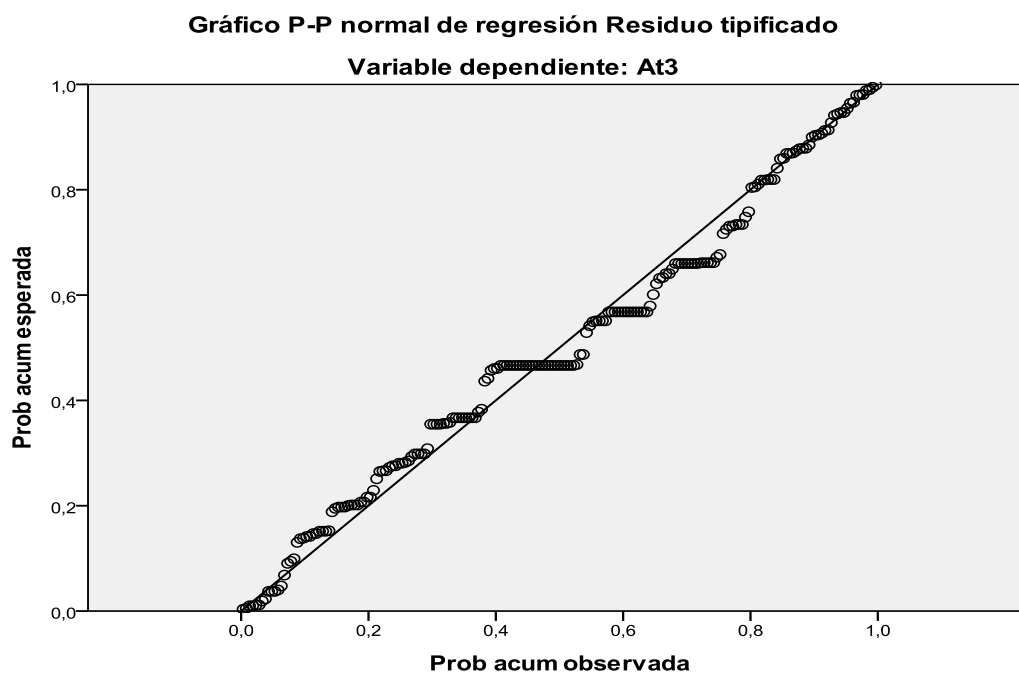
Como la R^2 corregida es 0,592, es muy aceptable y la significatividad es $\leq 0,001$ indica que hay relación lineal. Los intervalos de confianza nos dicen el margen de confianza, al 95%, de las β .

Tenemos ausente el valor de At3 en los individuos 66 (2 3 ? 2 3) y 78 (4 4 ? 3 4), obtendremos:

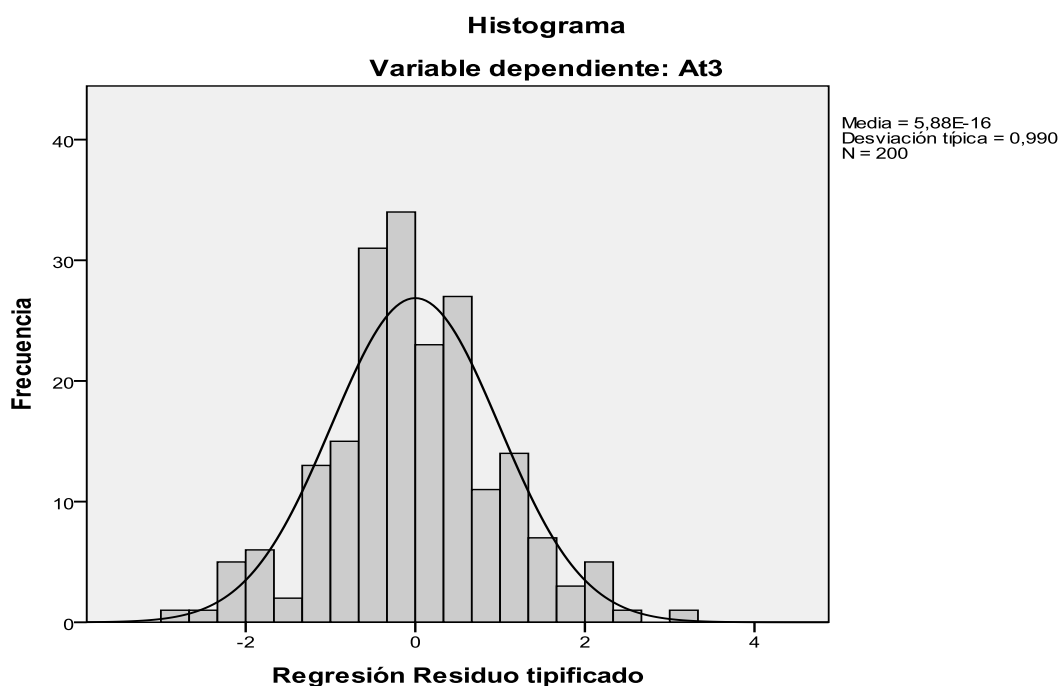
$$At3 = \beta_0 + \beta_1.V1 + \beta_2.V2 + \beta_3.V3 + \beta_4.V4 + \varepsilon = 0,652 + 0,293 \times At1 + 0,262 \times At2 + 0,125 \times At4 + 0,17 \times At5$$

Por lo que At3 valdrá 2,784 (con el 95% de confianza) \rightarrow 3 en 66, y 3,927 \rightarrow 4, en el 78

Adicionalmente, podemos comprobar en el gráfico P-P que hay normalidad pues la probabilidad acumulada de los residuos se ajusta a la diagonal



con:



Análogamente, necesitamos averiguar el valor de At4 en el sujeto 71, que ha dado las siguientes respuestas: 4 3 3 ? 4

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	At5, At1, At3, At2	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: At4

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación
1	,764 ^a	,583	,575	,682

a. Variables predictoras: (Constante), At5, At1, At3, At2

b. Variable dependiente: At4

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	126,887	4	31,722	68,265	,000 ^a
	Residual	90,613	195	,465		
	Total	217,500	199			

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	126,887	4	31,722	68,265	,000 ^a
	Residual	90,613	195	,465		
	Total	217,500	199			

a. Variables predictoras: (Constante), At5, At1, At3, At2

b. Variable dependiente: At4

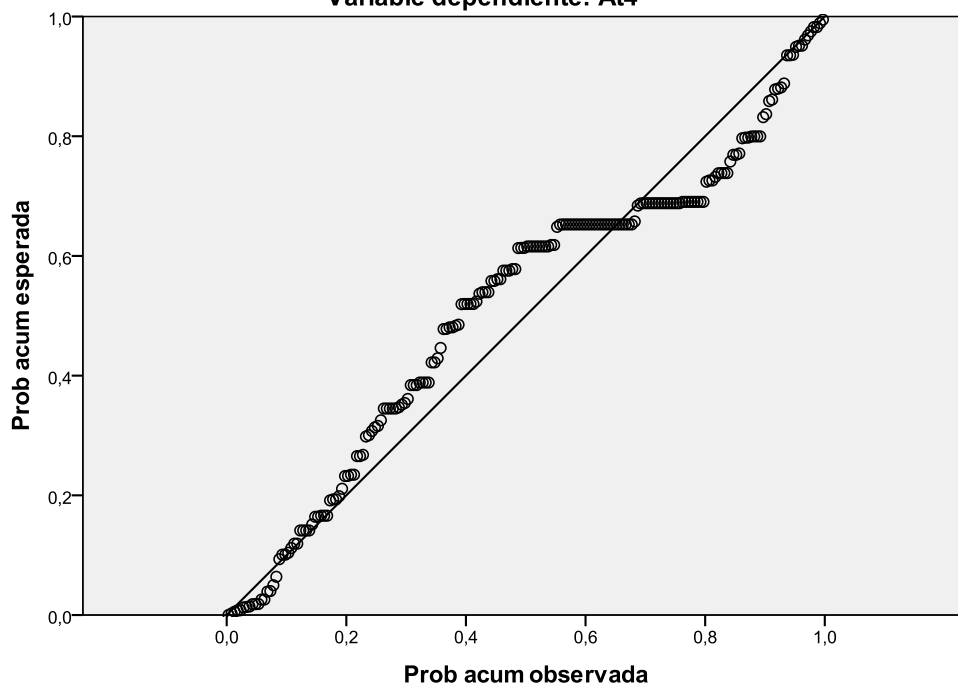
Coefficientes^a

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza de 95,0% para B	
		B	Error típ.	Beta			Límite inferior	Límite superior
1	(Constante)	-,001	,220		-,003	,998	-,435	,435
	At1	,071	,065	,068	1,090	,277	-,058	,216
	At2	,234	,080	,218	2,927	,004	,076	,392
	At3	,168	,082	,148	2,045	,042	,006	,321
	At5	,461	,075	,431	6,145	,000	,313	,609

a. Variable dependiente: At4

Gráfico P-P normal de regresión Residuo tipificado

Variable dependiente: At4



Obtenemos el valor:

$$-0.001 + 0.071 \times 4 + 0.234 \times 3 + 0.168 \times 3 + 0.461 \times 4 = -0.001 + 0.284 + 0.702 + 0.504 + 1.844 = 3.333 \rightarrow 3$$

Finalmente, para los valores de Atracción, debemos generar el valor perdido de At5 en el encuestado 159, que ha respondido 2 1 2 2 ?

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación
1	,798 ^a	,637	,629	,596

a. Variables predictoras: (Constante), At4, At1, At2, At3

b. Variable dependiente: At5

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	121,483	4	30,371	85,494	,000 ^a
	Residual	69,272	195	,355		
	Total	190,755	199			

a. Variables predictoras: (Constante), At4, At1, At2, At3

b. Variable dependiente: At5

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficients tipificados		t	Sig.	Intervalo de confianza de 95,0% para B	
		B	Error típ.	Beta				Límite inferior	Límite superior
1	(Constante)	,489	,190			2,581	,011	,115	,861
	At1	,026	,057	,027		,459	,647	-,086	,138
	At2	,343	,067	,341		5,120	,000	,211	,475
	At3	,174	,071	,164		2,434	,016	,033	,315
	At4	,352	,057	,376		6,145	,000	,239	,485

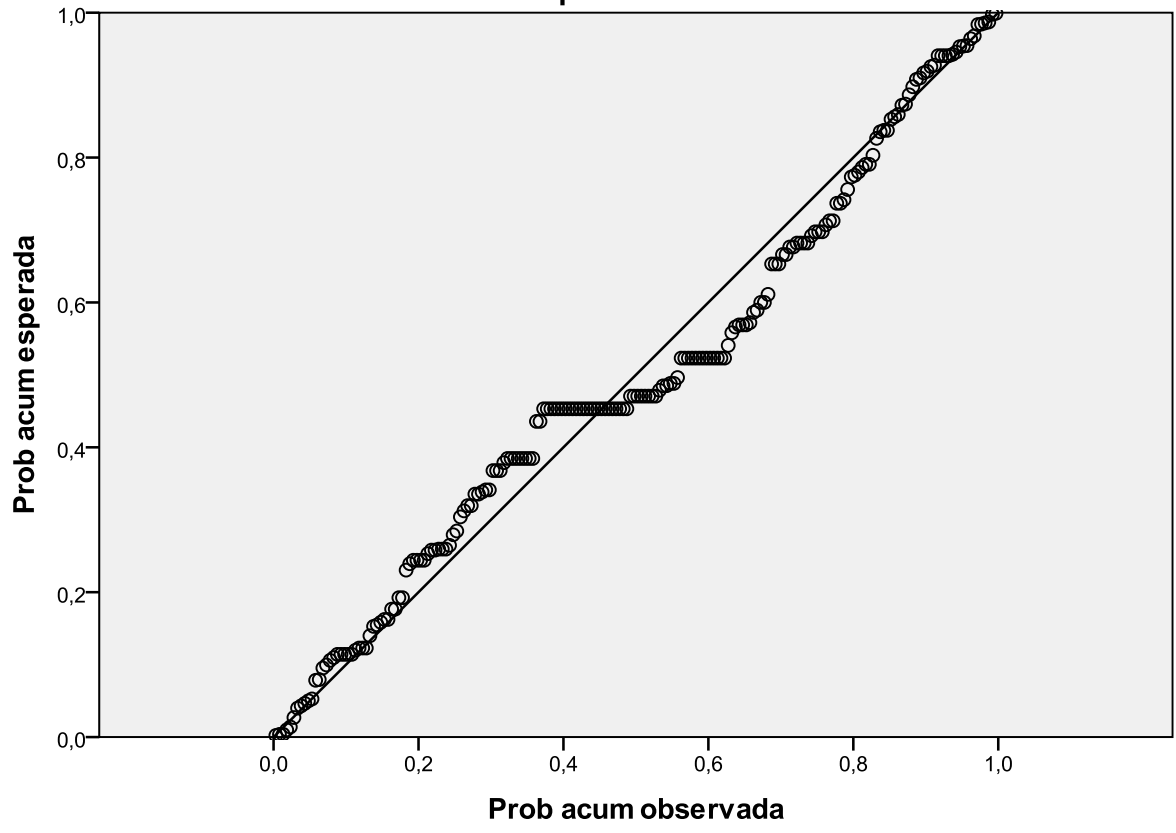
a. Variable dependiente: At5

Nos sale:

$$0,489 + 0,026 \times 2 + 0,343 + 0,174 \times 2 + 0,352 \times 2 = 1,936 \rightarrow 2$$

Gráfico P-P normal de regresión Residuo tipificado

Variable dependiente: At5



Otros valores ausentes son, en los encuestados 110 y 196, el valor de E2. Así que:

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación
1	,567 ^a	,322	,315	,922

a. Variables predictoras: (Constante), E5, E3

b. Variable dependiente: E2

Nos aparece un error a tener en cuenta, con una R² dudosa.

