UNIVERSIDAD POLITECNICA DE VALENCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

UNIVERSIDAD POLITÉCNICA DE VALENCIA
ESCUELA TÉCNICA SUPERIOR DE INFORMÁTICA APLICADA

Vulnerabilidades comunes en sistemas de información escolares y posibles soluciones

PROYECTO FIN DE CARRERA

Autor: Javier Villalta Frutos

Directora: Eva Mª Cutanda García

Diciembre de 2011

Contenido

Introducción

A lo largo de casi diez años dedicados a la educación no formal, he constatado que los sistemas de información escolares tienden a estar cuestionablemente protegidos. Desde el respeto a la labor del responsable y con el conocimiento adquirido durante mi formación, he intentando aconsejar de alguna manera siempre en pos de mejorar. Este precedente y una predisposición de ayuda al entorno, han sido los precursores del tema de este proyecto fin de carrera.

Obviamente, la auditoria y soluciones propuestas seguramente distarán del mismo trabajo realizado por un profesional curtido en este arte; pero aún así intentaré realizar el mejor trabajo posible atendiendo a las circunstancias.

La realización del presente proyecto también pretende solventar mis dudas acerca de una próxima incorporación al mundo laboral, marcando el rumbo hacia la auditoría o la consultoría.

A lo largo de este trabajo se intentará realizar una exposición clara y concisa, evitando formulas superfluas o explicaciones repetitivas.

Sobre la licencia de este documento

Definición del proyecto

Contenido

Iniciación

Cliente:

La Universidad Politécnica de Valencia y la Universidad del País Vasco/Euskal herriko unibertsitatea.

Objetivo:

Demostrar las competencias adquiridas durante la carrera en el ámbito de la gestión de proyectos y los conocimientos técnicos interiorizados.

Descripción del proyecto:

Abstract

Este proyecto puede ser descrito, a groso modo, por dos macro fases. Por un lado, el estudio de las vulnerabilidades presentes en los sistemas de información escolares seleccionados como representación del total de centros docentes. Y por otro lado, tras el análisis de los resultados, la proposición de soluciones lo más sencillas posibles a la vulnerabilidades más comunes.

Descripción desarrollada

Sobre el método de encuesta y la muestra seleccionada

Mediante una batería de preguntas se auditarán diferentes aspectos del sistema de información, en adelante SI, como configuraciones, diseño de red o políticas de seguridad. Las auditorías se realizarán principalmente vía telemática entre colegios de las tres provincias de la Comunitat Valenciana. Alternativamente, se realizarán algunas auditorias presenciales para asegurar un mínimo de datos. En este último caso, los centros seleccionados estarán localizados en área metropolitana de la ciudad de Valencia o poblaciones cercanas para facilitar el desplazamiento.

El análisis de los datos

En cuanto al análisis de datos, se ordenarán los items de la encuesta, que indican posibles vulnerabilidades, en función de su relevancia. Se entiende que a mayor número de centros afectados, mayor será la relevancia del ítem. En la primera

fase del análisis se considerarán todos los centros como iguales, y en una segunda fase se analizarán por clústeres; de esta forma se podrá deducir si las variables de agrupación influyen en la seguridad del SI. Son variables de agrupación a estudiar:

- El tamaño del SI: en función de que formaciones imparte el centro.
- El carácter del centro: público o privado.
- La implantación del sistema Ítaca.

Se inferirán posibles patrones, combinaciones de items, en función de la influencia de las variables de agrupación.

Proposición de soluciones

Con respecto a la proposición de soluciones, a priori, se definirá una solución por cada item para ofrecer un feedback inmediato a los centros escolares al finalizar la batería de preguntas. Tras el análisis de los datos propondrán soluciones a los patrones inferidos, sin perder de vista el binomio calidad-coste.

Resumen esquemático de las tareas principales

- Fase 1: Auditoría de centros
    - Estudio de precedentes
    - Elaboración del cuestionario
    - Proposición inicial de soluciones, una por ítem del cuestionario
    - Periodo de auditoría
        - Auditoría telemática
        - Auditoría presencial

- Fase 2: Estudio de soluciones
    - Análisis de datos
        - Inferencia de patrones sobre el conjunto total de datos
        - Inferencia de patrones sobre clústeres
        - Conclusiones sobre influencia de las variables de agrupación
    - Proposición de soluciones a los patrones inferidos

Criterios

- La muestra seleccionada debe ser representativa en cuanto que contendrá centros con sistemas de información de diferentes tamaños, en función de la oferta docente, y centros de carácter público y privado. Por cada combinación de oferta docente y carácter se seleccionan tres centros por provincia.
- El proyecto debe seguir el plan de calidad.
- El Proyecto debe ser entregado antes del 26 de julio de 2011.
- Pensar en la satisfacción del cliente.

Cambios de alcance

- Los cambios de alcance serán reflejados en este documento.
- En caso de retraso se realizarán las tareas estrictamente necesarias.

Implicados

- Eva Cutanda: Directora del proyecto, cuyas expectativas son:
    - Que se complete el proyecto.
    - Que el proyecto tenga un alcance suficiente.
    - Que se entregue en fecha.
- Javier Villalta: Alumno cuyas expectativas son:
    - Acumular experiencia.
    - Satisfacer a los clientes.
    - Cumplir con los plazos
    - Aprobar el proyecto fin de carrera
- Clientes (UPV, UPV/EHU):
    - Que se complete el proyecto.
    - Que se realice el mejor aprovechamiento de las facilidades y recursos proporcionados.

Requerimientos y restricciones

Los requerimientos serán cumplir las expectativas nombradas anteriormente.

Las restricciones serán, en principio, los plazos de entrega.

Enfoque del proyecto

Se busca conocer la situación de los sistemas de información escolares. Dada la diversidad de centros necesaria para obtener datos una auditoria mediante encuesta se estima como el mejor método. La encuesta debe ser lo más breve y concisa posible, pero obteniendo la mayor cantidad de información posible.

En la fase de análisis se investigará la influencia del tamaño del sistema de información y el modelo administrativo. Para inferir cualquier tipo de patrón los datos, presumiblemente, seguirán una distribución normal; por lo tanto el patrón deberá mostrarse en torno al 85% de la muestra.

Las soluciones serán lo más económicas posibles, sin obviar la facilidad de uso y la efectividad de las mismas ante las vulnerabilidades.

Estudio del arte

Las referencias empleadas en este proyecto son:

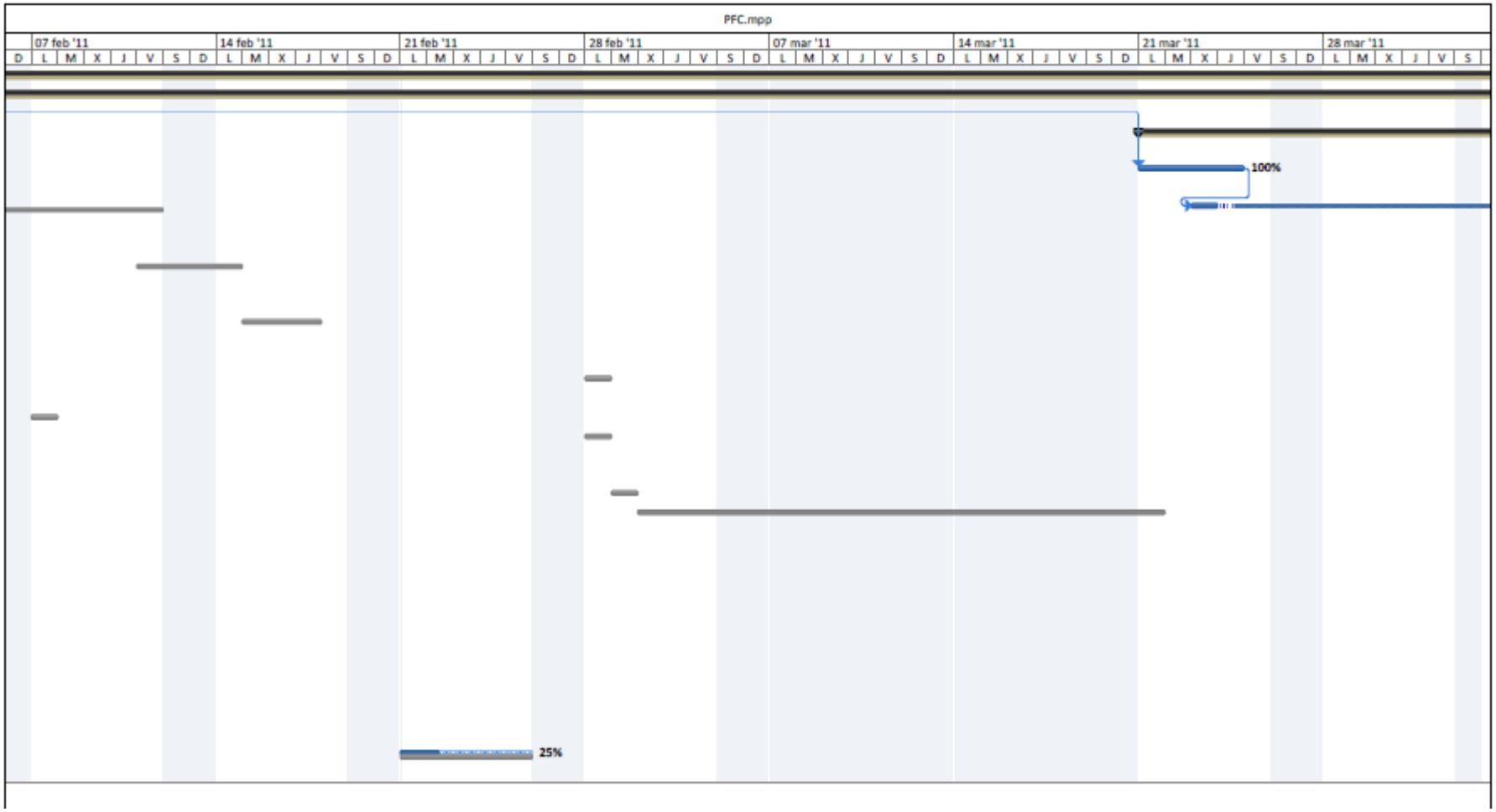
- Plan sectorial de oficio a la enseñanza reglada no universitaria de 29 de diciembre de 2006; Agencia Española de Protección de datos.
- Buenas prácticas TIC; Conselleria d'Educació.