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	80,253	2	40,127	47,240	,000 ^a
	Residual	169,034	199	,849		
	Total	249,287	201			

a. Variables predictoras: (Constante), E5, E3

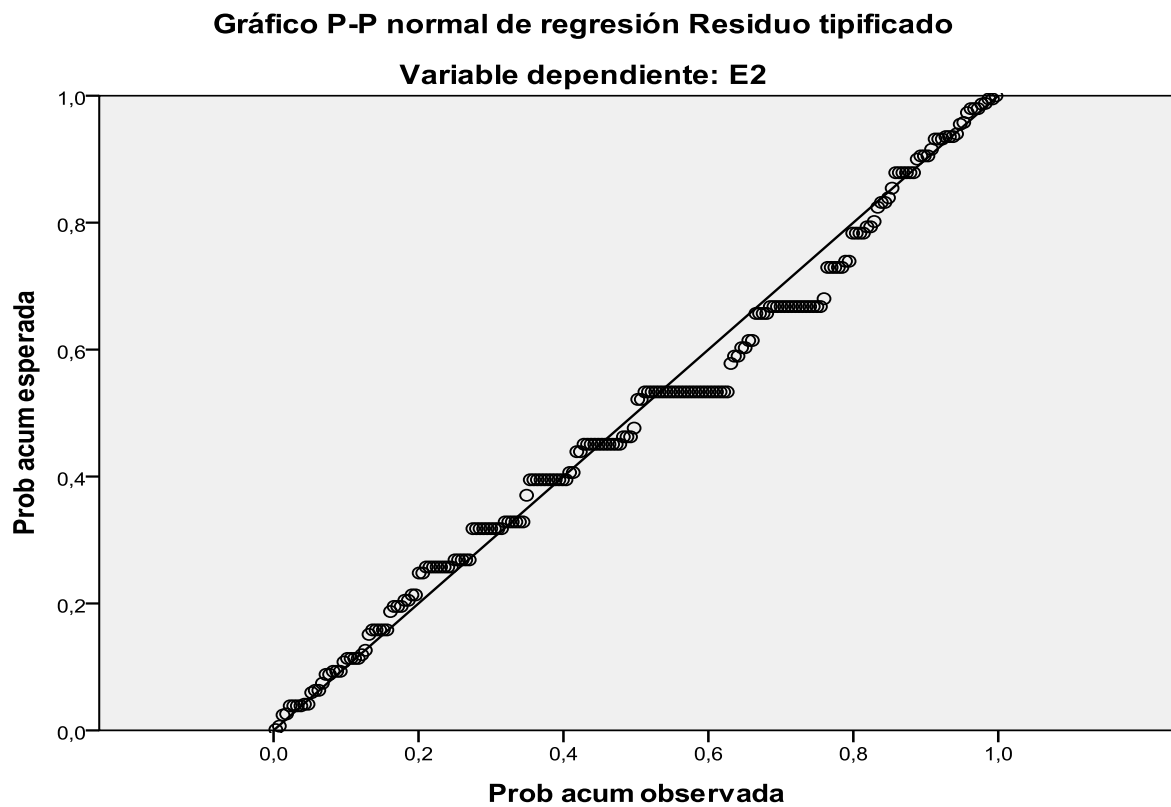
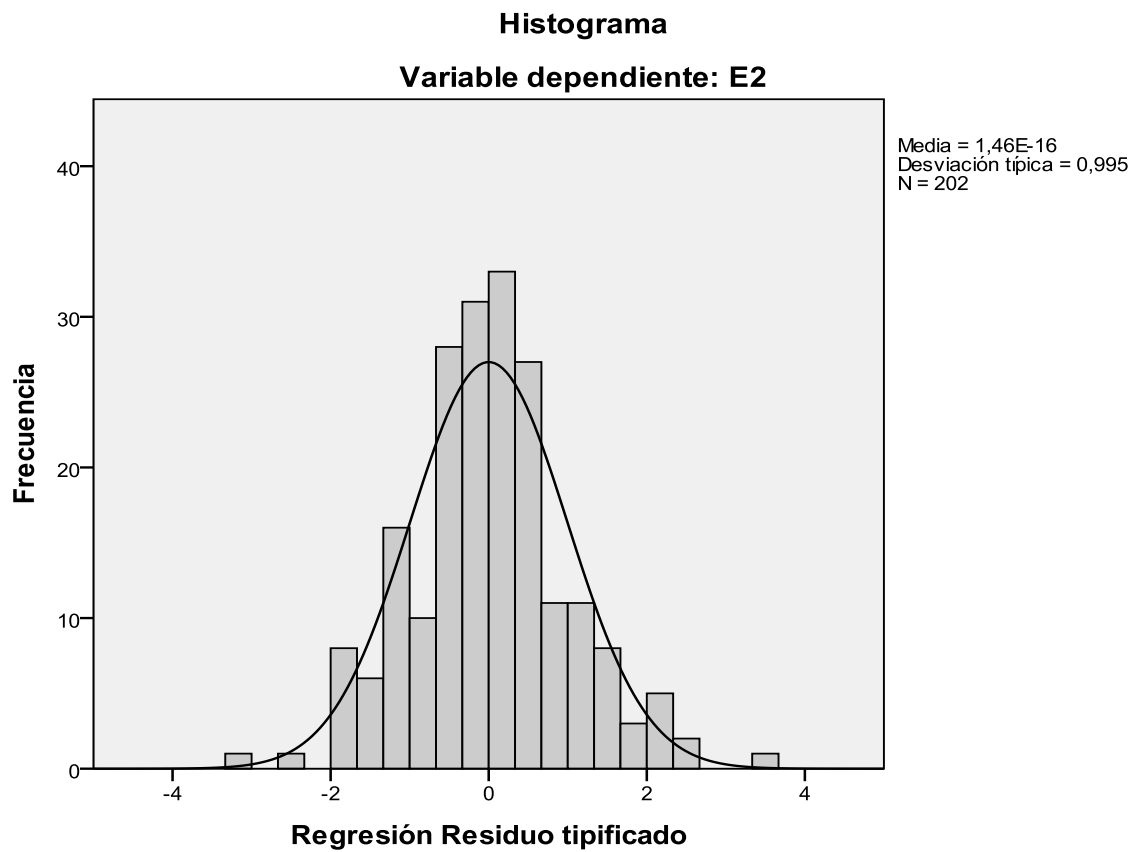
b. Variable dependiente: E2

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza de 95,0% para B	
		B	Error típ.	Beta			Límite inferior	Límite superior
1	(Constante)	,891	,240		3,718	,000	,419	1,3
	E3	,486	,067	,469	7,221	,000	,354	,6
	E5	,191	,071	,175	2,692	,008	,051	,3

a. Variable dependiente: E2

Tanto 110 como 196 respondieron ? 3 4, así que obtenemos:

$$0,891 + 0,486 \times 3 + 0,191 \times 4 = 3,113 \rightarrow 3$$



Con el último constructo, tenemos valores ausentes en U4 para el sujeto 93 y en U5 para el 129.

Así que:

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación
1	,793 ^a	,628	,619	,517

a. Variables predictoras: (Constante), U5, U2, E1, C4, U1

b. Variable dependiente: U4

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	88,310	5	17,662	66,204	,000 ^a
	Residual	52,289	196	,267		
	Total	140,599	201			

a. Variables predictoras: (Constante), U5, U2, E1, C4, U1

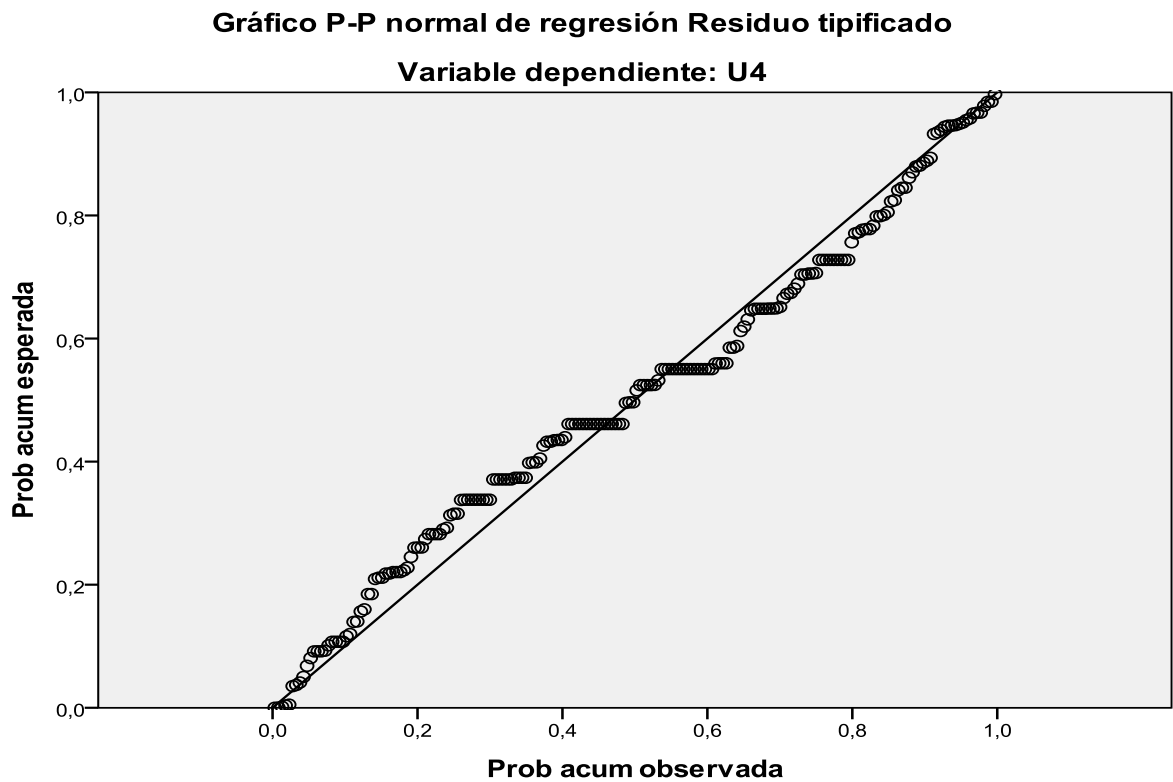
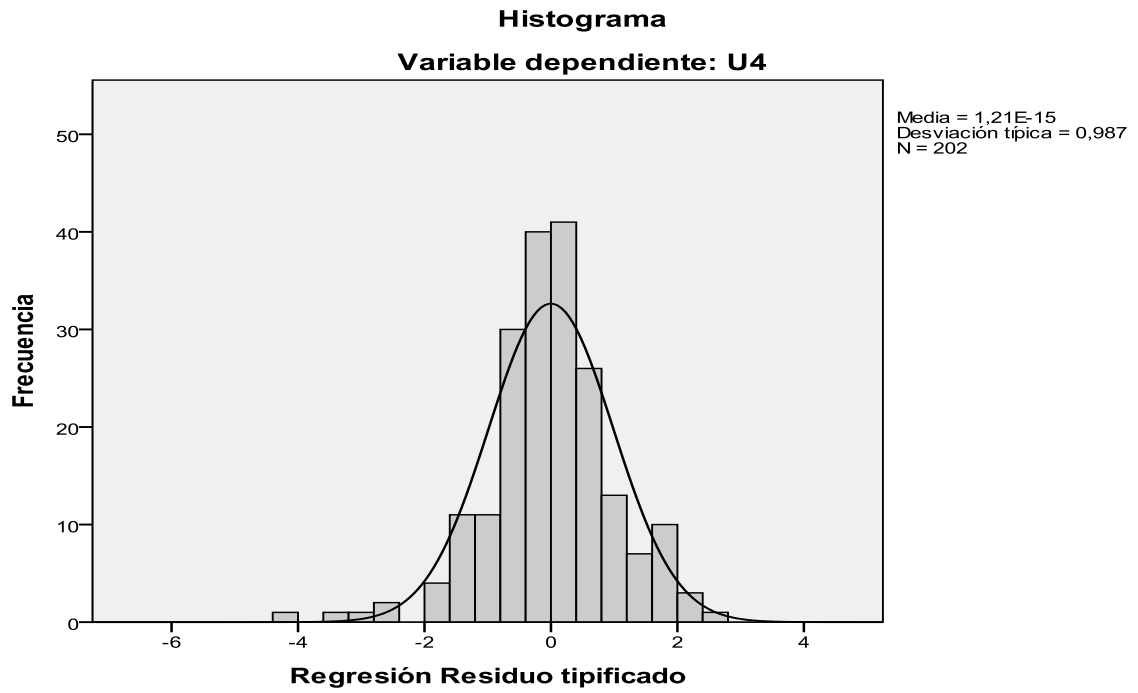
b. Variable dependiente: U4

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza de 95,0% para B	
		B	Error típ.	Beta			Límite inferior	Límite superior
		1	(Constante)	,514			,200	
	C4	,166	,060	,168	2,760	,006	,047	,285
	E1	,082	,050	,097	1,644	,102	-,016	,180
	U1	,046	,053	,056	,867	,387	-,058	,150
	U2	,120	,049	,153	2,436	,016	,023	,282
	U5	,471	,054	,491	8,731	,000	,365	,597

a. Variable dependiente: U4

$$U4 = 0,514 + 0,166 \times 2 + 0,082 \times 3 + 0,046 \times 5 + 0,12 \times 3 + 0,471 \times 3 = 3,095 \rightarrow 3$$



Para el último caso:

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación
1	,753 ^a	,567	,556	,580

a. Variables predictoras: (Constante), U4, U1, E1, C4, U2

b. Variable dependiente: U5

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	86,433	5	17,287	51,365	,000 ^a
	Residual	65,963	196	,337		
	Total	152,396	201			

a. Variables predictoras: (Constante), U4, U1, E1, C4, U2

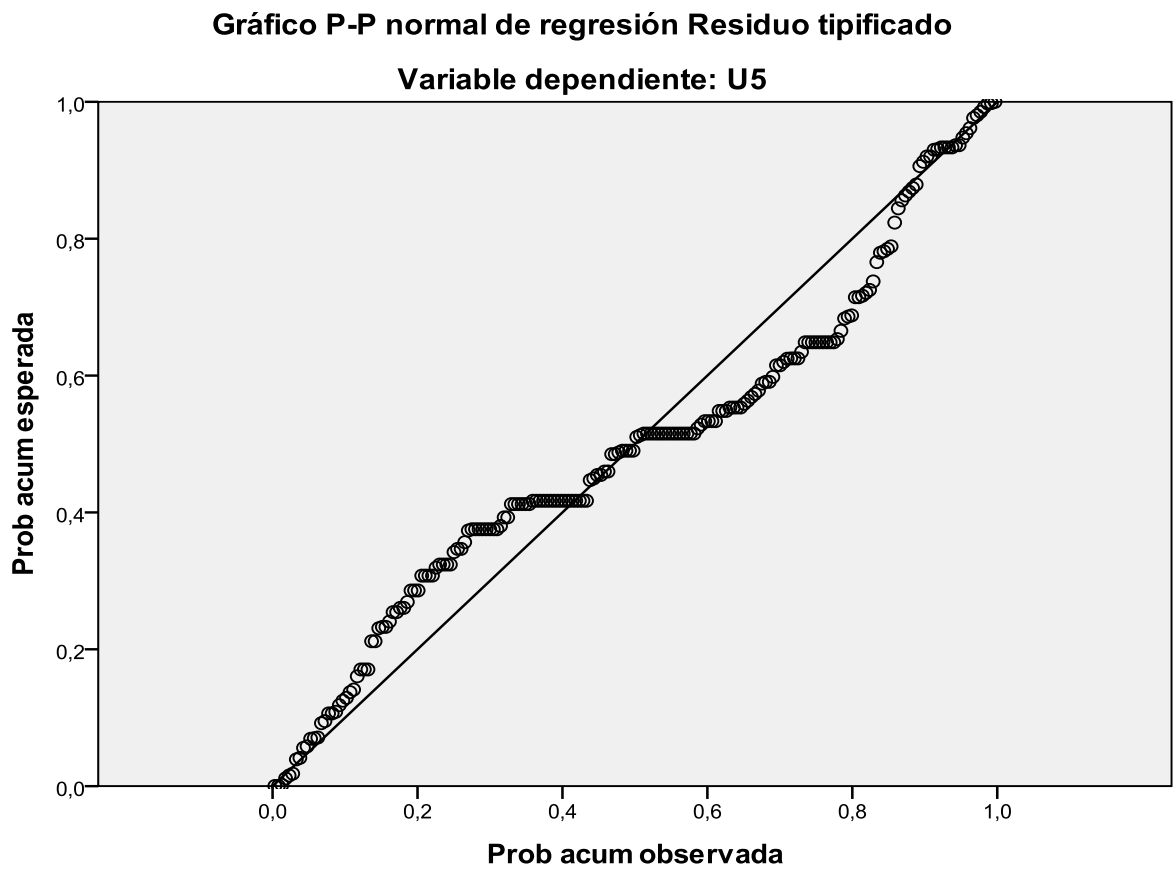
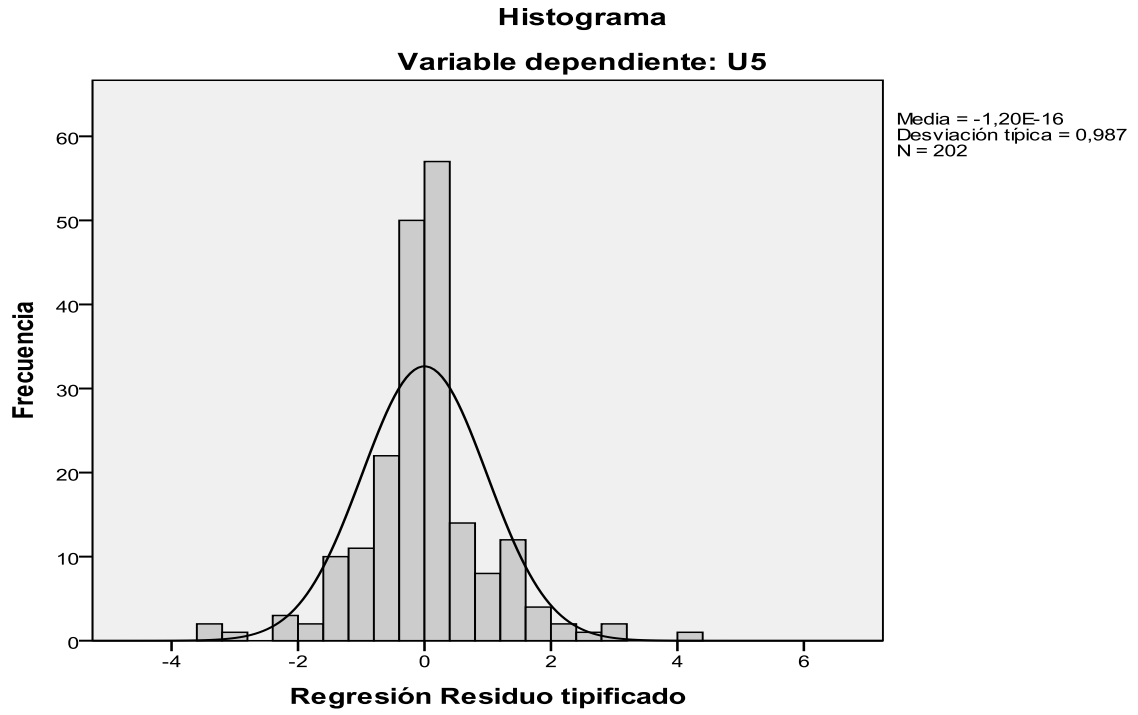
b. Variable dependiente: U5

Coeficientes^a

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza de 95,0% para B	
		B	Error típ.	Beta			Límite inferior	Límite superior
1	(Constante)	,696	,223		3,127	,002	,257	1,13
	C4	,092	,068	,090	1,344	,180	-,043	,22
	E1	,107	,056	,122	1,920	,056	-,003	,22
	U1	,055	,059	,065	,935	,351	-,061	,11
	U2	,007	,056	,009	,131	,896	-,103	,11
	U4	,594	,068	,571	8,731	,000	,460	,72

a. Variable dependiente: U5

$$U5 = 0,696 + 0,092 \times 4 + 0,107 \times 3 + 0,055 \times 4 + 0,007 \times 5 + 0,594 \times 3 = 3,522 \rightarrow 4$$



ANEXO C.1 – Cálculo de factores, curso 2011-12

En primer lugar hacemos un análisis factorial exploratorio para comprobar la “calidad” de las variables observables con las que queremos medir nuestras variables latentes, o constructos (atracción, confianza, estrés y utilidad).

Para lograrlo, con SPSS, procesamos conjuntamente las veinte variables y observamos como las agrupa el propio análisis estadístico, obteniendo los siguientes resultados:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,906
Prueba de esfericidad de Chi-cuadrado aproximado		2092,095
Bartlett	gl	190
	Sig.	,000

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	8,089	40,445	40,445	8,089	40,445	40,445	
2	2,000	9,998	50,443	2,000	9,998	50,443	
3	1,411	7,053	57,496	1,411	7,053	57,496	
4	1,002	5,009	62,505	1,002	5,009	62,505	
5	,984	4,922	67,427				
6	,810	4,050	71,476				
7	,688	3,442	74,918				
8	,586	2,928	77,846				
9	,579	2,897	80,743				
10	,543	2,714	83,458				
11	,516	2,582	86,040				
12	,439	2,197	88,236				
13	,420	2,098	90,334				
14	,353	1,763	92,097				
15	,346	1,730	93,827				
16	,325	1,623	95,450				
17	,266	1,332	96,782				
18	,241	1,206	97,988				
19	,217	1,085	99,073				
20	,185	,927	100,000				

Método de extracción: Análisis de Componentes principales.

Es decir, con una significatividad muy alta ($KMO= 0.906$ y $Sig<0.01$) se explica el 62,5% de la varianza.

Comunalidades		
	Inicial	Extracción
At1	1,000	,579
At2	1,000	,750
At3	1,000	,736
At4	1,000	,735
At5	1,000	,786
C1	1,000	,286
C2	1,000	,498
C3	1,000	,668
C4	1,000	,597
C5	1,000	,456
E1	1,000	,625
E2	1,000	,678
E3	1,000	,687
E4	1,000	,550
E5	1,000	,559
U1	1,000	,696
U2	1,000	,687
U3	1,000	,594
U4	1,000	,689
U5	1,000	,644

Método de extracción: Análisis de Componentes principales.

Donde vemos que la contribución de la variable C1 (<0.5) al factorial, es escasa, Si la eliminamos, nos queda:

KMO y prueba de Bartlett		
Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,907
Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	2006,353
	gl	171
	Sig.	,000

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	7,858	41,355	41,355	7,858	41,355	41,355	
2	1,989	10,468	51,823	1,989	10,468	51,823	
3	1,408	7,413	59,236	1,408	7,413	59,236	
4	1,002	5,272	64,508	1,002	5,272	64,508	
5	,814	4,283	68,791				
6	,696	3,663	72,453				
7	,657	3,458	75,911				
8	,583	3,067	78,979				
9	,579	3,047	82,025				
10	,518	2,727	84,752				
11	,496	2,609	87,361				
12	,439	2,312	89,673				
13	,356	1,873	91,546				
14	,351	1,846	93,392				
15	,328	1,727	95,118				
16	,270	1,423	96,541				
17	,253	1,329	97,870				
18	,217	1,144	99,014				
19	,187	,986	100,000				

Método de extracción: Análisis de Componentes principales.

Matriz de componentes rotados^a

	Componente			
	1	2	3	4
At1	,610	,311	,046	,329
At2	,774	,347	,101	,149
At3	,758	,255	,026	,310
At4	,834	,164	,023	,105
At5	,847	,194	,147	,095
C2	,518	,397	,152	,175
C3	,231	,178	-,094	,749
C4	,366	,556	,127	,374
C5	,167	,170	,054	,642
E1	,339	,543	,385	,239
E2	,036	,046	,802	,182
E3	-,040	,054	,828	,027

E4	,442	,395	,453	-,102
E5	,218	,143	,677	-,201
U1	,300	,775	-,038	,035
U2	,327	,764	,006	-,027
U3	,149	,609	,092	,449
U4	,229	,730	,190	,291
U5	,150	,699	,214	,307

Método de extracción: Análisis de componentes principales.

Método de rotación: Normalización Varimax con Kaiser.

a. La rotación ha convergido en 6 iteraciones.

Un factor (columna 1) lo determinan, exclusivamente, las variables de Atracción y C2.

Otro factor (columna 3) está formado por cuatro de las cinco variables (E2-5) de Estrés.

Un tercer factor (columna 2) lo forman las variables utilidad (U1-5) y C4 y E1

Y el último factor por C3 y C5.

Tenemos cuatro factores:

At1-5, C2

E2-5

C4, E1, U1-5

C3, C5

Veamos las alfas de Cronbach:

1er factor

Estadísticos de fiabilidad	
Alfa de Cronbach	N de elementos
,895	6

2°

Estadísticos de fiabilidad	
Alfa de Cronbach	N de elementos
,723	4

3°

Estadísticos de fiabilidad	
Alfa de Cronbach	N de elementos
,885	7

y 4º

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,475	2

El análisis de fiabilidad de este último factor, además de ser escasas (para AMOS) las variables que lo componen, nos aconsejan desestimarlos.

Vamos a estudiar cada uno de los factores, independientemente.

El primero está formado por las variables At1-At5, C2

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,895
Prueba de esfericidad de Chi-cuadrado aproximado		681,678
Bartlett	gl	15
	Sig.	,000

Comunalidades

	Inicial	Extracción
At1	1,000	,576
At2	1,000	,757
At3	1,000	,730
At4	1,000	,682
At5	1,000	,738
C2	1,000	,473

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	3,956	65,937	65,937	3,956	65,937	65,937
2	,608	10,127	76,064			
3	,555	9,253	85,317			
4	,333	5,555	90,872			
5	,293	4,889	95,761			
6	,254	4,239	100,000			

Método de extracción: Análisis de Componentes principales.

**Matriz de
componentes^a**

	Componente
	1
At1	,759
At2	,870
At3	,854
At4	,826
At5	,859
C2	,688

Método de extracción:

Análisis de
componentes
principales.

a. 1 componentes
extraídos

Si eliminamos C2 (variable con menor carga factorial), nos queda:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,870
Prueba de esfericidad de	Chi-cuadrado aproximado	598,806
Bartlett	gl	10
	Sig.	,000

Comunalidades

	Inicial	Extracción
At1	1,000	,593
At2	1,000	,765
At3	1,000	,738
At4	1,000	,708
At5	1,000	,750

Método de extracción: Análisis de
Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la	% acumulado	Total	% de la	% acumulado
		varianza			varianza	
1	3,555	71,091	71,091	3,555	71,091	71,091
2	,555	11,105	82,196			

3	,342	6,836	89,033		
4	,294	5,874	94,907		
5	,255	5,093	100,000		

Método de extracción: Análisis de Componentes principales.

Matriz de componentes^a

	Componente
	1
At1	,770
At2	,875
At3	,859
At4	,841
At5	,866

Con

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,897	5

Y unas correlaciones:

Correlaciones

		At1	At2	At3	At4	At5
At1	Correlación de Pearson	1	,582**	,648**	,524**	,532**
	Sig. (bilateral)		,000	,000	,000	,000
	N	204	204	204	204	204
At2	Correlación de Pearson	,582**	1	,694**	,669**	,724**
	Sig. (bilateral)	,000		,000	,000	,000
	N	204	204	204	204	204
At3	Correlación de Pearson	,648**	,694**	1	,622**	,653**
	Sig. (bilateral)	,000	,000		,000	,000
	N	204	204	204	204	204
At4	Correlación de Pearson	,524**	,669**	,622**	1	,723**
	Sig. (bilateral)	,000	,000	,000		,000
	N	204	204	204	204	204
At5	Correlación de Pearson	,532**	,724**	,653**	,723**	1
	Sig. (bilateral)	,000	,000	,000	,000	
	N	204	204	204	204	204

** . La correlación es significativa al nivel 0,01 (bilateral).

Veamos ahora el 2º factor (E2-5):

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,722
Prueba de esfericidad de	Chi-cuadrado aproximado	161,222
Bartlett	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
E2	1,000	,584
E3	1,000	,636
E4	1,000	,414
E5	1,000	,553

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	2,188	54,695	54,695	2,188	54,695	54,695
2	,772	19,296	73,991			
3	,592	14,812	88,803			
4	,448	11,197	100,000			

Método de extracción: Análisis de Componentes principales.

Veamos lo que sucede eliminando E4, de menor carga factorial:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,656
Prueba de esfericidad de	Chi-cuadrado aproximado	120,741
Bartlett	gl	3
	Sig.	,000

Comunalidades

	Inicial	Extracción
E2	1,000	,657
E3	1,000	,706
E5	1,000	,548

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,911	63,707	63,707	1,911	63,707	63,707
2	,641	21,356	85,063			
3	,448	14,937	100,000			

Método de extracción: Análisis de Componentes principales.

Matriz de componentes^a

	Componente
	1
E2	,811
E3	,840
E5	,740

Método de extracción:

Análisis de componentes principales.

a. 1 componentes extraídos

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,714	3

El 3er factor nos da:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,874
Prueba de esfericidad de	Chi-cuadrado aproximado	715,230
Bartlett	gl	21
	Sig.	,000

Comunalidades

	Inicial	Extracción
C4	1,000	,608
E1	1,000	,571
U1	1,000	,587
U2	1,000	,561
U3	1,000	,534
U4	1,000	,703
U5	1,000	,637

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
	1	4,202	60,033	60,033	4,202	60,033
2	,754	10,777	70,810			
3	,605	8,644	79,454			
4	,507	7,237	86,691			
5	,382	5,463	92,154			
6	,293	4,186	96,340			
7	,256	3,660	100,000			

Método de extracción: Análisis de Componentes principales.

La carga factorial con menor impacto es la de la variable U3. Eliminándola:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,847
Prueba de esfericidad de	Chi-cuadrado aproximado	606,009
Bartlett	gl	15
	Sig.	,000

Comunalidades

	Inicial	Extracción
C4	1,000	,633
E1	1,000	,586
U1	1,000	,586
U2	1,000	,587
U4	1,000	,709
U5	1,000	,635

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	3,736	62,267	62,267	3,736	62,267	62,267
2	,754	12,563	74,830			
3	,556	9,262	84,092			
4	,383	6,388	90,480			
5	,314	5,237	95,717			
6	,257	4,283	100,000			

Método de extracción: Análisis de Componentes principales.

Matriz de componentes^a

	Componente
	1
C4	,795
E1	,766
U1	,765
U2	,766
U4	,842
U5	,797

Método de extracción:
Análisis de componentes principales.
a. 1 componentes extraídos

Con:

Estadísticos de fiabilidad	
Alfa de Cronbach	N de elementos
,853	8

Y unas correlaciones como las siguientes:

		Correlaciones					
		C4	E1	U1	U2	U4	U5
C4	Correlación de Pearson	1	,616**	,507**	,486**	,600**	,551**
	Sig. (bilateral)		,000	,000	,000	,000	,000
	N	204	204	204	204	204	204
E1	Correlación de Pearson	,616**	1	,461**	,463**	,562**	,532**
	Sig. (bilateral)	,000		,000	,000	,000	,000
	N	204	204	204	204	204	204
U1	Correlación de Pearson	,507**	,461**	1	,687**	,519**	,469**
	Sig. (bilateral)	,000	,000		,000	,000	,000
	N	204	204	204	204	204	204
U2	Correlación de Pearson	,486**	,463**	,687**	1	,543**	,469**
	Sig. (bilateral)	,000	,000	,000		,000	,000
	N	204	204	204	204	204	204
U4	Correlación de Pearson	,600**	,562**	,519**	,543**	1	,732**
	Sig. (bilateral)	,000	,000	,000	,000		,000
	N	204	204	204	204	204	204
U5	Correlación de Pearson	,551**	,532**	,469**	,469**	,732**	1
	Sig. (bilateral)	,000	,000	,000	,000	,000	
	N	204	204	204	204	204	204

** . La correlación es significativa al nivel 0,01 (bilateral).

Con todas las variables utilizadas:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,890
Prueba de esfericidad de Chi-cuadrado aproximado		1524,281
Bartlett	gl	91
	Sig.	,000

Comunalidades

	Inicial	Extracción
At1	1,000	,580
At2	1,000	,760
At3	1,000	,727
At4	1,000	,744
At5	1,000	,781
E2	1,000	,661
E3	1,000	,717
E5	1,000	,532
U1	1,000	,620
U2	1,000	,606
U4	1,000	,725
U5	1,000	,672
C4	1,000	,619
E1	1,000	,610

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	6,271	44,796	44,796	6,271	44,796	44,796	
2	1,842	13,160	57,956	1,842	13,160	57,956	
3	1,240	8,858	66,814	1,240	8,858	66,814	
4	,749	5,349	72,163				
5	,657	4,690	76,853				
6	,540	3,859	80,711				
7	,530	3,785	84,497				
8	,433	3,095	87,591				
9	,374	2,671	90,262				

10	,369	2,634	92,896		
11	,292	2,088	94,984		
12	,267	1,906	96,891		
13	,225	1,609	98,500		
14	,210	1,500	100,000		

Método de extracción: Análisis de Componentes principales.