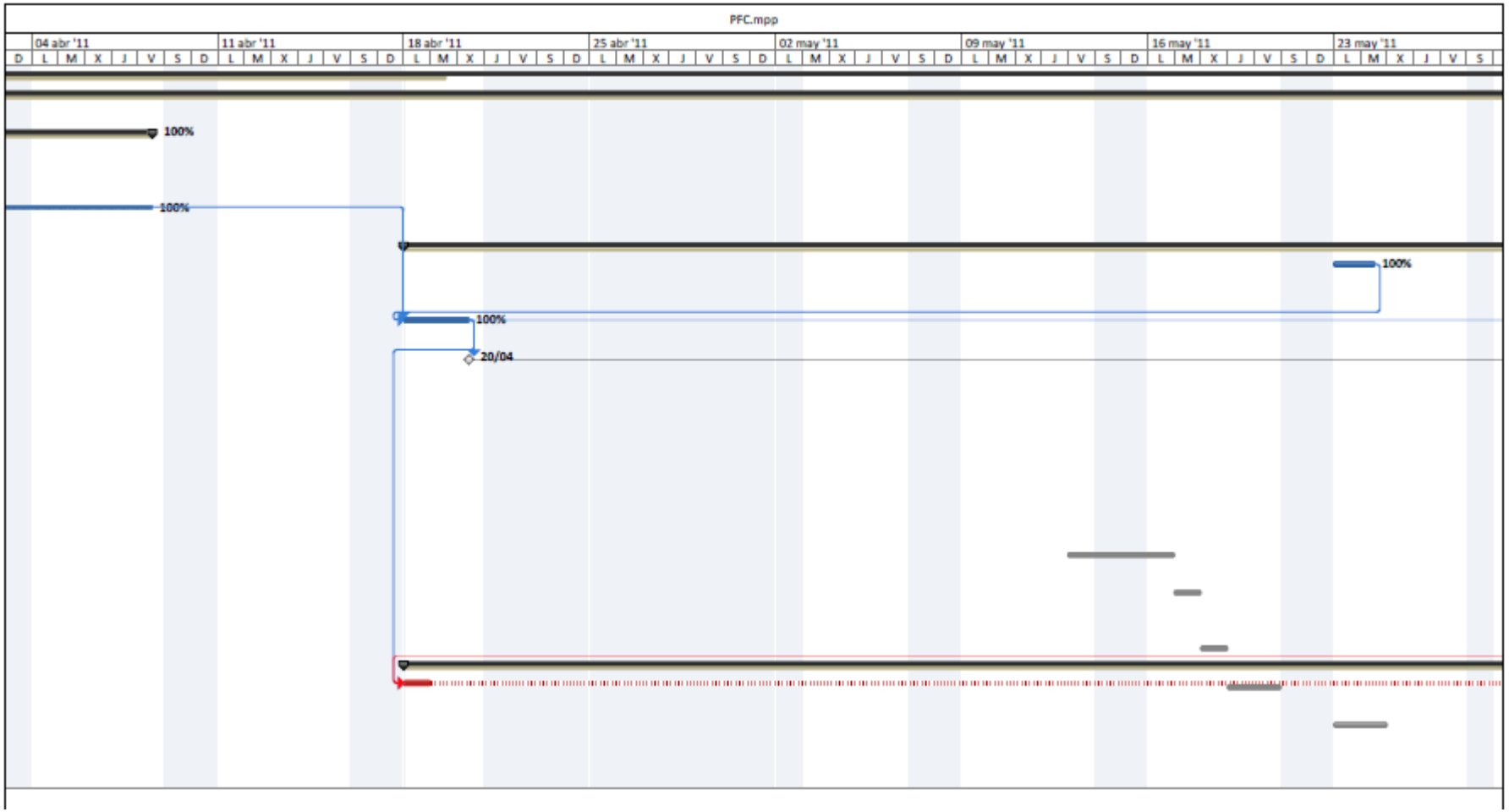
Estas referencias han sido tenidas en cuenta por ser, probablemente, las más fiables. Amén de que otros estudios sobre seguridad en centros escolares inciden más en cuestiones particulares, o comprenden riesgos ajenos al sistema de información.

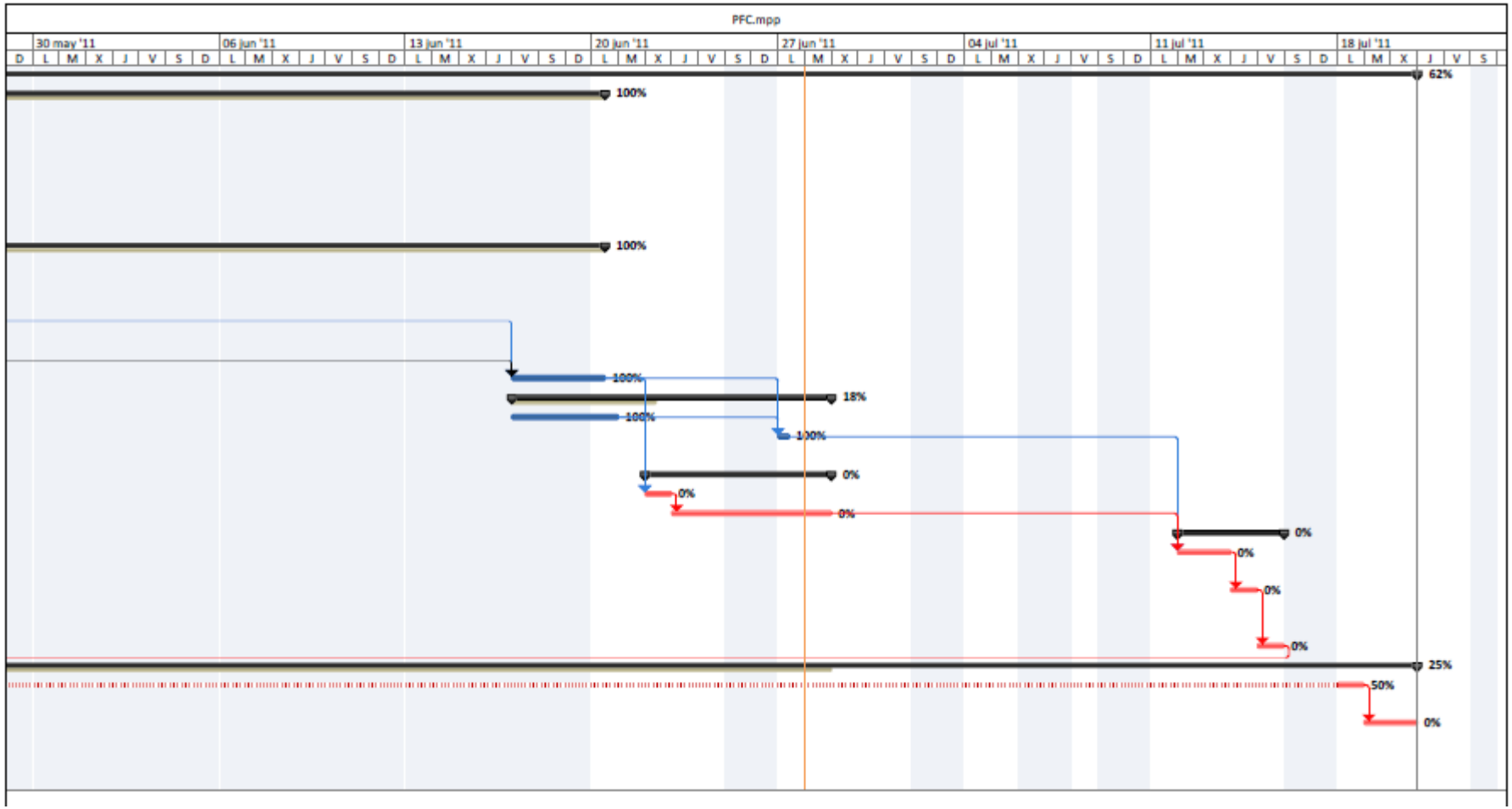
Diagrama de Gantt

PFC.mpp

Id	Nombre de tarea	Comienzo real	Fin real	% completado	% físico comp.	Duración real	Duración restante	Costo real	Trabajo real
1	**Auditoría de centros docentes**	**lun 31/01/11**	**NOD**	**62%**	**0%**	**54,4 días**	**33,6 días**	**4.284,00 €**	**204 horas**
2	**Preparación del cuestionario**	**lun 31/01/11**	**lun 20/06/11**	**100%**	**0%**	**67,38 días**	**0 días**	**3.717,00 €**	**177 horas**
3	Investigar normativa	lun 31/01/11	mar 01/02/11	100%	0%	2 días	0 días	336,00 €	16 horas
4	**consulta de precedentes similares**	**lun 21/03/11**	**vie 08/04/11**	**100%**	**0%**	**14,5 días**	**0 días**	**2.688,00 €**	**128 horas**
5	Buscar sobre seguridad en colegios	lun 21/03/11	jue 24/03/11	100%	0%	4 días	0 días	672,00 €	32 horas
6	Procesar información útil para este PFC	mié 23/03/11	vie 08/04/11	100%	0%	12 días	0 días	2.016,00 €	96 horas
7	**Diseñar cuestionarios**	**lun 18/04/11**	**lun 20/06/11**	**100%**	**0%**	**22,38 días**	**0 días**	**693,00 €**	**33 horas**
8	Buscar y comparar servicios de encuasta on-line	lun 23/05/11	mar 24/05/11	100%	0%	1,5 días	0 días	252,00 €	12 horas
9	Redactar batería de preguntas	lun 18/04/11	mié 20/04/11	100%	0%	2,25 días	0 días	378,00 €	18 horas
10	~~Traducción al Valencià~~	~~NOD~~	~~NOD~~	~~0%~~	~~0%~~	~~0 días~~	~~0 días~~	~~0,00 €~~	~~0 horas~~
11	Implementar cuationarios	vie 17/06/11	lun 20/06/11	100%	0%	0,38 días	0 días	63,00 €	3 horas
12	**Muestreo**	**vie 17/06/11**	**NOD**	**18%**	**0%**	**1,29 días**	**5,71 días**	**189,00 €**	**9 horas**
13	Selección de centros	vie 17/06/11	lun 20/06/11	100%	0%	1 día	0 días	168,00 €	8 horas
14	Enviar invitación de colaboración	lun 27/06/11	lun 27/06/11	100%	0%	0,13 días	0 días	21,00 €	1 hora
15	**Muestreo presencial**	**NOD**	**NOD**	**0%**	**0%**	**0 días**	**5 días**	**0,00 €**	**0 horas**
16	Contactar con centros	NOD	NOD	0%	0%	0 días	1 día	0,00 €	0 horas
17	Visitar centros	NOD	NOD	0%	0%	0 días	4 días	0,00 €	0 horas
18	**Análisis de datos**	**NOD**	**NOD**	**0%**	**0%**	**0 días**	**4 días**	**0,00 €**	**0 horas**
19	Computar datos por categorías	NOD	NOD	0%	0%	0 días	2 días	0,00 €	0 horas
20	Selección de vulnerabilidades significativas	NOD	NOD	0%	0%	0 días	1 día	0,00 €	0 horas
21	Buscar patrones comunes	NOD	NOD	0%	0%	0 días	1 día	0,00 €	0 horas
22	**Proposición de soluciones**	**lun 18/04/11**	**NOD**	**25%**	**0%**	**10,75 días**	**32,25 días**	**168,00 €**	**8 horas**
23	Proponer al menos una solución a cada indicador	lun 18/04/11	NOD	50%	0%	1 día	1 día	168,00 €	8 horas
24	Refinar soluciones en función de los patrones	NOD	NOD	0%	0%	0 días	2 días	0,00 €	0 horas
25	Planificación y gestión del proyecto	lun 21/02/11	NOD	25%	0%	1,25 días	3,75 días	210,00 €	10 horas