Matriz de componentes rotados^a

	Componente		
	1	2	3
At1	,395	,649	,043
At2	,378	,778	,107
At3	,327	,787	,031
At4	,197	,839	,037
At5	,215	,844	,153
E2	,133	,044	,801
E3	,076	-,043	,842
E5	,086	,188	,700
U1	,732	,288	-,036
U2	,722	,290	,010
U4	,804	,228	,161
U5	,783	,160	,182
C4	,684	,373	,111
E1	,626	,314	,347

Método de extracción: Análisis de componentes principales.

Método de rotación: Normalización Varimax con Kaiser.

a. La rotación ha convergido en 5 iteraciones.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,891	14

Nos salen los tres factores, tal y como los hemos definido

ANEXO C.2 - Modelos estructurales, curso 2011-12

General

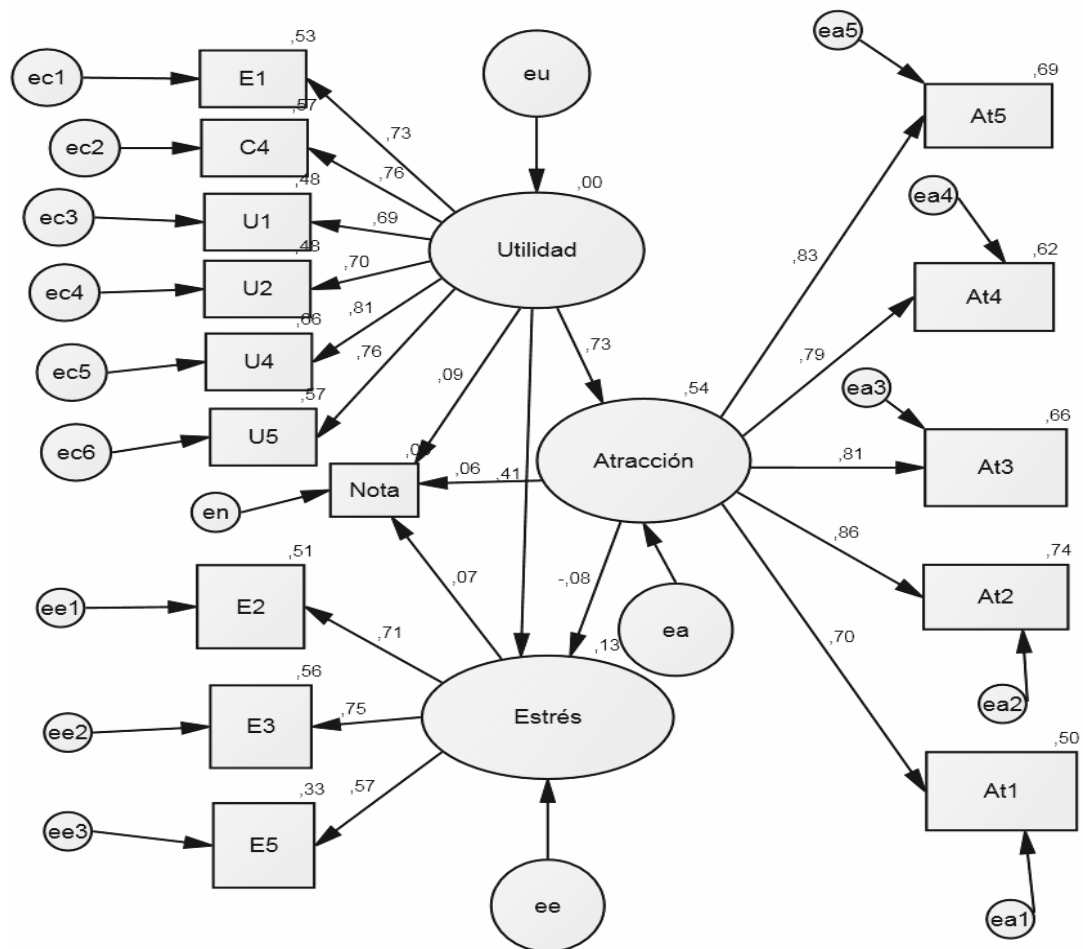
Minimum was achieved
 Chi-square = 198,598
 Degrees of freedom = 85
 Probability level = ,000

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,875	,845	,924	,905	,923

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,081	,066	,096	,000



Usuarios con antivirus actualizado

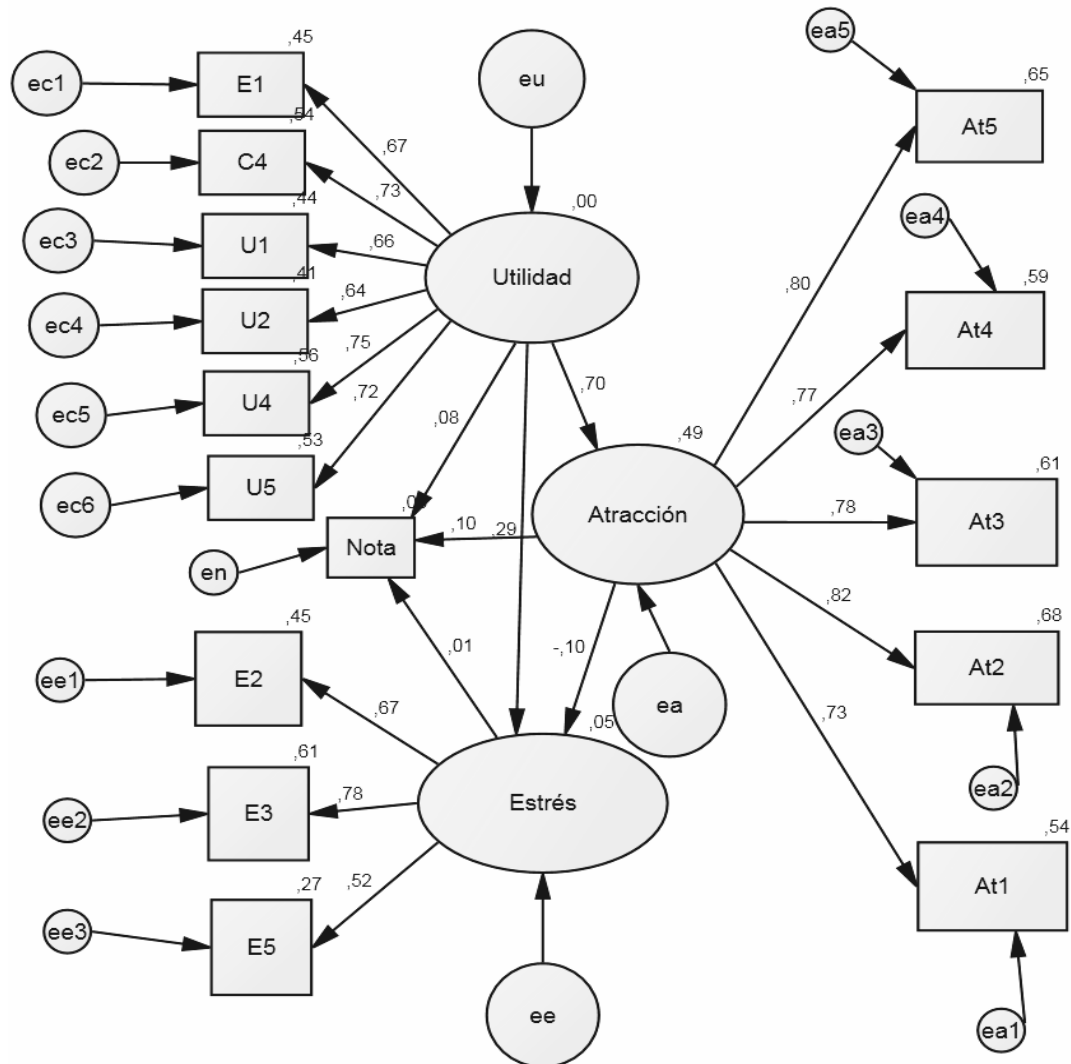
Minimum was achieved
 Chi-square = 150,981
 Degrees of freedom = 85
 Probability level = ,000

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,859	,825	,933	,915	,931

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,070	,051	,088	,040



Chicos

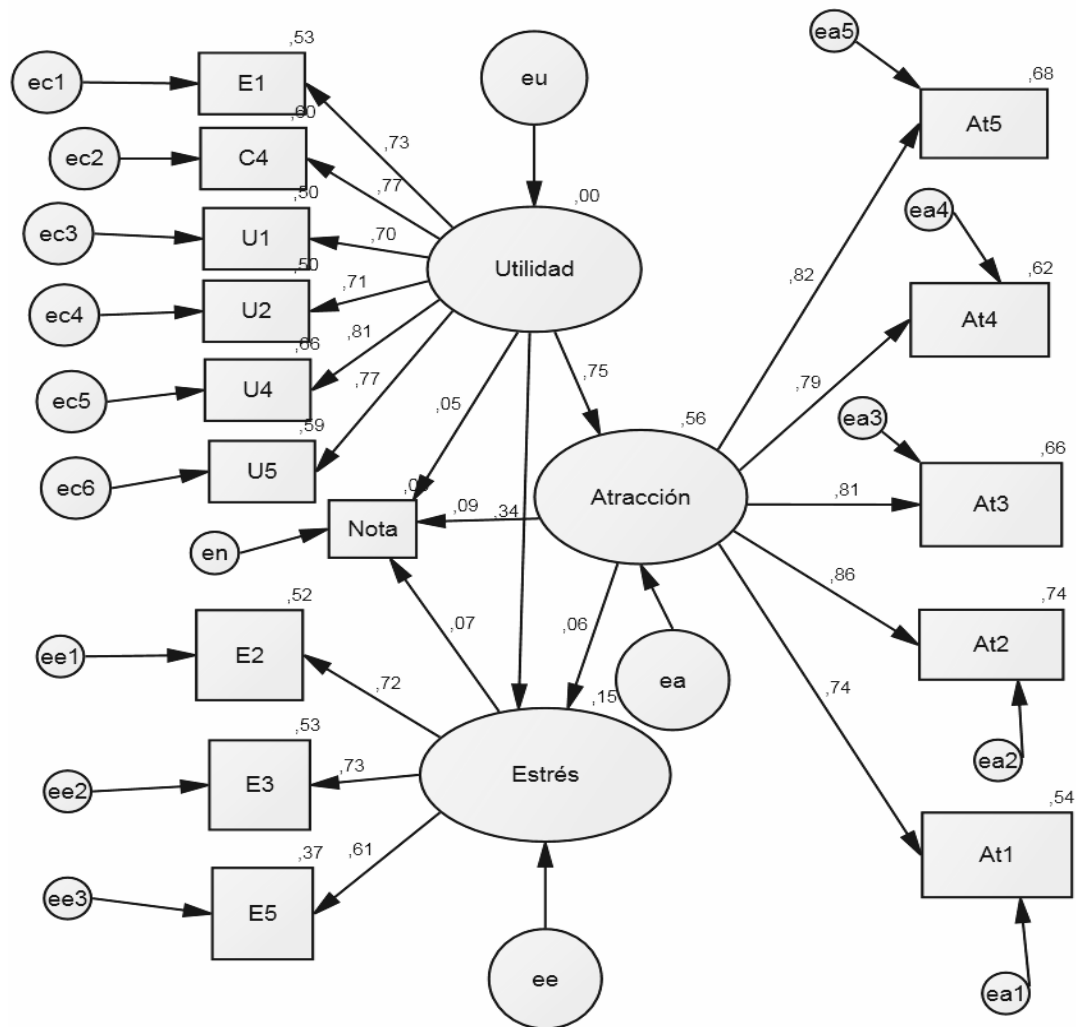
Minimum was achieved
 Chi-square = 174,807
 Degrees of freedom = 85
 Probability level = ,000

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,879	,851	,934	,917	,933

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,077	,061	,093	,004



Uso de password complejas

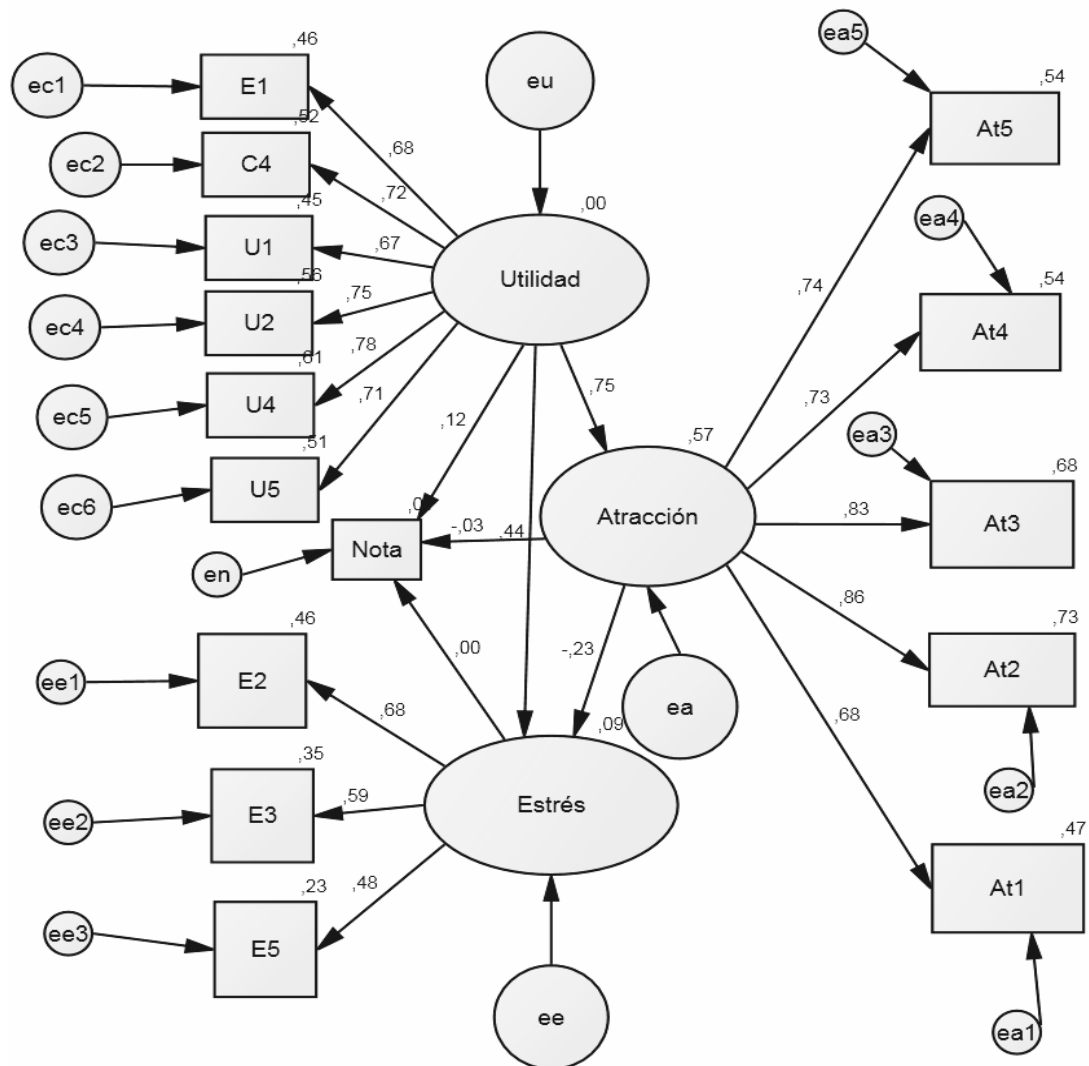
Minimum was achieved
 Chi-square = 138,192
 Degrees of freedom = 85
 Probability level = ,000

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,846	,809	,934	,917	,933

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,069	,047	,090	,072



Usuarios que borran el histórico de páginas visitadas

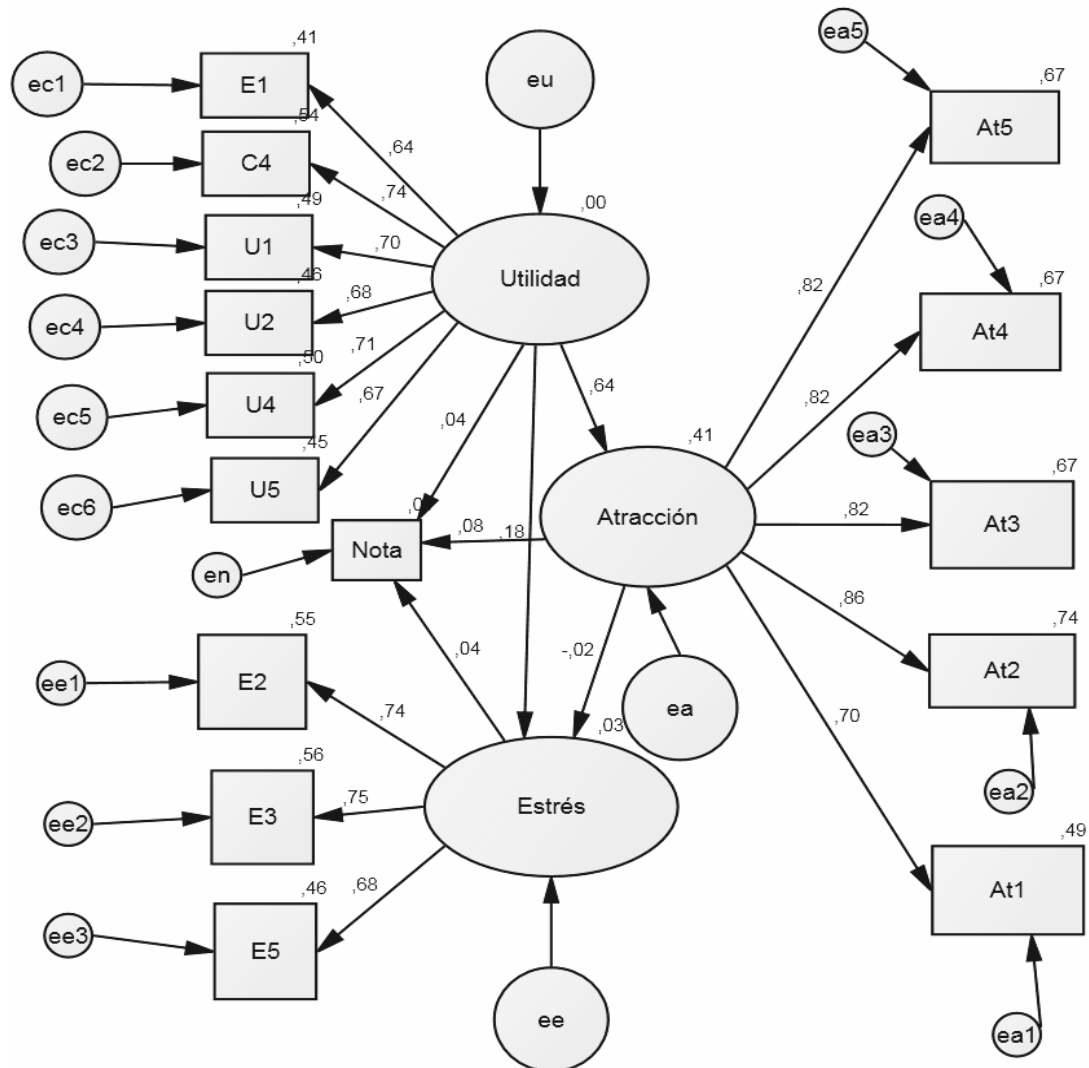
Minimum was achieved
 Chi-square = 132,089
 Degrees of freedom = 85
 Probability level = ,001

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,849	,814	,940	,925	,939

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,068	,044	,089	,102



Hacen backups

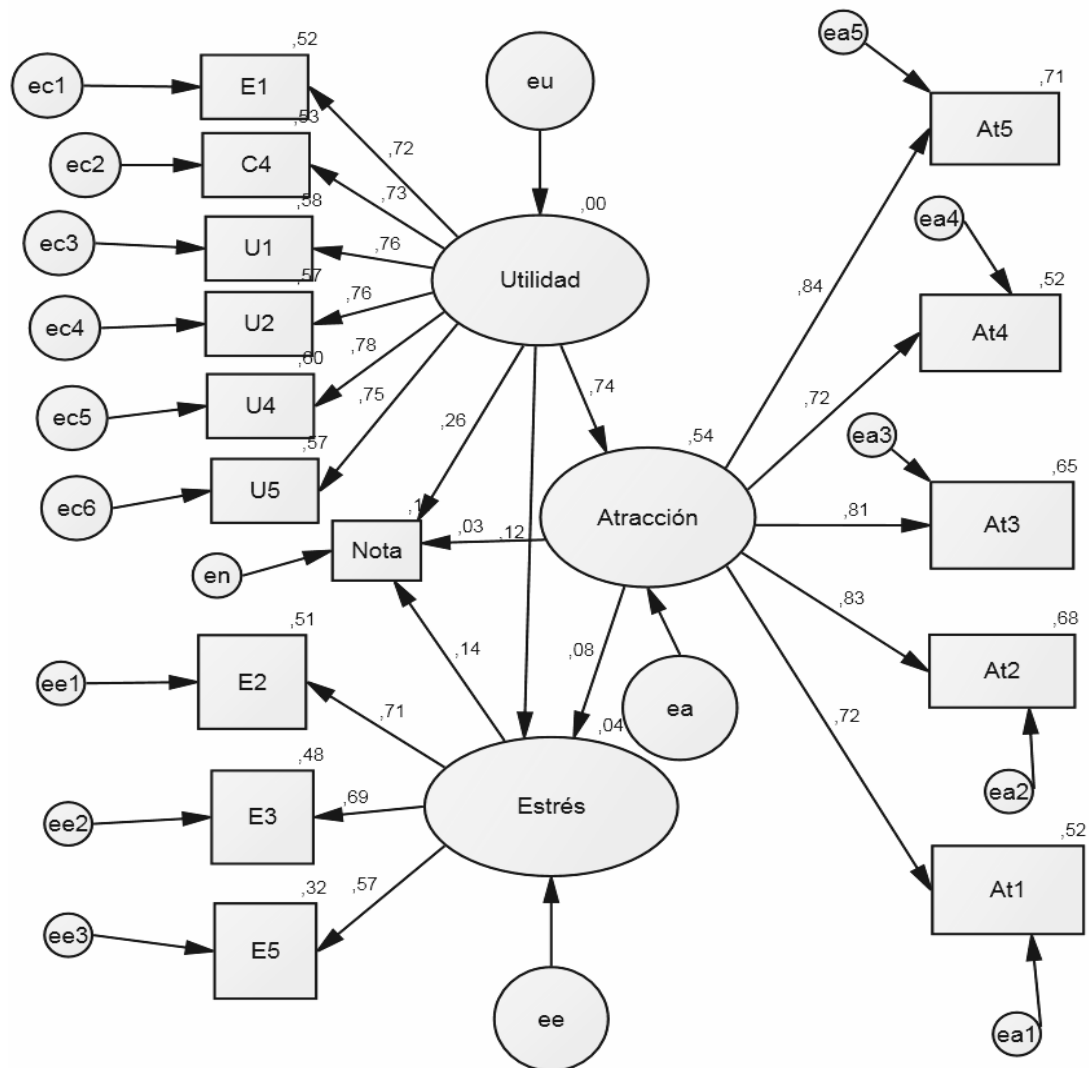
Minimum was achieved
 Chi-square = 121,166
 Degrees of freedom = 85
 Probability level = ,006

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,845	,808	,948	,934	,947

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,066	,036	,091	,169



Protegen inicio de sesión en PC

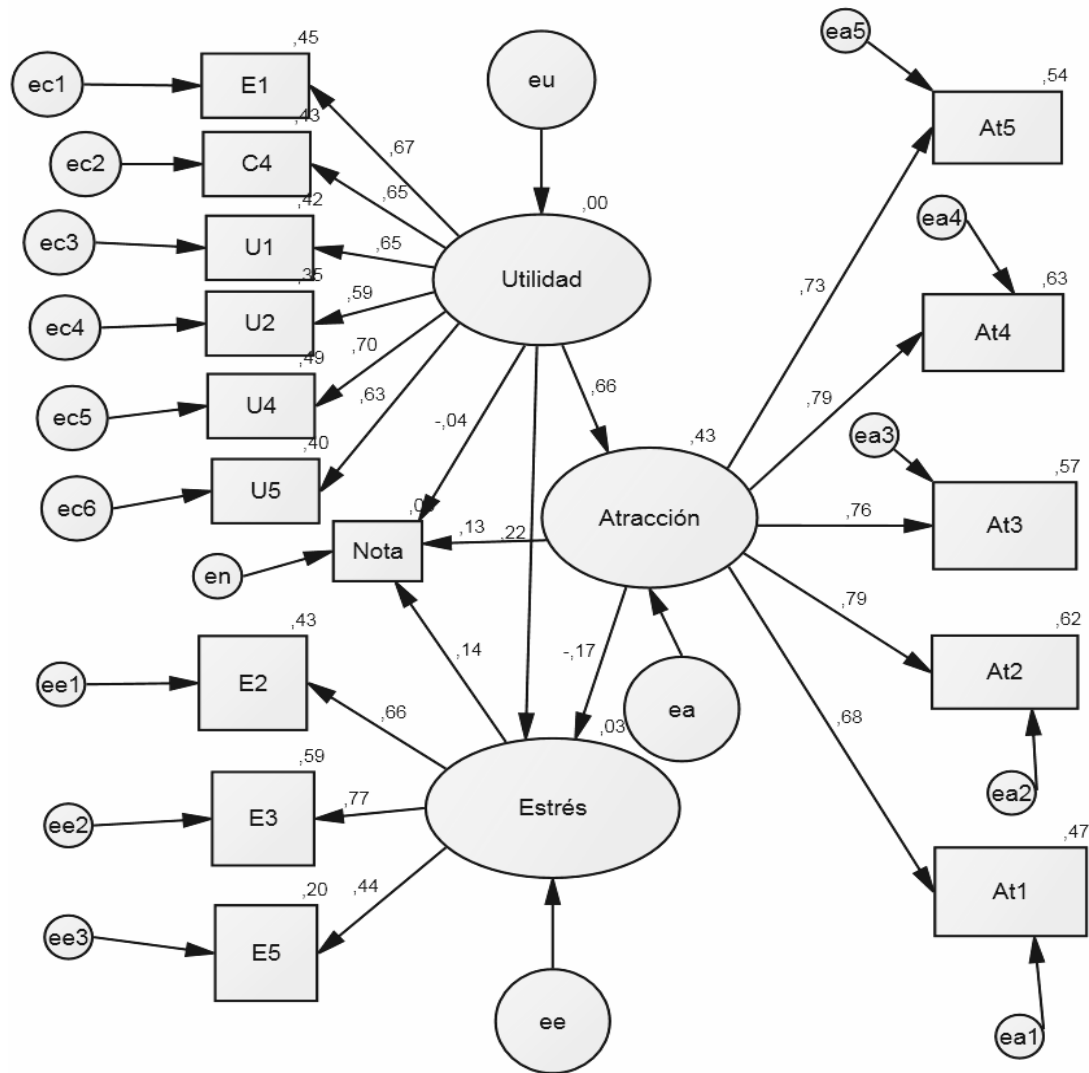
Minimum was achieved
 Chi-square = 114,682
 Degrees of freedom = 85
 Probability level = ,018

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,842	,805	,954	,941	,952

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,051	,023	,074	,443



Protegen privacidad eliminando archivos temporales v cookies

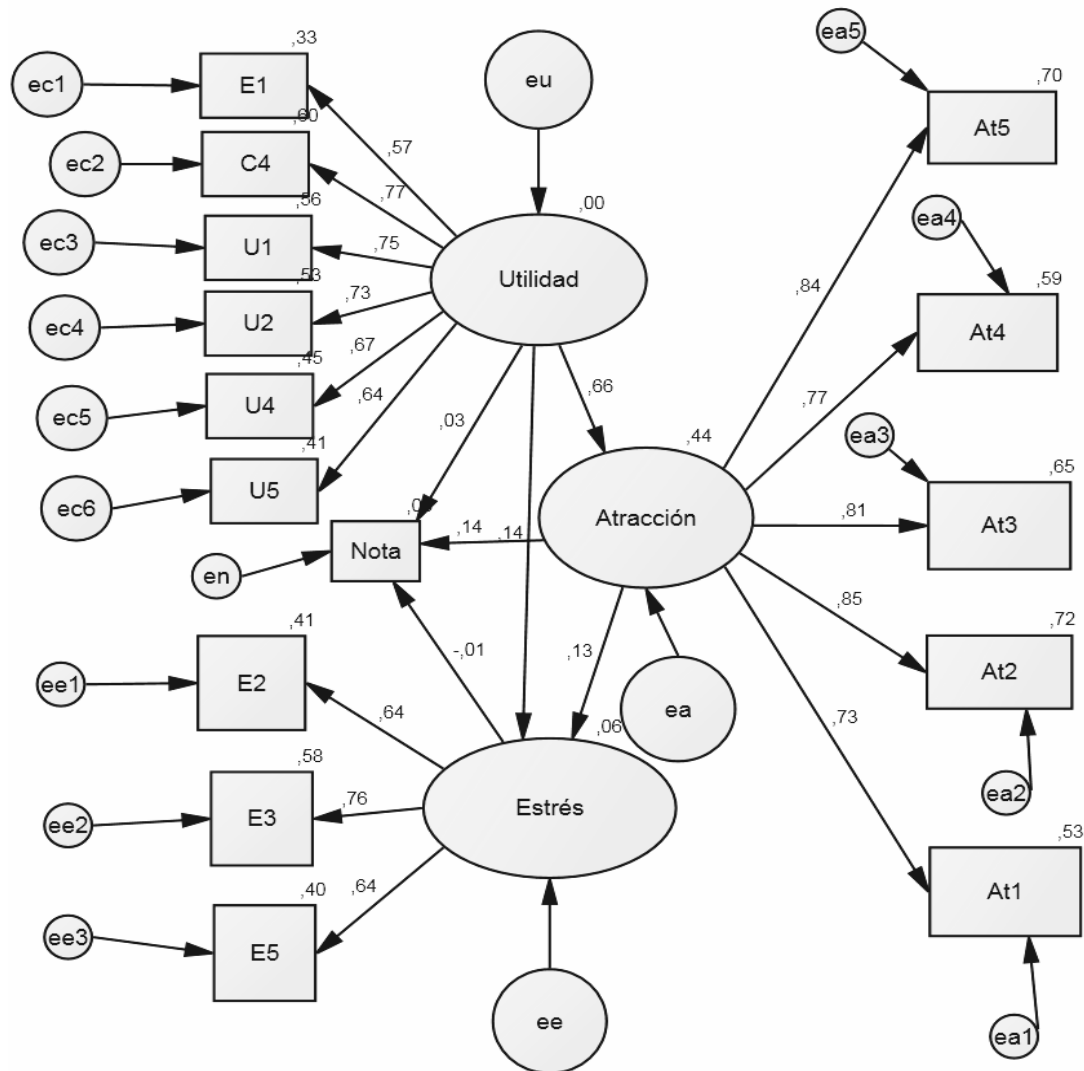
Minimum was achieved
 Chi-square = 121,202
 Degrees of freedom = 85
 Probability level = ,006