PFC.mpp
07 feb '11
14 feb '11
21 feb '11
28 feb '11
07 mar '11
14 mar '11
21 mar '11
28 mar '11
100%
25%


PFC.mpp
04 abr '11
11 abr '11
18 abr '11
25 abr '11
02 may '11
09 may '11
16 may '11
23 may '11
D L M X J V S D L M X J V S D L M X J V S D L M X J V S D L M X J V S D L M X J V S D L M X J V S D L M X J V S
100%
100%
100%
100%
20/04


PFC.mpp
30 may '11
06 jun '11
13 jun '11
20 jun '11
27 jun '11
04 jul '11
11 jul '11
18 jul '11
62%
100%
100%
100%
18%
100%
0%
0%
0%
0%
0%
0%
0%
25%
50%
0%

Plan de comunicaciones

Contenido

Requisitos comunicativos

- El alumno debe familiarizarse con los términos propios del ámbito de la seguridad informática para afinar la precisión de la comunicación.
- El alumno tratará de realizar la comunicación más clara posible en los entregables dirigidos a los centros docentes, pues se entiende que posiblemente necesiten explicaciones complementarias para comprender algunos conceptos.
- El equipo (directora y alumno) debe comunicarse para compartir información con el fin de sacar el proyecto adelante.
- El director debe poder dirigirse al alumno para poder indicar correcciones.

Comunicación entre implicados

- La comunicación con los centros se realiza a través del formulario/interfaz de la encuesta y la cuenta de correo electrónico "Gmail" que le da soporte.
- Son dos los modos de comunicación entre los miembros del equipo: presencial (reuniones) y no presencial.
    - Las reuniones tienen lugar cuando se estima que no es suficiente la comunicación por medio de correo electrónico. Se utilizan cuando es necesario firmar documentos o compartir información de modo más desarrollado que el escrito.
    - La otra forma en la que los diferentes miembros del equipo se ponen en contacto es mediante el correo electrónico y de manera más urgente, el teléfono móvil (Directora > alumno 615 722 756). Para compartir archivos de datos se adjuntan los ficheros a los correos.
- Finalmente, la memoria del proyecto compilará todos los entregables generados durante su desarrollo.

Descripción de elementos de comunicación

- Correo electrónico (UPV/Gmail): en el asunto de cada mensaje deben figurar las siglas PFC.
- Soportes de archivo (pendrive, Dropbox y disco duro externo): El espacio se divide en carpetas donde se recogerá la información de manera organizada.
- Calendario: muestra cuando se debe realizar cada tarea.
- Reuniones: se convocarán sólo las imprescindibles.
- Google Docs: Da soporte a la encuesta on-line.

Tabla Pull

Quien	Que	Permiso
Alumno	Archivo	Total
Alumno	Google Docs	Total
Mundo	Formulario de encuesta	Escritura[1]
Directora	Documentos	Lectura[2]

Tabla Push

De quien	Que	A quien	Cuando	Como	Coste
Directora	Directrices	Alumno	Horas de tutoría	Reunión	Temporal
Directora	Directrices	Alumno	Indiferente	E-mail	Temporal
Alumno	Encuesta	Centros escolares	Indiferente	Formulario web	Temporal
Centros escolares	Comentarios	Equipo	Indiferente	Formulario web	Temporal
Alumno	Consultas	Directora	Horas de tutoría	Reunión	Temporal
Alumno	Consultas	Directora	Siempre	E-mail	Temporal

[1] Únicamente pueden introducir sus respuestas, pero una vez enviadas no pueden corregirlas.

[2] No tiene facultad para modificar directamente los documentos, pero si para indicar correcciones en los mismos.

Gestión de riesgos

Contenido

Identificación de los riesgos

- **Planificación**
  - **Alcance**
    - **No llegar a todos los objetivos**: es probable que ocurra, puede que sea necesario recortar las prestaciones por falta de tiempo, esto ocurriría cuando se acercase la fecha límite.
  - **Plazos**
    - **Estimación de los plazos**: es medianamente probable que no haya estimado bien los plazos, esto pude darse en cualquier momento.
  - **Riesgos**
    - **Identificación**: es poco probable que se identifiquen todos los riesgos potenciales de este proyecto. Esto ocurre en la identificación de los riesgos.
  - **RRHH**
    - **Rendimiento**: probable, la dedicación no exclusiva al proyecto puede hacer que descienda el rendimiento.
    - **Tiempo disponible**: es probable que descienda el tiempo disponible para desarrollar el proyecto. Podría ocurrir en cualquier momento.
    - **Abandono**: poco o nada probable, las condiciones del programa de intercambio universitario dentro del cual se desarrolla este proyecto no permiten el abandono; salvo causa de fuerza mayor.
    - **Motivación**: es poco probable porque a medida que se avanza se tiene más ganas de terminar.
    - **Conocimiento**: es muy probable porque no se tiene experiencia en el área.
  - **Calidad**
    - **Identificación las expectativas a satisfacer**: es probable que las identifiquemos y pueden ser erróneas o aceptables, esto ocurriría durante la planificación de la calidad.
- **Técnicos**
  - **Archivo (Copia de seguridad en Dropbox)**
    - **Indisponibilidad temporal**: es muy probable y puede ocurrir en cualquier momento.
    - **Indisponibilidad permanente**: poco probable y podría ocurrir en cualquier momento.
    - **Desorganización**: es poco probable, puede haber mucha, poca o ninguna y puede ocurrir en cualquier momento.
  - **Archivo (Pendrive)**
    - **Indisponibilidad temporal**: es muy poco probable y puede ocurrir en cualquier momento.
    - **Indisponibilidad permanente**: muy poco probable y podría ocurrir en cualquier momento.

        - **Desorganización**: es poco probable, puede haber mucha, poca o ninguna y puede ocurrir en cualquier momento.
    - **Archivo (Copia de seguridad en un disco duro externo)**
        - **Indisponibilidad temporal**: es muy poco probable y puede ocurrir en cualquier momento.
        - **Indisponibilidad permanente**: muy poco probable y podría ocurrir en cualquier momento.
        - **Desorganización**: es poco probable, puede haber mucha, poca o ninguna y puede ocurrir en cualquier momento.
    - **Plataforma encuesta web (Google docs)**
        - **Indisponibilidad temporal**: es muy probable y puede ocurrir en cualquier momento.
        - **Indisponibilidad permanente**: poco probable y podría ocurrir en cualquier momento.
    - **Correo electrónico (UPV)**
        - **No disponibilidad temporal**: es poco probable pero podría ocurrir en cualquier momento.
    - **Hardware/Software**
        - **Integración**: es probable y puede ser mala, normal o buena y podría ocurrir en la ejecución del proyecto.
        - **Factores ambientales**: es probable que las temperaturas elevadas pongan en riesgo el buen funcionamiento de equipos informáticos.
        - **Malware, virus y otro patógenos**: es probable en el escenario actual, amén de que el software de prevención no puede detectar el 100% de las amenazas. Es un riesgo durante todo el proyecto.
- **Jurídicos**
    - **Marco legal**
        - **Incumplimiento**: es probable y puede ser muy grave, moderado, leve o ninguno; principalmente por desconocimiento. Puede ocurrir en cualquier momento.
- **Contexto**
    - **Tareas**
        - **Realización**: es muy probable y pueden ser buenas, normales o malas, pudiendo ocurrir en cualquier momento.
        - **Incoherencia**: es poco probable, puede haber mucha, poca o ninguna pudiendo ocurrir en cualquier momento.
    - **Entregas**
        - **Olvido**: es muy poco probable y puede ser completo, parcial o nulo y pude ocurrir cuando menos te lo esperas.
        - **Cumplimiento de plazos**: es probable, puede que se cumplan o puede que no y puede pasar en cualquier momento.
    - **RRHH**

        - **Baja temporal**: es probable que algún tiempo estén incapacitado, puede que sea mucho tiempo, poco o ninguno pudiendo ocurrir en cualquier momento.
        - **Baja permanente**: es muy poco probable y puede ocurrir en cualquier momento.
    - **Director del proyecto**
        - **Valoración del trabajo**: es probable y puede ser insuficiente, suficiente o destacada, puede ocurrir durante todo el proyecto.
        - **Aprobación del proyecto**: es probable que se apruebe y esto ocurriría al final del proyecto.
    - **Programa de intercambio**
        - **Incumplimiento de requisitos:** es poco probable su incumplimiento, puede suceder hacia el final del proyecto.
        - **Cultura local:** es muy probable durante todo el proyecto.