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,863	,830	,955	,942	,953

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,058	,032	,080	,279



ANEXO D – Cálculo de regresiones, curso 2012-13

1º Teleco.xls:

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	ABU3, ABU2 ^a	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: ABU1

Resumen del modelo

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación
1	,580 ^a	,336	,329	1,077

a. Variables predictoras: (Constante), ABU3, ABU2

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	112,202	2	56,101	48,352	,000 ^a
	Residual	221,612	191	1,160		
	Total	333,814	193			

a. Variables predictoras: (Constante), ABU3, ABU2

b. Variable dependiente: ABU1

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficients tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Límite superior
1	(Constante)	,458	,289		1,581	,116		-,113
	ABU2	,584	,066	,535	8,854	,000		,454
	ABU3	,149	,068	,133	2,202	,029		,016

a. Variable dependiente: ABU1

$$ABU1 = 0,458 + 4 * 0,584 + 4 * 0,149 = \rightarrow 3$$

VARIABLES INTRODUCIDAS/ELIMINADAS^b

Modelo	VARIABLES INTRODUCIDAS	VARIABLES ELIMINADAS	Método
1	ABU3, ABU1 ^a	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: ABU2

RESUMEN DEL MODELO^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,571 ^a	,326	,319	,995	,326	46,212	2	

a. Variables predictoras: (Constante), ABU3, ABU1

b. Variable dependiente: ABU2

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	91,443	2	45,722	46,212	,000 ^a
	Residual	188,974	191	,989		
	Total	280,418	193			

a. Variables predictoras: (Constante), ABU3, ABU1

b. Variable dependiente: ABU2

COEFICIENTES^a

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
		1	(Constante)	1,719			,239	
	ABU1	,498	,056	,544	8,854	,000	,387	
	ABU3	,088	,063	,085	1,391	,166	-,037	

a. Variable dependiente: ABU2

$$ABU2 = 1,719 + (5,1) * 0,498 + (5,1) * 0,088 = \rightarrow (5,2)$$

AURS (9-10):

Informática.xls:

Encuestado 30: **1 1 1**

“ 32: **2 2 2**

“ 65: **2 1 2**

“ 90: **4 3 4**

Elimino un encuestado que no contestó a A6-9 y que también tenía ceros en Ux

Añado un 5 en A8 a un encuestado que A9 tiene 5.

1º Teleco:

Elimino tres encuestados que no contestaron a A6-9 y que también tenían ceros en Ux

4º Teleco.xls:

Elimino un encuestado que no contestó a A6-9 y que también tenía ceros en Ux

Regresiones 2013:

- *Archivo 1º de Teleco*

At5 x encuestado 29

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	At4, At1, At2, At3	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: At5

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,891 ^a	,794	,761	,633	,794	24,097	4	

a. Variables predictoras: (Constante), At4, At1, At2, At3

b. Variable dependiente: At5

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	38,644	4	9,661	24,097	,000 ^a
	Residual	10,023	25	,401		
	Total	48,667	29			

a. Variables predictoras: (Constante), At4, At1, At2, At3

b. Variable dependiente: At5

Coefficientes^a

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
		1	(Constante)	,093			,388	
	At1	,324	,232	,313	1,397	,175	-,153	
	At2	,176	,197	,175	,892	,381	-,231	
	At3	,140	,278	,128	,504	,618	-,433	
	At4	,361	,165	,364	2,193	,038	,022	

a. Variable dependiente: At5

$$At5 = 0,093 + (At1 \times 0,324) + (At2 \times 0,176) + (At3 \times 0,14) + (At4 \times 0,361) = 1,779$$

$$(2 \ 1 \ 1 \ 2 \ ?) \rightarrow ? = 2$$

C2 x encuestados 1 y 2

VARIABLES INTRODUCIDAS/ELIMINADAS^b

Modelo	VARIABLES INTRODUCIDAS	VARIABLES ELIMINADAS	Método
1	C5, C3, C1, C4	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: C2

RESUMEN DEL MODELO^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio		
					Cambio en R cuadrado	Cambio en F	gl1
1	,876 ^a	,768	,729	,574	,768	19,822	4

a. Variables predictoras: (Constante), C5, C3, C1, C4

b. Variable dependiente: C2

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	26,100	4	6,525	19,822	,000 ^a
	Residual	7,900	24	,329		
	Total	34,000	28			

a. Variables predictoras: (Constante), C5, C3, C1, C4

b. Variable dependiente: C2

COEFICIENTES^a

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Límite superior
		1	(Constante)	-,196			,546	
	C1	,681	,128	,668	5,311	,000	,416	
	C3	,056	,107	,063	,527	,603	-,164	
	C4	,292	,147	,260	1,990	,058	-,011	
	C5	,015	,121	,014	,125	,902	-,235	

a. Variable dependiente: C2

$$C2 = -0,196 + (C1 \times 0,681) + (C3 \times 0,056) + (C4 \times 0,292) + (C5 \times 0,015) =$$

$$(1 \ ? \ 1 \ 1 \ 1) = 0,848 \rightarrow ? = 1$$

$$(2 \ ? \ 1 \ 2 \ 3) = 1,851 \rightarrow ? = 2$$

E2 x encuestado 3

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	E5, E1, E3, E4	.	Introducir

- a. Todas las variables solicitadas introducidas.
 b. Variable dependiente: E2

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,675 ^a	,456	,369	,858	,456	5,243	4	

- a. Variables predictoras: (Constante), E5, E1, E3, E4
 b. Variable dependiente: E2

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	15,450	4	3,863	5,243	,003 ^a
	Residual	18,416	25	,737		
	Total	33,867	29			

- a. Variables predictoras: (Constante), E5, E1, E3, E4
 b. Variable dependiente: E2

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
		1	(Constante)	-,071			,737	
	E1	,301	,159	,313	1,895	,070	-,026	
	E3	,511	,208	,503	2,460	,021	,083	
	E4	-,113	,201	-,119	-,562	,579	-,526	
	E5	,243	,170	,244	1,429	,165	-,107	

- a. Variable dependiente: E2

$$E2 = -0,071 + (E1 \times 0,301) + (E3 \times 0,511) - (E4 \times 0,113) + (E5 \times 0,243) = 3,697$$

$$(4 \ ? \ 4 \ 4 \ 4) \rightarrow ? = 4$$

U2 x encuestado 31

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	U5, U3, U1, U4	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: U2

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,643 ^a	,413	,289	,724	,413	3,340	4	

a. Variables predictoras: (Constante), U5, U3, U1, U4

b. Variable dependiente: U2

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	7,002	4	1,750	3,340	,031 ^a
	Residual	9,957	19	,524		
	Total	16,958	23			

a. Variables predictoras: (Constante), U5, U3, U1, U4

b. Variable dependiente: U2

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
		1	(Constante)	,607			1,061	
	U1	,428	,285	,380	1,503	,149	-,168	
	U3	,043	,187	,051	,230	,820	-,349	
	U4	,273	,395	,216	,691	,498	-,554	
	U5	,146	,407	,112	,359	,724	-,706	

a. Variable dependiente: U2

$$U2 = 0,607 + (U1 \times 0,428) + (U3 \times 0,043) + (U4 \times 0,273) + (U5 \times 0,146) = 2,524$$

$$(1 \ 2 \ 3 \ 4) \rightarrow ? = 3$$

U4 x encuestado 29

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	U5, U3, U2, U1	.	Introducir

- a. Todas las variables solicitadas introducidas.
 b. Variable dependiente: U4

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,832 ^a	,692	,627	,415	,692	10,659	4	

- a. Variables predictoras: (Constante), U5, U3, U2, U1
 b. Variable dependiente: U4

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	7,350	4	1,837	10,659	,000 ^a
	Residual	3,275	19	,172		
	Total	10,625	23			

- a. Variables predictoras: (Constante), U5, U3, U2, U1
 b. Variable dependiente: U4

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
		1	(Constante)	,266			,611	
	U1	,052	,173	,059	,304	,765	-,309	
	U2	,090	,130	,113	,691	,498	-,182	
	U3	,048	,107	,071	,447	,660	-,176	
	U5	,732	,163	,709	4,483	,000	,390	

- a. Variable dependiente: U4

$$U4 = 0,266 + (U1 \times 0,052) + (U2 \times 0,090) + (U3 \times 0,048) + (U5 \times 0,732) = 3,622$$

$$(2 \ 2 \ 3 \ ? \ 4) \rightarrow ? = 4$$

U5 x encuestados 12 y 17

VARIABLES INTRODUCIDAS/ELIMINADAS^b

Modelo	VARIABLES INTRODUCIDAS	VARIABLES ELIMINADAS	Método
1	U4, U3, U2, U1	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: U5

RESUMEN DEL MODELO^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,827 ^a	,684	,618	,407	,684	10,303	4	

a. Variables predictoras: (Constante), U4, U3, U2, U1

b. Variable dependiente: U5

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	6,816	4	1,704	10,303	,000 ^a
	Residual	3,142	19	,165		
	Total	9,958	23			

a. Variables predictoras: (Constante), U4, U3, U2, U1

b. Variable dependiente: U5

COEFICIENTES^a

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Límite superior
		1	(Constante)	,772			,575	
	U1	,146	,166	,169	,877	,391	- ,202	
	U2	,046	,128	,060	,359	,724	- ,223	
	U3	-,072	,104	-,111	-,696	,495	- ,290	
	U4	,702	,157	,725	4,483	,000	,374	

a. Variable dependiente: U5

$$U5 = 0,772 + (U1 \times 0,146) + (U2 \times 0,046) - (U3 \times 0,072) + (U4 \times 0,702) = 4,06 / 4,232$$

$$(4 \ 4 \ 4 \ 4 \ ?) \rightarrow ? = 4$$

$$(5 \ 3 \ 3 \ 4 \ ?) \rightarrow ? = 4$$

U1-U5 x encuestados 1, 2 y 25

Vamos a probar poniendo 0 ó 99

• **Archivo 4° de Teleco**

Encuestado 29 solo informa sobre At5

Haremos como en el caso anterior, probaremos AMOS poniendo todas a 0 ó 99, excepto At5

At3 x encuestado 34

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	At5, At1, At2, At4	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: At3

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio		
					Cambio en R cuadrado	Cambio en F	gl1
1	,860 ^a	,740	,708	,578	,740	23,447	4

a. Variables predictoras: (Constante), At5, At1, At2, At4

b. Variable dependiente: At3

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	31,302	4	7,825	23,447	,000 ^a
	Residual	11,014	33	,334		
	Total	42,316	37			

a. Variables predictoras: (Constante), At5, At1, At2, At4

b. Variable dependiente: At3

Coefficientes^a

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
		1	(Constante)	,175			,418	
	At1	,606	,107	,595	5,686	,000	,389	
	At2	,189	,116	,190	1,626	,113	-,047	
	At4	,319	,111	,345	2,879	,007	,094	
	At5	-,069	,153	-,064	-,453	,653	-,381	

a. Variable dependiente: At3

$$At3 = 0,175 + (At1 \times 0,606) + (At2 \times 0,189) + (At4 \times 0,319) - (At5 \times 0,069) = 2,316$$

$$(2 \ 3 \ ? \ 2 \ 4) \rightarrow ? = 2$$

E1 x encuestado 29

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	E5, E2, E4, E3	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: E1

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,822 ^a	,675	,637	,675	,675	17,683	4	

a. Variables predictoras: (Constante), E5, E2, E4, E3

b. Variable dependiente: E1

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	32,210	4	8,052	17,683	,000 ^a
	Residual	15,483	34	,455		
	Total	47,692	38			

a. Variables predictoras: (Constante), E5, E2, E4, E3

b. Variable dependiente: E1

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
		1	(Constante)	1,072			,465	
	E2	,769	,114	,780	6,764	,000	,538	
	E3	-,370	,132	-,366	-2,807	,008	-,638	
	E4	,322	,141	,279	2,286	,029	,036	
	E5	,045	,147	,041	,306	,761	-,253	

a. Variable dependiente: E1

$$E1 = 1,072 + (E2 \times ,0769) - (E3 \times 0,37) + (E4 \times 0,322) + (E5 \times 0,045) = 1,646$$

$$(? 1 5 5 1) \rightarrow ? = 2$$

U1 x encuestado 29

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	U5, U2, U3, U4	.	Introducir

- a. Todas las variables solicitadas introducidas.
 b. Variable dependiente: U1

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,730 ^a	,533	,477	,703	,533	9,420	4	

- a. Variables predictoras: (Constante), U5, U2, U3, U4
 b. Variable dependiente: U1

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	18,644	4	4,661	9,420	,000 ^a
	Residual	16,329	33	,495		
	Total	34,974	37			

- a. Variables predictoras: (Constante), U5, U2, U3, U4
 b. Variable dependiente: U1

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
1	(Constante)	,680	,760		,895	,377		-,866
	U2	,542	,141	,593	3,848	,001		,255
	U3	,088	,201	,091	,436	,666		-,321
	U4	,225	,360	,161	,623	,537		-,508
	U5	-,030	,251	-,026	-,119	,906		-,541

- a. Variable dependiente: U1

$$U1 = 0,68 + (U2 \times 0,542) + (U3 \times 0,088) + (U4 \times 0,225) - (U5 \times 0,03) = 1,934$$

$$(? \ 1 \ 4 \ 2 \ 3) \rightarrow ? = 2$$

Encuestado 5 no informa sobre Us

Haremos como antes, probaremos AMOS poniendo todas a 0 ó 99

- Archivo 5° de Teleco

At5 x encuestados 1 y 6

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	At4, At1, At3, At2	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: At5

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio		
					Cambio en R cuadrado	Cambio en F	gl1
1	,887 ^a	,788	,722	,518	,788	12,047	4

a. Variables predictoras: (Constante), At4, At1, At3, At2

b. Variable dependiente: At5

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	12,951	4	3,238	12,047	,000 ^a
	Residual	3,494	13	,269		
	Total	16,444	17			

a. Variables predictoras: (Constante), At4, At1, At3, At2

b. Variable dependiente: At5

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
1	(Constante)	,109	,750		,146	,887	-1,511	Lím
	At1	-,136	,237	-,096	-,572	,577	-,649	
	At2	,571	,206	,602	2,767	,016	,125	
	At3	,370	,269	,283	1,378	,192	-,210	
	At4	,147	,187	,146	,785	,446	-,257	

a. Variable dependiente: At5

$$At5 = 0,109 - (At1 \times 0,136) + (At2 \times 0,571) + (At3 \times 0,37) + (At4 \times 0,147) = 4,053 / 3,112$$

$$(3 \ 4 \ 4 \ 4 \ ?) \rightarrow ? = 4$$

$$(3 \ 3 \ 3 \ 4 \ ?) \rightarrow ? = 3$$

C1 x encuestados 6, 8, 9, 15 y 19

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	C5, C4, C3, C2	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: C1