Cuantificación de los riesgos

Rama	Tipo	Riesgo	Proba-bilidad	Impac-to	Valor espera-do
Planificación	Alcance	No llegar a todos los objetivos	20%	40%	8%
	Plazos	Estimación de los plazos	10%	5%	0,5%
	Riesgos	Identificación	10%	20%	2%
	RRHH	Rendimiento	20%	10%	2%
		Tiempo disponible	20%	20%	4%
		Abandono	2%	20%	0,4%
		Motivación	5%	5%	0,25
		Conocimiento	10%	10%	1%
	Calidad	Identificación de las expectativas a satisfacer	10%	20%	2%
Técnicos	Archivo (Dropbox)	Indisponibilidad temporal	20%	10%	2%
		Indisponibilidad permanente	2%	40%	0,8%
		Desorganización	25%	20%	5%
	Archivo (Pendrive)	Indisponibilidad temporal	15%	10%	1,5%
		Indisponibilidad permanente	5%	40%	2%
		Desorganización	25%	20%	5%
	Archivo (Disco duro)	Indisponibilidad temporal	10%	10%	1%

		Indisponibilidad permanente	1%	40%	0,4%
		Desorganización	25%	20%	5%
	Plataforma encuesta web	Indisponibilidad temporal	20%	10%	2%
		Indisponibilidad permanente	2%	40%	0,8%
	Correo electrónico	No disponibilidad temporal	2%	10%	0,2%
	Mensajería instantánea	No disponibilidad temporal	10%	2%	0,2%
	Hardware / software	Integración	5%	5%	0,25%
		Factores ambientales	1%	90%	0,9%
		Malware, virus y otro patógenos	5%	95%	4,75%
Jurídicos	Marco legal	incumplimiento	2%	45%	0,9%
Contexto	Tareas	Realización	30%	25%	7,5%
		incoherencia	20%	15%	3%
	Entregas	Olvido	20%	20%	4%
		Cumplimiento de los plazos	40%	30%	12%
	RRHH	Baja temporal	5%	20%	1%
		Baja permanente	1%	20%	0,2%
	Director	Valoración del trabajo	5%	10%	0,5%
		Aprobación del proyecto	5%	60%	3%

	Programa de intercambio	Incumplimiento de requisitos	30%	100%	30%
		Cultura local	90%	45%	40,5%

Síntomas de riesgos

- **Planificación**
  - **Alcance**
    - **No llegar a todos los objetivos**: demasiado optimismo al planificar el alcance.
    - **Modificación de los requisitos**: desarrollar pocos requisitos.
  - **Plazos**
    - **Estimación de los plazos**: tendencia a retrasar siempre las tareas.
  - **Riesgos**
    - **Identificación**: no identificar muchos riesgos.
  - **RRHH**
    - **Rendimiento**: ver poca productividad.
    - **Tiempo disponible**: tener poco tiempo libre para dedicar al proyecto.
    - **Abandono**: dejadez de las tareas programadas.
    - **Motivación**: pasotismo y desidia ante el montante de trabajo restante.
    - **Conocimiento**: no demostrar conocimiento durante el desarrollo de las tareas.
    - **Inversión de tiempo**: estadísticas de partes.
    - **Tensiones internas**: malas contestaciones y malas caras.
  - **Calidad**
    - **Identificación las expectativas a satisfacer**: si se identifican muy pocas, seguramente habrá que repetir o añadir más.
- **Técnicos**
  - **Archivo (Dropbox)**
    - **Disponibilidad temporal**: caídas del servicio en otras ocasiones.
    - **Disponibilidad permanente**: por las caídas del servicio en otras ocasiones.
    - **Desorganización**: no encontrar lo que se busca fácilmente.
  - **Archivo (Pendrive)**
    - **Disponibilidad temporal**: escrituras incorrectas o extravío del dispositivo.
    - **Disponibilidad permanente**: pérdida, sustracción o avería del dispositivo.
    - **Desorganización**: no encontrar lo que se busca fácilmente.
  - **Archivo (Disco duro externo)**
    - **Disponibilidad temporal**: sectores defectuosos o archivos corrompidos.
    - **Disponibilidad permanente**: pérdida, sustracción o avería del dispositivo.
    - **Desorganización**: no encontrar lo que se busca fácilmente.

    - **Plataforma encuesta web (Google Docs)**
        - **Disponibilidad temporal**: caídas del servicio en otras ocasiones.
        - **Disponibilidad permanente**: por las caídas del servicio en otras ocasiones.
    - **Correo electrónico (UPV)**
        - **No disponibilidad temporal**: caídas del servicio en otras ocasiones, u otras incidencias como correos perdidos o entregados con retraso.
    - **Mensajería instantánea**
        - **No disponibilidad temporal**: caídas del servicio en otras ocasiones.
    - **Hardware/Software**
        - **Integración**: en caso de no ser accesible la información.
        - **Factores ambientales**: temperaturas por encima del régimen de trabajo de los componentes.
        - **Malware, virus y otros patógenos**: desaparición de archivos, creación de ficheros sospechosos, desempeño errático de sistema operativo o aplicaciones de muy dudosa procedencia.
- **Jurídicos**
    - **Marco legal**
        - **Incumplimiento**: no informarse sobre las condiciones particulares del "contrato de licencia de usuario final" de los servicios empleados.
- **Contexto**
    - **Tareas**
        - **Realización**: en caso de que no se realicen las tareas.
        - **Incoherencia**: revisando todas las tareas.
    - **Entregas**
        - **Olvido**: si faltan entregables o tareas de la EDT sin realizar.
        - **Cumplimiento de plazos**: realizando un seguimiento del calendario.
    - **RRHH**
        - **Baja temporal**: principalmente, cuestiones médicas; o de cualquier otra índole que afecten a la disponibilidad.
        - **Baja permanente**: principalmente, cuestiones médicas; o de cualquier otra índole que afecten a la disponibilidad.
    - **Director del proyecto**
        - **Valoración del trabajo**: si detecta alguna falta una falta.
        - **Aprobación del proyecto**: en caso de que el director indique falta de alcance.
    - **Programa de intercambio**
        - **Incumplimiento de requisitos:** incumplir el calendario establecido.

- **Cultura local:** interesarse por la cultura local, no teniendo tiempo para dedicar a la misma; desviando el tiempo necesario para completar el proyecto.

Control de riesgos

- **Planificación**
  - **Alcance**
    - **No llegar a todos los objetivos**: intentar planificar bien el alcance. Modificarlo en caso de que sea necesario.
    - **Modificación de los requisitos**: intentar realizar correctamente los requisitos. Actualizarlos cuando sea necesario.
  - **Plazos**
    - **Estimación de los plazos**: tener en cuenta el calendario. Siempre se podrán modificar.
  - **Riesgos**
    - **Identificación**: intentar identificarlos correctamente. Ir añadiendo riesgos según vayan apareciendo.
  - **RRHH**
    - **Rendimiento**: motivar. En caso de que no haya rendimiento, planificar mejor las tareas a realizar.
    - **Tiempo disponible**: tener en cuenta el calendario y las tareas prioritarias en cada momento. Distribuir mejor las tareas según el tiempo disponible.
    - **Abandono**: realizar los trámites oportunos.
    - **Motivación**: estimular la curiosidad por el área en la que se desarrolla el proyecto.
    - **Conocimiento**: estudiar y profundizar en los aspectos que se ignoren del proyecto.
  - **Calidad**
    - **Identificación las expectativas a satisfacer**: prestar atención sobre las expectativas a satisfacer.
- **Técnicos**
  - **Archivo (Copia de seguridad en Dropbox)**
    - **Disponibilidad temporal**: utilizar otra copia de seguridad. En caso reiterado, cambiar de sistema.
    - **Disponibilidad permanente**: utilizar otra copia de seguridad. En caso reiterado, cambiar de sistema.
    - **Desorganización**: nombrar bien cada sección. Modificar las secciones.
  - **Archivo (Pendrive)**
    - **Disponibilidad temporal**: utilizar una copia de seguridad. En caso reiterado, cambiar de dispositivo.
    - **Disponibilidad permanente**: utilizar una copia de seguridad. En caso reiterado, cambiar de dispositivo.
    - **Desorganización**: nombrar bien cada sección. Modificar las secciones.
  - **Archivo (Copia de seguridad en disco duro externo)**

        - **Disponibilidad temporal**: utilizar otra copia de seguridad. En caso reiterado, cambiar de dispositivo.
        - **Disponibilidad permanente**: utilizar otra copia de seguridad. En caso reiterado, cambiar de dispositivo.
        - **Desorganización**: nombrar bien cada sección. Modificar las secciones.
    - **Plataforma encuesta web (Google docs)**
        - **Disponibilidad temporal**: esperar al restablecimiento del servicio.
        - **Disponibilidad permanente**: cambiar de sistema.
        - **Desorganización**: nombrar bien cada sección. Modificar las secciones.
    - **Correo electrónico (UPV)**
        - **No disponibilidad temporal**: disponer de más de un servidor de correo. Utilizar otro método de comunicación si ocurre. Informar a los posibles receptores de la dirección alternativa.
    - **Hardware/Software**
        - **Integración**: estudiar las posibles incompatibilidades y soluciones a las mismas.
        - **Factores ambientales:** detectar y estudiar medidas para corregir dichos factores. VG: ayudar a la refrigeración del equipo informático.
        - **Malware, virus y otro patógenos**: emplear software específico para la protección y/o desinfección del sistema; en caso extremo, restaurar el sistema siguiendo un plan de contingencia.
- **Jurídicos**
    - **Marco legal**
        - **Incumplimiento**: prestar atención a los documentos de naturaleza legal.
- **Contexto**
    - **Tareas**
        - **Realización**: realizar las tareas para días antes de la entrega.
        - **Incoherencia**: comprender bien lo que se debe realizar, solventar todas las dudas. Revisar y arreglar las tareas.
    - **Entregas**
        - **Olvido**: recordar las fechas de entrega. Programar avisos en el gestor de correo electrónico.
        - **Cumplimiento de plazos**: recordar las fechas de entrega. Programar avisos en el gestor de correo electrónico.
    - **RRHH**
        - **Baja temporal**: seguir el tratamiento médico o mitigar la causa de la baja temporal.
        - **Baja permanente**: seguir el tratamiento médico o mitigar la causa de la baja.
    - **Director del proyecto**

        - **Valoración del trabajo**: ceñirse a lo que se debe hacer. Corregir errores.
        - **Aprobación del proyecto**: llevar comunicación con el director. Modificar cuanto sea necesario.
    - **Programa de intercambio**
        - **Incumplimiento de requisitos:** leer y comprender las condiciones del programa. Destacar los requisitos para tenerlos presentes.
        - **Cultura local:** dedicar tiempo a conocer la cultura local cuando se dispone del mismo, no en picos de trabajo.