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,432 ^a	,187	-,139	,890	,187	,573	4	

a. Variables predictoras: (Constante), C5, C4, C3, C2

b. Variable dependiente: C1

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	1,816	4	,454	,573	,688 ^a
	Residual	7,917	10	,792		
	Total	9,733	14			

a. Variables predictoras: (Constante), C5, C4, C3, C2

b. Variable dependiente: C1

Coefficientes^a

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
		1	(Constante)	2,759			3,217	
	C2	,187	,482	,142	,388	,706	-,888	
	C3	-,409	,631	-,225	-,649	,531	-1,815	
	C4	,467	,318	,518	1,468	,173	-,242	
	C5	-,057	,546	-,038	-,105	,919	-1,274	

a. Variable dependiente: C1

Los resultados son malos en significatividad y R cuadrado corregida, así que vamos a ver cómo se correlacionan:

Correlaciones

			C1	C2	C3	C4	C5
Rho de Spearman	C1	Coefficiente de correlación	1,000	,003	,049	,421	,127
		Sig. (bilateral)	.	,993	,861	,118	,651
		N	15	15	15	15	15
	C2	Coefficiente de correlación	,003	1,000	,284	-,103	,419
		Sig. (bilateral)	,993	.	,225	,667	,066
		N	15	20	20	20	20
	C3	Coefficiente de correlación	,049	,284	1,000	,440	,282
		Sig. (bilateral)	,861	,225	.	,052	,228
		N	15	20	20	20	20
	C4	Coefficiente de correlación	,421	-,103	,440	1,000	,101
		Sig. (bilateral)	,118	,667	,052	.	,672
		N	15	20	20	20	20
	C5	Coefficiente de correlación	,127	,419	,282	,101	1,000
		Sig. (bilateral)	,651	,066	,228	,672	.
		N	15	20	20	20	20

Vemos que, en efecto, C1 solo tiene correlación con C4. Así que, como vemos que ambas tienen el mismo orden de magnitud

Estadísticos descriptivos

	Media	Desviación típica	N
C1	3,13	,834	15
C2	4,35	,813	20
C3	3,95	,686	20
C4	3,05	,826	20
C5	4,20	,696	20

Tabla de contingencia C1 * C4

Recuento

		C4			Total
		2	3	4	
C1	1	1	0	0	1
	3	5	2	4	11
	4	0	0	2	2
	5	0	1	0	1
Total		6	3	6	15

Asumiremos los valores de C4 como válidos también para las C1

- **Archivo Informática**

At3 x encuestados 35 y 37

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	At5, At1, At4, At2	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: At3

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio		
					Cambio en R cuadrado	Cambio en F	gl1
1	,796 ^a	,633	,618	,541	,633	42,727	4

a. Variables predictoras: (Constante), At5, At1, At4, At2

b. Variable dependiente: At3

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	50,017	4	12,504	42,727	,000 ^a
	Residual	28,973	99	,293		
	Total	78,990	103			

a. Variables predictoras: (Constante), At5, At1, At4, At2

b. Variable dependiente: At3

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
1	(Constante)	,499	,283		1,762	,081		-,063
	At1	,236	,070	,244	3,376	,001		,097
	At2	,429	,079	,468	5,429	,000		,272
	At4	,199	,072	,228	2,761	,007		,056
	At5	,040	,093	,040	,430	,668		-,144

a. Variable dependiente: At3

$$At3 = 0,499 + (At1 \times 0,236) + (At2 \times 0,429) + (At4 \times 0,199) + (At5 \times 0,04) = 3,41 / 4,82$$

$$(3 \ 3 \ ? \ 4 \ 3) \rightarrow ? = 3$$

$$(5 \ 5 \ ? \ 4 \ 5) \rightarrow ? = 5$$

E1 x encuestado 95

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	E5, E4, E3, E2	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: E1

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio		
					Cambio en R cuadrado	Cambio en F	gl1
1	,460 ^a	,212	,180	,811	,212	6,656	4

a. Variables predictoras: (Constante), E5, E4, E3, E2

b. Variable dependiente: E1

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	17,490	4	4,372	6,656	,000 ^a
	Residual	65,039	99	,657		
	Total	82,529	103			

a. Variables predictoras: (Constante), E5, E4, E3, E2

b. Variable dependiente: E1

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
		1	(Constante)	2,102			,403	
	E2	,215	,088	,260	2,449	,016	,041	
	E3	-,016	,078	-,020	-,211	,833	-,171	
	E4	,285	,094	,293	3,030	,003	,098	
	E5	,015	,084	,018	,175	,861	-,152	

a. Variable dependiente: E1

$$E1 = 2,102 + (E2 \times 0,215) - (E3 \times 0,016) + (E4 \times 0,285) + (E5 \times 0,015) = 3,383$$

$$(? \ 2 \ 4 \ 3 \ 4) \rightarrow ? = 3$$

E3 x encuestado 74

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	E5, E1, E4, E2	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: E3

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,365 ^a	,133	,098	1,043	,133	3,803	4	

a. Variables predictoras: (Constante), E5, E1, E4, E2

b. Variable dependiente: E3

Mala R cuadrado corregida

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	16,545	4	4,136	3,803	,006 ^a
	Residual	107,676	99	1,088		
	Total	124,221	103			

a. Variables predictoras: (Constante), E5, E1, E4, E2

b. Variable dependiente: E3

Coefficientes^a

Modelo		Coefficients no estandarizados		Coefficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
1	(Constante)	2,167	,543		3,991	,000	1,090	
	E1	-,027	,129	-,022	-,211	,833	-,284	
	E2	,221	,114	,217	1,929	,057	-,006	
	E4	-,142	,126	-,118	-1,125	,263	-,391	
	E5	,247	,106	,244	2,335	,022	,037	

a. Variable dependiente: E3

$$E3 = 2,167 - (E1 \times 0,027) + (E2 \times 0,221) - (E4 \times 0,142) + (E5 \times 0,247) = 3,064$$

(3 3 ? 3 3) → ? = 3, como parece normal

U5 x encuestado 54

Variables introducidas/eliminadas^b

Modelo	Variables introducidas	Variables eliminadas	Método
1	U4, U2, U3, U1	.	Introducir

a. Todas las variables solicitadas introducidas.

b. Variable dependiente: U5

Resumen del modelo^b

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio			
					Cambio en R cuadrado	Cambio en F	gl1	
1	,854 ^a	,729	,718	,408	,729	66,629	4	

a. Variables predictoras: (Constante), U4, U2, U3, U1

b. Variable dependiente: U5

ANOVA^b

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	44,471	4	11,118	66,629	,000 ^a
	Residual	16,519	99	,167		
	Total	60,990	103			

a. Variables predictoras: (Constante), U4, U2, U3, U1

b. Variable dependiente: U5

Coefficientes^a

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza para B	
		B	Error típ.	Beta			Límite inferior	Lím
1	(Constante)	1,131	,273		4,144	,000	,590	
	U1	-,047	,054	-,054	-,880	,381	-,153	
	U2	,040	,056	,043	,711	,479	-,072	
	U3	,027	,042	,039	,652	,516	-,056	
	U4	,740	,055	,838	13,571	,000	,632	

a. Variable dependiente: U5

$$U5 = 1,131 - (U1 \times 0,047) + (U2 \times 0,04) + (U3 \times 0,027) + (U4 \times 0,74) = 4,945$$

$$(3 \ 3 \ 5 \ 5 \ ?) \rightarrow ? = 5$$

Encuestado 96 no informa sobre Us

Haremos como antes, probaremos AMOS poniendo todas a 0 ó 99

ANEXO D.1 – Cálculo de factores, curso 2012-13

Hacemos un nuevo análisis exploratorio, como en el curso anterior, y encontramos:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,818
Prueba de esfericidad de	Chi-cuadrado aproximado	1770,550
Bartlett	gl	190
	Sig.	,000

Comunalidades

	Inicial	Extracción
At1	1,000	,626
At2	1,000	,775
At3	1,000	,824
At4	1,000	,680
At5	1,000	,796
C1	1,000	,420
C2	1,000	,567
C3	1,000	,669
C4	1,000	,618
C5	1,000	,330
E1	1,000	,645
E2	1,000	,591
E3	1,000	,507
E4	1,000	,413
E5	1,000	,639
U1	1,000	,716
U2	1,000	,754
U3	1,000	,565
U4	1,000	,843
U5	1,000	,804

Método de extracción: Análisis de Componentes principales.

Eliminamos C1, C5 y E4, por su escasa contribución y nos sale:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,802
Prueba de esfericidad de	Chi-cuadrado aproximado	1566,565
Bartlett	gl	136
	Sig.	,000

Comunalidades

	Inicial	Extracción
At1	1,000	,640
At2	1,000	,764
At3	1,000	,829
At4	1,000	,673
At5	1,000	,785
C2	1,000	,514
C3	1,000	,691
C4	1,000	,587
E1	1,000	,716
E2	1,000	,640
E3	1,000	,532
E5	1,000	,702
U1	1,000	,761
U2	1,000	,780
U3	1,000	,586
U4	1,000	,860
U5	1,000	,829

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	5,672	33,364	33,364	5,672	33,364	33,364	
2	1,980	11,645	45,009	1,980	11,645	45,009	
3	1,867	10,985	55,994	1,867	10,985	55,994	
4	1,232	7,247	63,241	1,232	7,247	63,241	
5	1,138	6,697	69,938	1,138	6,697	69,938	
6	,801	4,711	74,649				
7	,707	4,162	78,811				
8	,656	3,858	82,669				
9	,494	2,908	85,577				
10	,487	2,866	88,443				
11	,434	2,554	90,997				
12	,401	2,357	93,354				
13	,337	1,982	95,337				
14	,254	1,492	96,828				
15	,248	1,456	98,284				
16	,155	,909	99,193				

17	,137	,807	100,000			
----	------	------	---------	--	--	--

Método de extracción: Análisis de Componentes principales.

Matriz de componentes rotados^a

	Componente				
	1	2	3	4	5
At1	,675	,042	,417	,037	,080
At2	,853	,026	,047	-,070	,170
At3	,807	,146	,379	,003	,115
At4	,781	,181	,159	-,045	,052
At5	,866	,074	,099	,105	,090
C2	,384	,156	,570	,080	,104
C3	,202	,200	,608	-,482	-,093
C4	,309	,120	,632	-,027	,277
E1	,178	,184	,707	,311	,233
E2	-,076	-,006	,363	,709	,032
E3	-,014	-,014	,026	,691	-,231
E5	,142	,079	-,143	,788	,185
U1	,136	,180	,198	-,006	,819
U2	,173	,137	,119	-,007	,847
U3	-,083	,733	,171	-,039	,108
U4	,223	,882	,093	,018	,154
U5	,245	,863	,115	,057	,092

Método de extracción: Análisis de componentes principales.

Método de rotación: Normalización Varimax con Kaiser.

a. La rotación ha convergido en 7 iteraciones.

Obtenemos cinco factores integrados por las siguientes variables:

Columna 1: At1-5

“ 2: U3-5

“ 3: C2-4, E1

“ 4: E2-3, E5

“ 5: U1-2

Observamos que dos de los factores coinciden con el modelo del curso anterior, los integrados por las variables de Atracción (At1-5) y de Estrés (E2, 3, 5). Por otra parte, en el caso presente aparecen otros tres factores, estando identificados dos de ellos por dos variables cada uno. Necesitando, al menos, tres variables para el modelo estructural, utilizaríamos como tercer factor el de Confianza (C2, 3, 4, E1)

Primer factor (At1-5)

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,835
Prueba de esfericidad de	Chi-cuadrado aproximado	586,944
Bartlett	gl	10
	Sig.	,000

Comunalidades

	Inicial	Extracción
At1	1,000	,613
At2	1,000	,722
At3	1,000	,809
At4	1,000	,671
At5	1,000	,747

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la	% acumulado	Total	% de la	% acumulado
		varianza			varianza	
1	3,563	71,253	71,253	3,563	71,253	71,253
2	,527	10,534	81,787			
3	,437	8,740	90,527			
4	,280	5,608	96,135			
5	,193	3,865	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,897	5

Segundo factor (E2, 3, 5):

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,637
Prueba de esfericidad de	Chi-cuadrado aproximado	64,049
Bartlett	gl	3
	Sig.	,000

Comunalidades

	Inicial	Extracción
E2	1,000	,542
E3	1,000	,536
E5	1,000	,623

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,701	56,688	56,688	1,701	56,688	56,688
2	,704	23,468	80,156			
3	,595	19,844	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,616	3

Tercer factor (C2, 3, 4, E1):

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,710
Prueba de esfericidad de Chi-cuadrado aproximado		147,528
Bartlett	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
C2	1,000	,552
C3	1,000	,392
C4	1,000	,633
E1	1,000	,586

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la	% acumulado	Total	% de la	% acumulado
		varianza			varianza	
1	2,163	54,075	54,075	2,163	54,075	54,075
2	,789	19,724	73,799			
3	,604	15,088	88,887			
4	,445	11,113	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,704	4

Aunque la fiabilidad es alta, la explicación de lo varianza es algo escasa (54%).

Vamos a estudiar el caso de utilizar para este tercer factor las mismas variables del curso anterior:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,674
Prueba de esfericidad de Chi-cuadrado aproximado		460,546
Bartlett	gl	15
	Sig.	,000

Comunalidades

	Inicial	Extracción
C4	1,000	,511
E1	1,000	,477
U1	1,000	,676
U2	1,000	,614
U4	1,000	,897
U5	1,000	,915

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la	% acumulado	Total	% de la	% acumulado	
		varianza			varianza		
1	2,906	48,432	48,432	2,906	48,432	48,432	
2	1,184	19,738	68,171	1,184	19,738	68,171	
3	,903	15,055	83,225				
4	,461	7,678	90,903				
5	,392	6,526	97,429				
6	,154	2,571	100,000				

Método de extracción: Análisis de Componentes principales.

Matriz de componentes^a

	Componente	
	1	2
C4	,671	,246
E1	,668	,175
U1	,692	,445
U2	,639	,453
U4	,755	-,573
U5	,744	-,602

Método de extracción: Análisis de componentes principales.

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,674
Prueba de esfericidad de Chi-cuadrado aproximado		460,546
Bartlett	gl	15

a. 2 componentes extraídos

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,782	6

Obtenemos una mayor explicación de la varianza.

Los tres factores del conjunto:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,781
Prueba de esfericidad de Chi-cuadrado aproximado		1315,410
Bartlett	gl	91
	Sig.	,000

Comunalidades

	Inicial	Extracción
At1	1,000	,629
At2	1,000	,722
At3	1,000	,823
At4	1,000	,654
At5	1,000	,741
E2	1,000	,621
E3	1,000	,548
E5	1,000	,546
E1	1,000	,549
C4	1,000	,438
U1	1,000	,469
U2	1,000	,419
U4	1,000	,664
U5	1,000	,621

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	5,035	35,964	35,964	5,035	35,964	35,964	
2	1,827	13,047	49,012	1,827	13,047	49,012	
3	1,583	11,304	60,316	1,583	11,304	60,316	
4	1,193	8,519	68,834				
5	,948	6,770	75,604				
6	,752	5,370	80,975				
7	,572	4,088	85,063				
8	,464	3,315	88,378				
9	,429	3,064	91,441				
10	,367	2,624	94,065				
11	,273	1,951	96,015				
12	,250	1,788	97,804				
13	,164	1,174	98,977				
14	,143	1,023	100,000				

Método de extracción: Análisis de Componentes principales.

Matriz de componentes rotados^a

	Componente		
	1	2	3
At1	,765	,184	,100
At2	,835	,134	-,088
At3	,857	,293	,045
At4	,780	,212	-,029
At5	,846	,117	,103
E2	,001	,116	,780
E3	-,006	-,221	,706
E5	,039	,124	,728
E1	,341	,491	,437
C4	,462	,467	,079
U1	,177	,662	,021
U2	,176	,623	-,002
U4	,133	,804	-,004
U5	,149	,773	,035

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,828	14

Correlaciones:

Correlaciones

			At1	At2	At3	At4	At5
Rho de Spearman	At1	Coefficiente de correlación	1,000	,528**	,652**	,499**	,541**
		Sig. (bilateral)	.	,000	,000	,000	,000
		N	192	192	192	192	192
	At2	Coefficiente de correlación	,528**	1,000	,724**	,557**	,703**
		Sig. (bilateral)	,000	.	,000	,000	,000
		N	192	192	192	192	192
	At3	Coefficiente de correlación	,652**	,724**	1,000	,660**	,671**
		Sig. (bilateral)	,000	,000	.	,000	,000
		N	192	192	192	192	192
	At4	Coefficiente de correlación	,499**	,557**	,660**	1,000	,668**
		Sig. (bilateral)	,000	,000	,000	.	,000
		N	192	192	192	192	192
	At5	Coefficiente de correlación	,541**	,703**	,671**	,668**	1,000
		Sig. (bilateral)	,000	,000	,000	,000	.
		N	192	192	192	192	192

** . La correlación es significativa al nivel 0,01 (bilateral).

Correlaciones

			E2	E3	E5
Rho de Spearman	E2	Coefficiente de correlación	1,000	,307**	,374**
		Sig. (bilateral)	.	,000	,000
		N	192	192	192
	E3	Coefficiente de correlación	,307**	1,000	,366**
		Sig. (bilateral)	,000	.	,000
		N	192	192	192
	E5	Coefficiente de correlación	,374**	,366**	1,000
		Sig. (bilateral)	,000	,000	.
		N	192	192	192

** . La correlación es significativa al nivel 0,01 (bilateral).

Correlaciones

		C4	E2	U1	U2	U4	U5
C4	Correlación de Pearson	1	,027	,376**	,315**	,300**	,311**
	Sig. (bilateral)		,711	,000	,000	,000	,000
	N	192	192	192	192	192	192
E2	Correlación de Pearson	,027	1	,090	,049	,072	,067
	Sig. (bilateral)	,711		,214	,495	,322	,358
	N	192	192	192	192	192	192
U1	Correlación de Pearson	,376**	,090	1	,606**	,329**	,264**
	Sig. (bilateral)	,000	,214		,000	,000	,000
	N	192	192	192	192	192	192
U2	Correlación de Pearson	,315**	,049	,606**	1	,277**	,257**
	Sig. (bilateral)	,000	,495	,000		,000	,000
	N	192	192	192	192	192	192
U4	Correlación de Pearson	,300**	,072	,329**	,277**	1	,840**
	Sig. (bilateral)	,000	,322	,000	,000		,000
	N	192	192	192	192	192	192
U5	Correlación de Pearson	,311**	,067	,264**	,257**	,840**	1
	Sig. (bilateral)	,000	,358	,000	,000	,000	
	N	192	192	192	192	192	192

** . La correlación es significativa al nivel 0,01 (bilateral).

ANEXO E – Cálculo para todos los alumnos de los dos cursos

Vamos a hacer un análisis confirmatorio sobre las variables utilizadas en todos los alumnos encuestados:

Variabes Atracción:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,860
Prueba de esfericidad de Chi-cuadrado aproximado		1191,842
Bartlett	gl	10
	Sig.	,000

Comunalidades

	Inicial	Extracción
At1	1,000	,604
At2	1,000	,745
At3	1,000	,776
At4	1,000	,691
At5	1,000	,749

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la	% acumulado	Total	% de la	% acumulado
		varianza			varianza	
1	3,566	71,322	71,322	3,566	71,322	71,322
2	,536	10,720	82,042			
3	,382	7,646	89,688			
4	,286	5,712	95,400			
5	,230	4,600	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,898	5

Variables Estrés:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,711
Prueba de esfericidad de	Chi-cuadrado aproximado	374,009
Bartlett	gl	10
	Sig.	,000

Comunalidades

	Inicial	Extracción
E1	1,000	,422
E2	1,000	,565
E3	1,000	,429
E4	1,000	,465
E5	1,000	,473

Método de extracción: Análisis de Componentes principales.

Eliminamos E1:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,731
Prueba de esfericidad de	Chi-cuadrado aproximado	241,157
Bartlett	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
E2	1,000	,551
E3	1,000	,551
E4	1,000	,405
E5	1,000	,559

Método de extracción: Análisis de Componentes principales.

Eliminamos E4:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,661
Prueba de esfericidad de Chi-cuadrado aproximado		173,930
Bartlett	gl	3
	Sig.	,000

Comunalidades

	Inicial	Extracción
E2	1,000	,597
E3	1,000	,625
E5	1,000	,584

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	1,806	60,202	60,202	1,806	60,202	60,202
2	,622	20,734	80,935			
3	,572	19,065	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,669	3

Nos quedamos con E2, E3, E5

Variables Confianza:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,705
Prueba de esfericidad de	Chi-cuadrado aproximado	365,719
Bartlett	gl	10
	Sig.	,000

Comunalidades

	Inicial	Extracción
C1	1,000	,439
C2	1,000	,591
C3	1,000	,382
C4	1,000	,561
C5	1,000	,349

Método de extracción: Análisis de Componentes principales.

Eliminamos C3 y C5:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,669
Prueba de esfericidad de	Chi-cuadrado aproximado	206,148
Bartlett	gl	3
	Sig.	,000

Comunalidades

	Inicial	Extracción
C1	1,000	,641
C2	1,000	,648
C4	1,000	,584

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
	1	1,873	62,417	62,417	1,873	62,417
2	,605	20,156	82,573			
3	,523	17,427	100,000			

Método de extracción: Análisis de Componentes principales.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,696	3

Variables Utilidad:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,736
Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	841,383
	gl	10
	Sig.	,000

Comunalidades

	Inicial	Extracción
U1	1,000	,545
U2	1,000	,512
U3	1,000	,502
U4	1,000	,713
U5	1,000	,656

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	2,928	58,558	58,558	2,928	58,558	58,558
2	,936	18,722	77,280			
3	,579	11,583	88,863			
4	,339	6,781	95,643			
5	,218	4,357	100,000			

Método de extracción: Análisis de Componentes principales.

Observamos que eliminando U2:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,726
Prueba de esfericidad de	Chi-cuadrado aproximado	605,475
Bartlett	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
U1	1,000	,437
U3	1,000	,567
U4	1,000	,784
U5	1,000	,739

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
	1	2,527	63,185	63,185	2,527	63,185
2	,697	17,416	80,601			
3	,558	13,951	94,552			
4	,218	5,448	100,000			

Método de extracción: Análisis de Componentes principales.

Y eliminando también U1 por su escasa contribución:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,657
Prueba de esfericidad de	Chi-cuadrado aproximado	504,158
Bartlett	gl	3
	Sig.	,000

Comunalidades

	Inicial	Extracción
U3	1,000	,579
U4	1,000	,827
U5	1,000	,802

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	2,208	73,601	73,601	2,208	73,601	73,601
2	,573	19,085	92,686			
3	,219	7,314	100,000			

Método de extracción: Análisis de Componentes principales.

Obtenemos una mayor explicación de la varianza, y el mismo KMO, que eliminando U3:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,657
Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	687,636
	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
U1	1,000	,586
U2	1,000	,581
U4	1,000	,707
U5	1,000	,656

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	2,530	63,251	63,251	2,530	63,251	63,251
2	,904	22,597	85,849			
3	,347	8,687	94,535			
4	,219	5,465	100,000			

Método de extracción: Análisis de Componentes principales.

Incluso obtenemos un, aunque ligero, mejor Alfa de Cronbach:

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,805	3

Así que definimos Utilidad mediante las variables U3, U4, U5.

El conjunto de variables seleccionadas para los cuatro factores nos da lo siguiente:

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,872
Prueba de esfericidad de	Chi-cuadrado aproximado	2508,780
Bartlett	gl	91
	Sig.	,000

Comunalidades

	Inicial	Extracción
At1	1,000	,596
At2	1,000	,752
At3	1,000	,775
At4	1,000	,711
At5	1,000	,768
C1	1,000	,811
C2	1,000	,628
C4	1,000	,548
E2	1,000	,589
E3	1,000	,642
E5	1,000	,593
U3	1,000	,636
U4	1,000	,806
U5	1,000	,775

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	5,414	38,674	38,674	5,414	38,674	38,674	
2	1,787	12,764	51,438	1,787	12,764	51,438	
3	1,468	10,484	61,922	1,468	10,484	61,922	
4	,961	6,866	68,788	,961	6,866	68,788	
5	,683	4,877	73,666				
6	,612	4,369	78,035				
7	,592	4,232	82,267				
8	,521	3,718	85,985				
9	,482	3,442	89,428				
10	,405	2,895	92,323				

11	,377	2,691	95,014			
12	,274	1,954	96,968			
13	,215	1,533	98,501			
14	,210	1,499	100,000			

Método de extracción: Análisis de Componentes principales.

Matriz de componentes rotados^a

	Componente			
	1	2	3	4
At1	,705	,207	,050	,234
At2	,846	,158	,031	,101
At3	,812	,189	,015	,283
At4	,825	,156	-,002	,071
At5	,849	,090	,140	,142
C1	,121	,106	,099	,881
C2	,422	,177	,114	,637
C4	,397	,360	,012	,511
E2	,032	,071	,755	,117
E3	-,037	,034	,800	,010
E5	,143	,053	,754	,042
U3	,097	,790	,020	,040
U4	,260	,838	,082	,168
U5	,225	,817	,111	,211

Método de extracción: Análisis de componentes principales.

Método de rotación: Normalización Varimax con Kaiser.

a. La rotación ha convergido en 5 iteraciones.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,853	14

Confirmando la distribución de las variables en los factores definidos

Correlaciones:

		Correlaciones				
		At1	At2	At3	At4	At5
At1	Correlación de Pearson	1	,566**	,675**	,532**	,542**
	Sig. (bilateral)		,000	,000	,000	,000
	N	396	396	396	396	396
At2	Correlación de Pearson	,566**	1	,712**	,621**	,730**
	Sig. (bilateral)	,000		,000	,000	,000
	N	396	396	396	396	396
At3	Correlación de Pearson	,675**	,712**	1	,654**	,666**
	Sig. (bilateral)	,000	,000		,000	,000
	N	396	396	396	396	396
At4	Correlación de Pearson	,532**	,621**	,654**	1	,702**
	Sig. (bilateral)	,000	,000	,000		,000
	N	396	396	396	396	396
At5	Correlación de Pearson	,542**	,730**	,666**	,702**	1
	Sig. (bilateral)	,000	,000	,000	,000	
	N	396	396	396	396	396

** . La correlación es significativa al nivel 0,01 (bilateral).

		Correlaciones		
		C1	C2	C4
C1	Correlación de Pearson	1	,477**	,411**
	Sig. (bilateral)		,000	,000
	N	396	396	396
C2	Correlación de Pearson	,477**	1	,419**
	Sig. (bilateral)	,000		,000
	N	396	396	396
C4	Correlación de Pearson	,411**	,419**	1
	Sig. (bilateral)	,000	,000	
	N	396	396	396

** . La correlación es significativa al nivel 0,01 (bilateral).

Correlaciones

		E2	E3	E5
E2	Correlación de Pearson	1	,421**	,379**
	Sig. (bilateral)		,000	,000
	N	396	396	396
E3	Correlación de Pearson	,421**	1	,408**
	Sig. (bilateral)	,000		,000
	N	396	396	396
E5	Correlación de Pearson	,379**	,408**	1
	Sig. (bilateral)	,000	,000	
	N	396	396	396

** . La correlación es significativa al nivel 0,01 (bilateral).

Correlaciones

		U3	U4	U5
U3	Correlación de Pearson	1	,527**	,491**
	Sig. (bilateral)		,000	,000
	N	396	396	396
U4	Correlación de Pearson	,527**	1	,779**
	Sig. (bilateral)	,000		,000
	N	396	396	396
U5	Correlación de Pearson	,491**	,779**	1
	Sig. (bilateral)	,000	,000	
	N	396	396	396

** . La correlación es significativa al nivel 0,01 (bilateral).

Tablas de frecuencia

A6

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	32	8,1	8,1	8,1
	2	19	4,8	4,8	12,9
	3	29	7,3	7,3	20,2
	4	95	24,0	24,0	44,2
	5	221	55,8	55,8	100,0
	Total	396	100,0	100,0	

A7

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	32	8,1	8,1	8,1
	2	21	5,3	5,3	13,4
	3	60	15,2	15,2	28,5
	4	102	25,8	25,8	54,3
	5	181	45,7	45,7	100,0
	Total	396	100,0	100,0	

A8

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	25	6,3	6,3	6,3
	2	54	13,6	13,6	19,9
	3	74	18,7	18,7	38,6
	4	106	26,8	26,8	65,4
	5	137	34,6	34,6	100,0
	Total	396	100,0	100,0	

A9

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	34	8,6	8,6	8,6
	2	53	13,4	13,4	22,0
	3	84	21,2	21,2	43,2
	4	114	28,8	28,8	72,0
	5	111	28,0	28,0	100,0
	Total	396	100,0	100,0	

Las correlaciones entre las variables de control son las siguientes:

		ABU1	ABU2
ABU1	Correlación de Pearson	1	,568**
	Sig. (bilateral)		,000
	N	396	396
ABU2	Correlación de Pearson	,568**	1
	Sig. (bilateral)	,000	
	N	396	396

** . La correlación es significativa al nivel 0,01 (bilateral).

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,723	2

Correlaciones

		A8	A9
A8	Correlación de Pearson	1	,784**
	Sig. (bilateral)		,000
	N	396	396
A9	Correlación de Pearson	,784**	1
	Sig. (bilateral)	,000	
	N	396	396

** . La correlación es significativa al nivel 0,01 (bilateral).

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,879	2

Nos dan dos factores diferenciados que son los que nos facilitan las puntuaciones para el análisis

KMO y prueba de Bartlett

Medida de adecuación muestral de Kaiser-Meyer-Olkin.		,519
Prueba de esfericidad de Chi-cuadrado aproximado		546,064
Bartlett	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
ABU1	1,000	,780
ABU2	1,000	,790
A8	1,000	,890
A9	1,000	,895

Método de extracción: Análisis de Componentes principales.

Varianza total explicada

Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma
	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	
1	1,987	49,683	49,683	1,987	49,683	49,683	
2	1,368	34,196	83,879	1,368	34,196	83,879	
3	,433	10,837	94,716				
4	,211	5,284	100,000				

Método de extracción: Análisis de Componentes principales.

Matriz de componentes

rotados^a

	Componente	
	1	2
ABU1	,107	,877
ABU2	,047	,887
A8	,937	,114
A9	,945	,051

Método de extracción: Análisis de componentes principales.

Método de rotación:

Normalización Varimax con Kaiser.

a. La rotación ha convergido en 3 iteraciones.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,656	4