Informe de costes, contrataciones y compras

Contenido

Costes

Necesidades de recursos

1. Preparación del cuestionario 120h
   1.1. Investigar normativa 16h 1 persona
   1.2. Consulta de precedentes similares 56h
      1.2.1. Buscar sobre seguridad en colegios 16h 1 persona
      1.2.2. Procesar información útil para este PFC 40h 1 persona
   1.3. Diseñar cuestionarios 48h
      1.3.1. Buscar y comparar servicios de encuesta on-line 12h 1 persona
      1.3.2. Redactar batería de preguntas 24h 1 persona
      1.3.3. Traducción a Valencià 8h 2 personas
         - Se requiere colaboración para la traducción pues el alumno no habla valenciano.
      1.3.4. Implementar cuestionarios 4h 1 persona
         - El cuestionario se implementa a través de la tecnología de Google Docs. Su uso es gratuito.
2. Muestreo 48h
   2.1. Selección de centros 4h 1 persona
   2.2. Enviar invitación de colaboración 4h 1 persona
      - Gracias a la integración de servicios de Google, es posible mandar la encuesta por e-mail desde la interfaz de Google Docs usando Gmail. Servicio gratuito.
   2.3. Muestreo presencial 40h
      2.3.1. Contactar con centros 8h 1 persona
      2.3.2. Visitar centros 32h 1 persona
3. Análisis de datos 32h
   3.1. Computar datos por categorías 16h 1 persona
   3.2. Selección de vulnerabilidades significativas 8h 1 persona
   3.3. Busca patrones comunes 8h 1 persona
4. Proposición de soluciones 32h
   4.1. Proponer al menos una solución a cada indicador 16h 1 persona
   4.2. Refinar soluciones en función de los patrones 16h 1 persona
5. Planificación y gestión 40h 1 persona
      - Ms Project: MSDN Academic Aliance aporta licencias gratuitas a estudiantes para el uso de las mismas en trabajos académicos, como es el caso. Necesario para la gestión del proyecto.
      - Drop box: licencia de uso gratuita. Necesidad de archivo.
      - Pendrive: amortizado. Necesidad de archivo.
      - Disco duro externo: amortizado. Necesidad de archivo.

Estimación de costes

Se requieren aproximadamente 280h de esfuerzo y una partida económica nula para el uso de los servicios específicos requeridos. El valor económico de la ejecución del proyecto se estima en 6.938€ ± 694€. Los equipos y licencias (sistema operativo, suite ofimática,...) empleados serían imputables a costes generales pero por su edad se pueden considerar amortizados. Ver el desglose en la base de costes.

Base de costes

Nivel	Descripción	Esfuerzo Horas/persona	Personas asignadas	Esfuerzo total	Otros recursos Descripción	Otros recursos Coste en €	Coste de la tarea Coste en €	Coste de la tarea Coste con IVA
1	Preparación del cuestionario	120	1	128			2.688 €	3.172 €
1 1	Investigar normativa	16	1	16			336 €	396 €
1 2	Consulta de precedentes similares	56	1	56			1.176 €	1.388 €
1 2 1	Buscar sobre seguridad en colegios	16	1	16			336 €	396 €
1 2 2	Procesar información útil para este PFC	40	1	40			840 €	991 €
1 3	Diseñar cuestionarios	48	1	56			1.176 €	1.388 €
1 3 1	Buscar y comparar servicios de encuesta on-line	12	1	12			252 €	297 €
1 3 2	Redactar batería de preguntas	24	1	24			504 €	595 €
1 3 3	Traducción a Valencià	8	2	16			336 €	396 €
1 3 4	Implementar cuestionarios	4	1	4	GoogleDocs	0 €	84 €	99 €
2	Muestreo	48	1	48			1.008 €	1.189 €
2 1	Selección de centros	4	1	4			84 €	99 €
2 2	Enviar invitación de colaboración	4	1	4	Gmail	0 €	84 €	99 €
2 3	Muestreo presencial	40	1	40			840 €	991 €
2 3 1	Contactar con centros	8	1	8			168 €	198 €
2 3 2	Visitar centros	32	1	32			672 €	793 €
3	Análisis de datos	32	1	32			672 €	793 €
3 1	Computar datos por categorías	16	1	16			336 €	396 €
3 2	Selección de vulnerabilidades significativas	8	1	8			168 €	198 €
3 3	Busca patrones comunes	8	1	8			168 €	198 €
4	Proposición de soluciones	32	1	32			672 €	793 €
4 1	Proponer al menos una solución a cada indicador	16	1	16			336 €	396 €
4 2	Refinar soluciones en función de los patrones	16	1	16			336 €	396 €
5	Planificación y gestión	40	1	40	Ms Project	0 €	840 €	991 €
					Drop box	0 €		
					Pendrive	0 €		
					Disco duro externo	0 €		
			total horas	**280**		**- €**	**5.880,00 €**	**6.938,00 €**
			coste hora	**21 €**				

Contrataciones y compras

Elementos principales de aprovisionamiento

Supuestos

- Las herramientas ofimáticas, equipos y demás software de uso corriente que ya estén a disposición del alumno; se consideran amortizadas.
- La licencia MSDN Academic Aliance cubre el uso de Ms Project dentro de este proyecto.
- Para la valoración económica del proyecto, se ha supuesto que el coste de por hora del trabajo del alumno sería de veintiún euros. Esta cifra se ha obtenido a partir de las prácticas de la asignatura ENT, pues se estima que era una buena referencia.

Restricciones

- No se dispone de liquidez para adquirir ningún tipo de herramienta.

Compras

- Cuenta de usuario Google ..... 0€
- Cuenta de usuario Drop box ..... 0€
- Licencia Ms Project (MSDN Academic Aliance) ..... 0€

Análisis de compra

- Google Docs: se optó por esta opción por la facilidad para implementar el formulario, la posibilidad de mandarlo en el cuerpo de un e-mail y la compilación de datos en hoja de cálculo.
- Drop box: está elección de almacenamiento en la nube fue seleccionada en lugar de otras candidatas como Skydrive de Microsoft, por su fácil integración con el sistema, a través de una carpeta local sincronizada con el servidor; a pesar de que oferta menos espacio, 2 GB.
- Ms Project: entre las distintas oportunidades sin coste, Project se postulaba como la más completa.

Tiempo dedicado a la planificación de contrataciones y compras

En el caso de Google Docs el tiempo dedicado está asignado en una tarea específica para ello. En los casos restantes, dicho trabajo se encuentra embebido en la tarea de gestión del proyecto.

Sobre las contrataciones

El personal disponible para ejecutar este proyecto es la directora y el alumno. La aportación al proyecto de la directora es el visado y corrección del trabajo del alumno. Por su parte, el alumno es el encargado de completar la EDT del proyecto.

No median otras relaciones contractuales en este proyecto.

Estructura de Descomposición del Trabajo

EDT

Nivel			Descripción
1			Preparación del cuestionario
1	1		Investigar normativa
1	2		Consulta de precedentes similares
1	2	1	Buscar sobre seguridad en colegios
1	2	2	Procesar información útil para este PFC
1	3		Diseñar cuestionarios
1	3	1	Buscar y comparar servicios de encuesta on-line
1	3	2	Redactar batería de preguntas
1	3	3	Traducción a Valencià
1	3	4	Implementar cuestionarios
2			Muestreo
2	1		Selección de centros
2	2		Enviar invitación de colaboración
2	3		Muestreo presencial
2	3	1	Contactar con centros
2	3	2	Visitar centros
3			Análisis de datos
3	1		Computar datos por categorías
3	2		Selección de vulnerabilidades significativas
3	3		Busca patrones comunes
4			Proposición de soluciones
4	1		Proponer al menos una solución a cada indicador
4	2		Refinar soluciones en función de los patrones
5			Planificación y gestión

Lista de entregables

Contenido

Entregables sobre la gestión del proyecto

- Informe de definición del proyecto.
    - Alcance.
    - Implicados.
    - Enfoque del proyecto.
    - Criterios de finalización.
- Plan del proyecto.
    - Diagrama de Gantt.
    - Plan de comunicaciones
    - Plan de gestión de riesgos.
    - Informe de costes, contrataciones y compras.
    - Estructura de desglose del trabajo.
    - Lista de entregables (este documento).
    - Informe de calidad.
    - Plan de gestión de la seguridad.
        - Plan de copias de seguridad.
        - Políticas de seguridad.
- Informe de seguimiento.

Entregables propios del proyecto

- Análisis de riesgos de los centros.
- Cuestionario empleado en la auditoría.
- Listado de centros empleado como muestra.
- Hoja de cálculo con los datos de la encuesta.
- Informe de análisis de datos.
- Informe de soluciones.

Entregables anexos

- Solicitud de aprobación de proyecto - modelo 'B', según ETS de informática de la UPV.
- Solicitud de evaluación del proyecto por Director, según ETS de informática de la UPV.
- Autorización para la difusión de obras digitales a favor del Área de Biblioteca y Documentación Científica de la Universidad Politécnica de Valencia, según ETS de informática de la UPV.

Informe de calidad

Contenido

Criterios de calidad

A fin de establecer una idea de los posibles procesos contra el sistema de información, se toma en consideración el *Plan sectorial de oficio a la enseñanza reglada no universitaria* de la Agencia Española de protección de datos. Adicionalmente, para la elaboración del cuestionario de la auditoría también se han tenido en cuenta la norma ISO 27002, así como el libro *Buenas prácticas TIC* desarrollado por la Conselleria d'Educació.

Será criterio de calidad el hecho de proponer al menos una solución por cada ítem del cuestionario.

Definiremos como *patrón*, el conjunto de vulnerabilidades (Ítems con respuesta negativa) comunes a la muestra sin agrupación o en función de una variable de agrupación. Será criterio de calidad el hecho de proponer al menos una solución a cada *patrón* deducido.

Las propuestas de solución vinculadas al tratamiento de datos de carácter personal deberán observar la LOPD[3].

Las posibles soluciones deberán poseer un valor económico razonable.

Se considerará posible solución cualquier elemento técnico, organizativo o de gestión que elimine, mitigue o capacite la continuidad en caso de explotación de alguna vulnerabilidad.

El informe resultante redactarse de modo inteligible para cualquier responsable escolar, con la mayor rigurosidad técnica posible.

En el caso de soluciones técnicas, el cumplimiento de los requerimientos legales es responsabilidad de sus respectivos desarrolladores. De igual modo, la responsabilidad subsidiaria del buen funcionamiento del software o hardware no es imputable al equipo del proyecto o la UPV. El proyecto no incluye fase alguna relativa al control del buen funcionamiento de la integración de soluciones total o parcialmente.

El equipo tampoco se hace responsable de la calidad de los manuales de las aplicaciones.

La gestión del proyecto será verificada por la directora, Eva Mª Cutanda García.

Todo entregable o documento de gestión tendrá en su nombre de archivo la numeración de la versión. Concretamente, la leyenda seguirá este formato "_V*.&"; siendo '*' y '&' números enteros. El primer digito expresa cambio importantes entre versiones del documento, mientras que el segundo informa sobre variaciones que afectan de forma limitada al documento.

Los cambios y correcciones en los documentos de gestión podrán ser introducidos en reunión o por vía telemática a petición de la directora. Los cambios se comunicarán a la directora por e-mail adjuntando la versión revisada del documento objeto de dicha

[3] Ley orgánica de protección de datos (ver https://www.agpd.es/portalweb/index-ides-idphp.php)

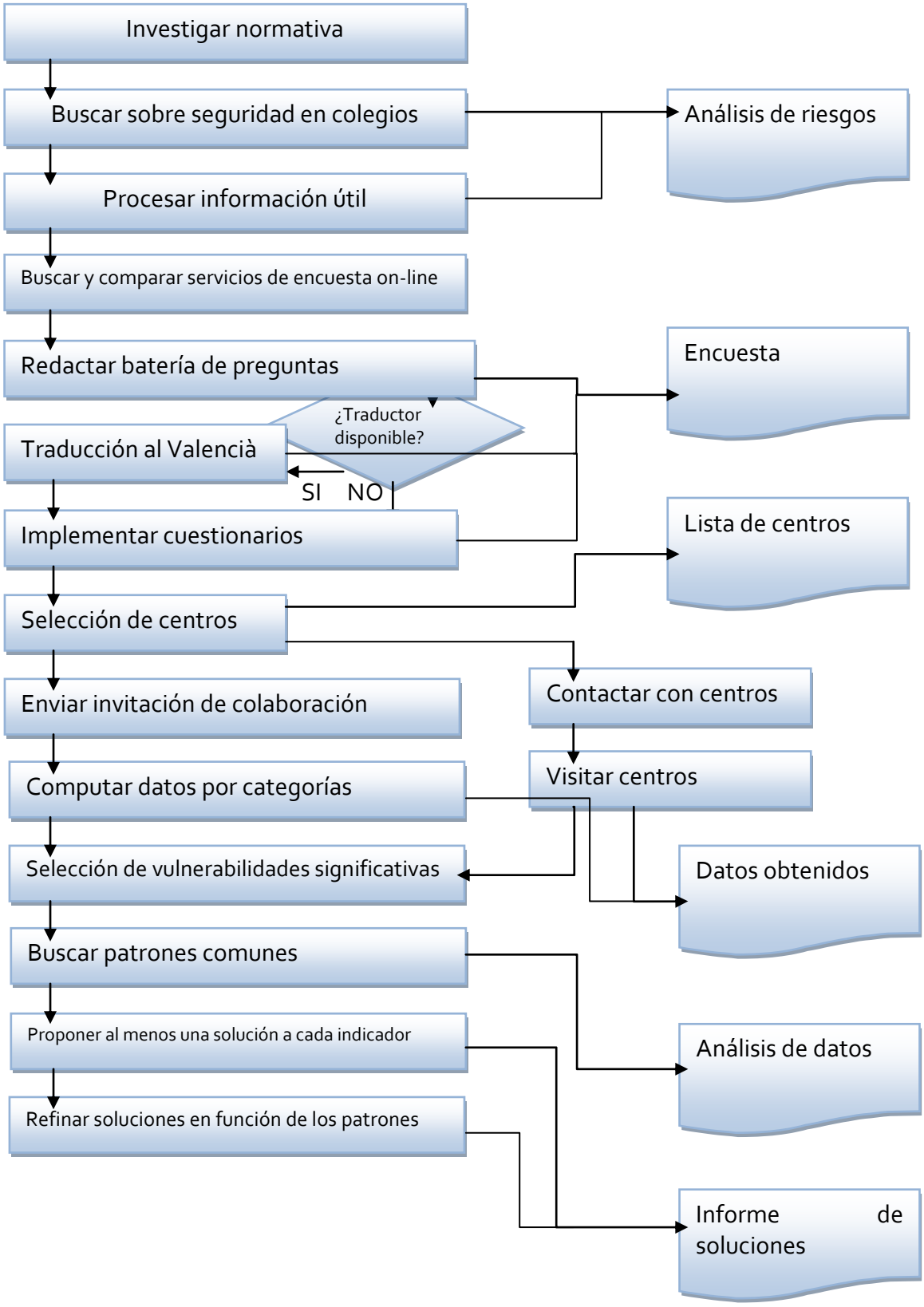
modificación; siempre y cuando se le haya hecho participe de una versión anterior. El alumno es libre de modificar los documentos en cuanto estime oportuno hasta la petición inicial de visado de los mismos; tras lo cual, seguirá la norma anteriormente mentada.

Finalmente, los cambios en el plan de calidad podrán ser introducidos siguiendo el mismo proceso que cualquier otro documento del proyecto.

Definiciones operativas

- Activo: elemento del sistema de información poseedor de un valor intrínseco para el mismo.
- Amenaza: evento de diversa naturaleza que perjudica el valor del activo.
- Riesgo: Probabilidad de materialización de una amenaza.
- Vulnerabilidad: error u omisión en la protección de un activo que incrementa el riego de una amenaza potencial.
- Impacto: medida del valor restado al activo tras la plasmación de una amenaza. Un impacto total o del 100% supone la total pérdida del valor del activo.
- Solución: medida de naturaleza técnica, orgánica o gestora encaminada a eliminar, mitigar o recuperar el impacto causado por la culminación de una amenaza.

Flujos de trabajo



Plan de seguridad

Contenido

Plan de copias de seguridad

- El pendrive será el soporte principal del archivo, por tanto, sobre el que se trabajará directamente.
- Todo cambio sobre los documento del soporte principal será sincronizado sobre la carpeta *DropBox* local al finalizar el trabajo; y a su vez, esta carpeta se sincronizará con su equivalente en la nube en cuanto sea posible.
- Semanalmente se harán copias incrementales sobre un disco duro externo, actualizando todos los documentos existentes. Las versiones anteriores serán reemplazadas.
- Al menos uno de los soportes *off-line* (pendrive, carpeta local *DropBox* y disco duro externo) será almacenado separadamente de los demás y será cuidadosamente guardado.
- El disco duro externo no abandonará el domicilio del alumno.
- En caso de fallo del soporte principal, en primera instancia se acudirá a la carpeta local *DropBox*; y en caso de indisponibilidad de esta, se acudirá a la copia *DropBox* en la nube o a la del disco duro externo según cuál sea su actualidad.

Políticas de seguridad

- El equipo de trabajo tendrá instalado un antivirus, el cual se actualizará siempre que sea posible.
- Cada pendrive que se conecte al equipo de trabajo será examinado, para evitar una posible infección.
- Las cuentas de usuario empleadas en el proyecto, bien sean servicios on-line bien sea la cuenta de usuario del sistema operativo, tendrán contraseñas sujetas a los siguiente criterios.
    - Una longitud mínima de ocho caracteres.
    - Se emplearán caracteres alfanuméricos en mayúsculas y minúsculas y símbolos.
    - No se emplearán datos personales como fechas señaladas o nombres significativos.
    - No utilizar palabras contenidas en diccionarios.
    - Se usarán claves generadas aleatoriamente.
    - No se empleará la misma contraseña para todas las cuentas.
    - Las contraseñas se guardarán en una base de datos protegida con la aplicación passwordsafe.
    - No dejar ninguna contraseña o indicio de contraseña al alcance.

    - Cambiar las contraseñas periódicamente en el caso de servicios en los que previamente se tenía cuenta de usuario. En el caso de cuenta abierta para este proyecto no será necesario pues su vigencia acabará con el proyecto.
- En todo momento el equipo contará con la batería para poder ser utilizada como SAI en caso de corte del suministro eléctrico.
- Cerrar las sesiones al término del trabajo.
- Propiciar las mejores condiciones ambientales para el uso de equipo.

Informe de seguimiento

Contenido

Cambios de alcance

Se ha mantenido el alcance del proyecto pero ha requerido mucho esfuerzo obtener la colaboración de los centros educativos

Riesgos materializados

- Calendario académico: los periodos de exámenes y las semanas previas dedicadas a la preparación de los mismos, han retrasado el proyecto.
- Distracciones culturales: el descubrimiento de las fallas restó varios días de trabajo.
- Bajas por enfermedad: una subluxación acromio-clavicular retrasó el trabajo por las fuertes molestias para articular el bazo durante un mes.
- Aparición de riesgos no detectados-sujetos a gestión o detectados y cuyas medidas corretoras no ha surtido efecto. P. e.: la escasa participación que se ha registrado hasta conseguir unos datos representativos.

Coste real

Se presupuestaron 280 horas y finalmente, a pesar de la dilatación de algunas tareas, se ha completado el proyecto con 267 horas. A pesar del desvío del proyecto y las dificultades, finalmente no se sale del presupuesto inicial. Económicamente se estimaba en 5.880,00€ (6.938,00€ con IVA), el coste real sería de 5.607,00€ (6.616,00€ con IVA)

Análisis de riesgos de los centros

Por cada activo se enumerarán las amenazas a las que está expuesto, el riesgo de materialización, el impacto y la relación entre ambos empleando una escala cualitativa. Sólo se analizarán las amenazas directamente relacionadas con el sistema de información; quedando fuera, por ejemplo, la seguridad perimetral.

- Aula informática:
    - Alumnos: se corre un alto riesgo de que el equipo sea desconfigurado, independientemente de la intención. En función de las contramedidas y permisos otorgados al alumno, el impacto puede oscilar entre nulo y total. Por tanto, la relación riesgo-impacto que, de forma orientativa, pondera la relevancia de la amenaza puede ser desde nulo hasta alto.
    - Malaware, virus…: el riesgo es medio-alto, y dependiendo del patógeno y las contramedidas, el impacto puede ser entre nulo y alto. De esta forma el riesgo ponderado queda entre bajo y alto.
    - Factores ambientales (polvo, humedad, temperatura…): riesgo muy alto, pero el impacto es muy bajo; luego el riesgo ponderado es bajo.
    - Sobretensión: debido a la calidad de las instalaciones actuales, este riesgo es prácticamente nulo, no así en las instalaciones antiguas. En caso de materialización de esta amenaza, el impacto sería medio pues seguramente el único componente afectado sería la fuente de alimentación.
    - Manipulación de Hardware / periféricos:
- Equipos informáticos de profesores:
    - Accesos no autorizados: hay un riesgo bajo de que se intente acceder a un ordenador sobre el que se tienen permisos. El impacto puede ser medio-alto. Luego el riesgo ponderado se evalúa como medio.
    - Malware, virus…: ídem que el activo anterior.
    - Factores ambientales: ídem que el activo anterior.
    - Sobre tensión: ídem que el activo anterior.
    - Usuarios que conculcan las políticas de seguridad: riesgo alto, impacto medio; riesgo ponderado, medio.
- Información almacenada:
    - Sustracción / revelación de secreto: el riesgo es alto pues este activo es el más valioso del sistema de información, su impacto es alto con fuertes implicaciones legales; el riesgo ponderado, por tanto, es alto.
    - Perdida: aunque el riesgo de que esto suceda es bajo, con un buen plan de copias de seguridad el impacto sería prácticamente nulo; luego, el riesgo ponderado será muy bajo. En el caso que nos ocupa, ITACA centraliza los datos en la Conselleria de

forma que esta es la responsable del plan de copias de seguridad.

- Usuarios:
    - Suplantación: independientemente de las motivaciones, se estima un riesgo medio de suplantación. Bien sea un usuario legítimo que desee realizar tareas para las que no tiene permiso, bien sea un tercero malintencionado. El impacto puede variar según las motivaciones de la suplantación entre medio y total si se suplanta al administrador. El riesgo ponderado es alto.
    - Ingeniería social: ligado a la amenaza anterior, la ingeniería social merece mención a aparte pues ataca al eslabón más débil, el usuario; mientras que realizar una suplantación utilizando medios exclusivamente técnicos puede ser más laborioso. El riesgo es medio, pero el empleo de estos recursos denota el interés en la cuenta administrador, luego su impacto es total. Riesgo ponderado, muy alto.
    - Legales: riesgo bajo, pues saltarse las políticas de seguridad no implica una acción ilegal, pero determinados usos de los datos del sistema o un tratamiento inadecuado pueden desembocar en los juzgados. El impacto es medio, pues la pena será administrativa no carcelaria. Riesgo ponderado bajo.

Listado de centros empleado como muestra

Nombre	e-mail	tipo	docencia	provincia
ESCUELA EUROPEA - DE ALICANTE	03016250@edu.gva.es	Público	Eso + Bachiller	Alicante
INSTITUTO DE EDUCACIÓN SECUNDARIA - EL PLA	03015543@edu.gva.es	Público	Eso + Bachiller	Alicante
INSTITUTO DE EDUCACIÓN SECUNDARIA - GRAN VÍA	03014861@edu.gva.es	Público	Eso + Bachiller	Alicante
INSTITUTO DE EDUCACIÓN SECUNDARIA - SERRA D'IRTA	12004394@edu.gva.es	Público	Eso + Bachiller	Castellón
INSTITUTO DE EDUCACIÓN SECUNDARIA - XIMÉN D'URREA	12004011@edu.gva.es	Público	Eso + Bachiller	Castellón
INSTITUTO DE EDUCACIÓN SECUNDARIA - VILA-ROJA	12005647@edu.gva.es	Público	Eso + Bachiller	Castellón
INSTITUTO DE EDUCACIÓN SECUNDARIA – ADEMUZ	46020248@edu.gva.es	Público	Eso + Bachiller	Valencia
INSTITUTO DE EDUCACIÓN SECUNDARIA - DOCTOR FAUSTÍ BARBERÁ	46000161@edu.gva.es	Público	Eso + Bachiller	Valencia
INSTITUTO DE EDUCACIÓN SECUNDARIA – ALBAL	46022831@edu.gva.es	Público	Eso + Bachiller	Valencia
CENTRO INTEGRADO PÚBLICO DE FORMACIÓN PROFESIONAL - MARÍTIMO PESQUERO DEL MEDITERRÁNEO	aracil_jos@gva.es	Público	FP	Alicante
INSTITUTO DE EDUCACIÓN SECUNDARIA - MIGUEL HERNÁNDEZ	03001891@edu.gva.es	Público	FP	Alicante
INSTITUTO DE EDUCACIÓN SECUNDARIA - VIRGEN DEL REMEDIO	03010119@edu.gva.es	Público	FP	Alicante
CENTRO INTEGRADO PÚBLICO DE FORMACIÓN PROFESIONAL – BENICARLÓ	csf_benicarlo@gva.es	Público	FP	Castellón
INSTITUTO DE EDUCACIÓN SECUNDARIA - JOAN COROMINES	12003390@edu.gva.es	Público	FP	Castellón
INSTITUTO DE EDUCACIÓN SECUNDARIA - RAMÓN CID	12000480@edu.gva.es	Público	FP	Castellón
INSTITUTO DE EDUCACIÓN SECUNDARIA – PORÇONS	46022099@edu.gva.es	Público	FP	Valencia
INSTITUTO DE EDUCACIÓN SECUNDARIA - CLARA CAMPOAMOR	46023225@edu.gva.es	Público	FP	Valencia
INSTITUTO DE EDUCACIÓN SECUNDARIA - JOSÉ SEGRELLES	46000213@edu.gva.es	Público	FP	Valencia
I.E.S. SAN VICENTE DE S.V.DEL RASPEIG	03015531@edu.gva.es	Público	Sec. Obligatoria	Alicante
INSTITUTO DE EDUCACIÓN SECUNDARIA - LAS LOMAS	03014460@edu.gva.es	Público	Sec. Obligatoria	Alicante
SECCIÓN DE EDUCACIÓN SECUNDARIA - I.E.S. PLAYA SAN JUAN	03015038@edu.gva.es	Público	Sec. Obligatoria	Alicante
SECCIÓN DE EDUCACIÓN SECUNDARIA - I.E.S. ALFONSO XIII (SECCIÓN DE BENASAL)	12005507@edu.gva.es	Público	Sec. Obligatoria	Castellón
CENTRO PÚBLICO INTEGRADO - EXCELENTÍSIMA DIPUTACIÓN	iespenyeta@dipcas.es	Público	Sec. Obligatoria	Castellón
INSTITUTO DE EDUCACIÓN SECUNDARIA - L'ALCALATÉN	12005659@edu.gva.es	Público	Sec. Obligatoria	Castellón
SECCIÓN DE EDUCACIÓN SECUNDARIA - I.E.S. SIVERA FONT DE CANALS	46024382@edu.gva.es	Público	Sec. Obligatoria	Valencia
SECCIÓN DE EDUCACIÓN SECUNDARIA - I.E.S. LA SERRANÍA (SECCIÓN DE ALPUENTE)	46022440@edu.gva.es	Público	Sec. Obligatoria	Valencia

INSTITUTO DE EDUCACIÓN SECUNDARIA - COMARCAL –BURJASSOT	46022865@edu.gva.es	Público	Sec. Obligatoria	Valencia
CENTRO DOCENTE PRIVADO EXTRANJERO - SIERRA BERNIA SCHOOL	duncan@ctv.es	Privado	Eso + Bachiller	Alicante
CENTRO DOCENTE PRIVADO EXTRANJERO - COSTA BLANCA INTERNATIONAL COLLEGE, SL	costablancacollege@hotmail.com	Privado	Eso + Bachiller	Alicante
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - LOPE DE VEGA	colegiointernacional@lopedevega.es	Privado	Eso + Bachiller	Alicante
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - SALESIANOS SAN JUAN BAUTISTA	burriana@salesianos.edu	Privado	Eso + Bachiller	Castellón
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - SEMINARI MENOR DIOCESÀ MATER DEI	recepcion@colegiomaterdei.org	Privado	Eso + Bachiller	Castellón
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - NUESTRA SEÑORA DE LA CONSOLACIÓN	colnsconsola@planalfa.es	Privado	Eso + Bachiller	Castellón
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - MADRE JOSEFA CAMPOS	mjcampos@planalfa.es	Privado	Eso + Bachiller	Valencia
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - PARROQUIAL DON JOSÉ LLUCH	info@col-legiparroquialdonjoselluch.es	Privado	Eso + Bachiller	Valencia
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - NUESTRA SEÑORA DEL SOCORRO	COLEGIO.SOCORRO@telefonica.net	Privado	Eso + Bachiller	Valencia
CENTRO PRIVADO FORMACIÓN PROFESIONAL ESPECÍFICA – GALERA	correo@peluquerosgalera.com	Privado	FP	Alicante
CENTRO PRIVADO FORMACIÓN PROFESIONAL ESPECÍFICA - CENTRO POLIVALENTE SOCIAL Y EDUCATIVO	secretaria.copsea@gmail.com	Privado	FP	Alicante
CENTRO PRIVADO FORMACIÓN PROFESIONAL ESPECÍFICA - ACADEMIA COTS	accots@cotsalicante.com	Privado	FP	Alicante
CENTRO PRIVADO FORMACIÓN PROFESIONAL ESPECÍFICA – CERVANTES	c.cervantesfp-almassora@ono.com	Privado	FP	Castellón
CENTRO PRIVADO DE EDUCACIÓN SECUNDARIA - IZQUIERDO-SOROLLA	informacion@centrosizquierdo.com	Privado	FP	Castellón
CENTRO PRIVADO FORMACIÓN PROFESIONAL ESPECÍFICA - F.P.FINA IZQUIERDO S.A.	informacion@centrosizquierdo.com	Privado	FP	Castellón
CENTRO PRIVADO FORMACIÓN PROFESIONAL ESPECÍFICA - FOLGUERA-VICENT	informacion@folgueravicent.com	Privado	FP	Valencia
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA – VAMAR	colegiovamar@hotmail.com	Privado	FP	Valencia
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - SAN ANTONIO DE PADUA	sanantonio@telefonica.net	Privado	FP	Valencia
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - EL VALLE	secre.ali@colegioelvalle.com	Privado	Sec. Obligatoria	Alicante
LICEO FRANCÉS	secretprov@e.lyceefrancaisalicante.com	Privado	Sec. Obligatoria	Alicante
BRITISH SCHOOL OF ALICANTE	info@bsalicante.com	Privado	Sec. Obligatoria	Alicante
CENTRO PRIVADO DE EDUCACIÓN SECUNDARIA - ALT MAESTRAT	maestrat@cdrtcampos.es	Privado	Sec. Obligatoria	Castellón
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - LA SALLE	alcora@lasallevp.es	Privado	Sec. Obligatoria	Castellón
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - PUÉRTOLAS PARDO	puertolaspardo@gmail.com	Privado	Sec. Obligatoria	Castellón
CENTRO PRIVADO DE EDUCACIÓN SECUNDARIA - MARE DE DÉU DE L'OLIVAR II	mdolivarii@planalfa.es	Privado	Sec. Obligatoria	Valencia
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - SANTA ANA Y SAN JOSÉ DE LA MONTAÑA	sasjm@planalfa.es	Privado	Sec. Obligatoria	Valencia
CENTRO PRIVADO E. INFANTIL, PRIMARIA Y SECUNDARIA - SANTA MARÍA-MARIANISTAS	santamariaa@planalfa.es	Privado	Sec. Obligatoria	Valencia

Cuestionario: Encuesta sobre sistemas de información escolares en la Comunidad Valenciana

A la atención del / de la responsable de TICs del centro: Le pedimos su colaboración para determinar las vulnerabilidades más comunes en sistemas de información escolares y, consecuentemente, proponer posibles soluciones. Este cuestionario es parte de un proyecto fin de carrera de la Universidad Politécnica de Valencia. Nótese, que el planteamiento de las preguntas está encaminado a sugerir mejoras. Rogamos máxima sinceridad pues el cuestionario es anónimo. Esperamos que le sea tan útil este cuestionario a usted y su centro, como a nosotros. Gracias por su colaboración

*Obligatorio

Educación impartida en el centro *

- ☐ Educación Secundaria Obligatoria
- ☐ Bachiller
- ☐ Formación Profesional

Carácter del centro *

- ○ Público
- ○ Privado-concertado
- ○ Privado

Emplea el sistema "ITACA" de la Conselleria d'educació

- ○ Si
- ○ No

1- ¿Se realizan copias de seguridad periódicas del sistema de información? Es obligatorio tener un plan de copias de seguridad y realizar las mismas semanalmente o cuando se modifican los datos

- ○ Si
- ○ No
- ○ NS/NC

2- ¿Se almacenan las copias de seguridad en un edificio diferente o servicio on-line especializado? Es obligatorio y recomendable conservar las copias de seguridad en otro edificio como medida de protección. (Ej: incendios)

- Si
- No
- NS/NC

3- ¿Se almacenan las copias de seguridad encriptadas/codificadas? Es obligatorio y recomendable conservar las copias de seguridad tan protegidas como sea posible, esto incluye la encriptación de los datos y el almacenaje en lugares de acceso restringido.

- Si
- No
- NS/NC

4- ¿Se verifica que se ha realizado correctamente la copia de seguridad? Es obligatorio y recomendable comprobar la legibilidad de la copias para saber que se podrán emplear para restaurar el sistema.

- Si
- No
- NS/NC

5- ¿Los soportes empleados para las copias de seguridad están debidamente inventariados? Realizar un inventario de los soportes evitando etiquetas alusivas al contenido (v.g.: "Expedientes servicio orientación"), es útil para controlar las copias y no dar facilidades ante posibles accesos no autorizados.

- Si
- No
- NS/NC

6- ¿Se almacenan las copias de seguridad bajo contraseña? Establecer una contraseña para la copia de seguridad sobre el soporte en el se hace. Ej: guardarla en ficheros 'zip', discos duros con particiones protegidas...

- Si
- No
- NS/NC

7- ¿Cada usuario (no alumnos) conoce sus funciones y obligaciones con respecto al tratamiento de datos de carácter personal? Redactar un epígrafe en el documento de seguridad que establezca los distintos roles, sus funciones y responsabilidades. Quien tiene acceso al sistema, para qué y cuáles son sus obligaciones.

- Si
- No
- NS/NC

8- ¿Existe un registro de incidencias del sistema? Establecer un registro de incidencias que contenga: tipo de incidencia, momento, persona que notifica, a quién notifica y los efectos derivados; de forma que quede constancia y sea posible solucionarlas.

- Si
- No
- NS/NC

9- ¿Se cambian periódicamente las contraseñas? Cambiar las contraseñas al menos semestralmente y no repetirlas.

- Si
- No
- NS/NC

10- ¿Las contraseñas empleadas contienen caracteres alfanuméricos, caracteres especiales y no incluyen palabras existentes en diccionarios, nombres o datos vinculados al usuario (v.g.: fechas)? Activar un control de contraseñas en la política de seguridad del dominio, si se emplea una gestión centralizada tipo LDAP o MS Active Directory. En otro caso, formar y sensibilizar a los usuarios del valor de la seguridad.

- Si
- No
- NS/NC

11- ¿Es habitual que los usuarios apunten sus contraseñas y dejen el papel accesible? Concienciar a los usuarios de la importancia de no dejar indicios de las contraseñas.

- Si
- No

- NS/NC

12- En los ordenadores en los que se realiza algún tratamiento de datos de carácter personal ¿Se emplea el protector de pantalla con contraseña para mantener la privacidad? Activar el protector de pantalla protegido por contraseña para evitar miradas indiscretas.

- Si
- No
- NS/NC

13- Antes de abandonar la mesa de trabajo ¿Se guardan debidamente todos los papeles que contienen datos de carácter personal? Seguir una política de "mesas limpias" y guardar debidamente, por ejemplo, los informes del orientador cuando no está en su mesa.

- Si
- No
- NS/NC

14- ¿Las cuentas de usuario de ex-empleados son desactivadas o eliminadas al finalizar la relación laboral? Desactivar, y tras un tiempo prudencial, eliminar dichas cuentas.

- Si
- No
- NS/NC

15- Cuando se remite documentación, en papel, que contiene datos de carácter personal ¿Se entrega en mano o correo certificado? Enviar los documentos por correo certificado, y si es posible, entregarlos en mano.

- Si
- No
- NS/NC

16- Cuando se remite documentación, en digital, que contiene datos de carácter personal ¿Se emplea una conexión segura ("VPN") o, alternativamente, se envían los datos cifrados? Emplear conexiones seguras como VPN o https para aplicaciones vía web.

- Si

- No
- NS/NC

17- ¿Existe una persona o personas con formación suficiente para administrar el sistema con soltura? Formar al administrador en las tecnologías empleadas en el centro para poder exprimir al máximo el sistema.

- Si
- No
- NS/NC

18- En el caso de documentos en papel que contenga datos especialmente protegidos ¿Están protegidos por una portada con la leyenda "Confidencial" y la lista de personas autorizadas? Disponer una portada que indique la confidencialidad de los datos y los nombres de aquellos que cuentan con permiso para acceder al documento.

- Si
- No
- NS/NC

19- ¿Existe alguna limitación al empleo de memorias USB para con los alumnos? Permitir únicamente el uso de memorias controladas por el centro; establecer el escaneo obligatorio con antivirus las memorias de los alumnos o emplear servicios de alojamiento en red pueden ser buenas estrategias.

- Si
- No
- NS/NC

20- ¿Existe alguna limitación al empleo de memorias USB en los ordenadores en los que residen datos de carácter personal? Inhibir este tipo de dispositivos en estas máquinas salvo usuarios con permisos elevados.

- Si
- No
- NS/NC

21- En caso de distribuir circulares u otros documentos por medio digital ¿Se plantea alguna

medida para evitar manipulaciones? Firmar digitalmente los documentos enviados evita manipulaciones y permite identificar al autor sin sombra de duda.

- Si
- No
- NS/NC

22- ¿Se toma en consideración alguna guía de buenas prácticas en la gestión de TICs (Tecnologías de Información y Comunicación) como la propuesta por la Conselleria d'educació, ISO 20000, ITIL v3,....? Tomar en consideración al menos la guía de buenas prácticas TIC de la Conselleria d'educació

- Si
- No
- NS/NC

23- ¿El software empleado es legítimo, se han comprado las licencias necesarias? Emplear software Open source, freeware o comprar licencias legítimas evitan problemas de desactualización y aplicaciones infectadas

- Si
- No
- NS/NC

24- ¿Se actualiza regularmente el software y sistema operativo? Revisar las actualizaciones disponibles semanalmente.

- Si
- No
- NS/NC

25- ¿Se escanean periódicamente los ordenadores en busca de malware (virus, troyanos, spyware...)? Escanear periódicamente el sistema con aplicaciones detectoras de malware (antivirus...)

- Si
- No
- NS/NC

26- ¿Se han limitado el empleo de cookies (pequeños ficheros de información que instalan las webs en el navegador) sólo a webs de confianza? Limitar las cookies a webs de confianza.

- Si
- No
- NS/NC

27- ¿El personal del centro está sensibilizado con la seguridad informática? Formar al personal poniendo en valor la seguridad informática, consecuencias del incumplimiento de las diferentes políticas y fundamentos de ofimática en general

- Si
- No
- NS/NC

28- ¿Se toma en consideración alguna guía de buenas prácticas en la gestión de la seguridad informática como la propuesta por la conselleria, ISO 27000,....? Tomar en consideración al menos la guía de buenas prácticas TIC de la Conselleria d'educació

- Si
- No
- NS/NC

29- ¿El plan de contingencia contempla los activos informáticos? Incluir en el plan de contingencia los activos informático vitales para la continuidad de las operaciones del centro.

- Si
- No
- NS/NC

30- ¿Los activos informáticos conservan su contraseña por defecto? Cambiar las contraseñas siguiendo la política al respecto, tenga en cuenta que existen web que recopilan las contraseñas por defecto de multitud de productos y fabricantes.

- Si
- No
- NS/NC

31- ¿Existe un dispositivo que filtre el tráfico ("Firewall") entre Internet y la red local? Establecer un firewall entre la red local e Internet

- Si
- No
- NS/NC

32- ¿Existe un dispositivo que filtre el tráfico ("Firewall") entre los ordenadores accesibles por los alumnos y el resto de la red local? Establecer un firewall entre la red local y las aulas informáticas para aislar los equipos a los que tienen acceso los alumnos y los que contienen información sensible

- Si
- No
- NS/NC

33- En caso de contar con servicios telemáticos en las máquinas del centro (web, plataformas de apoyo a la docencia, correo electrónico) ¿Existe una zona de seguridad intermedia ("DMZ") entre Internet y la red local para los servicios telemáticos del centro? Establecer una zona de seguridad media ("DMZ") para prestar servicios protegiendo la parte más interior de la red local

- Si
- No
- NS/NC

34- ¿Cada usuario (no alumnos) del sistema tiene su propia cuenta de trabajo en el dominio? Crear una cuenta por usuario, emplear soluciones como Ms Active directory o LDAP para simplificar la gestión y centralizar las cuentas en el dominio.

- Si
- No
- NS/NC

35- ¿Los usuarios carecen de privilegios administrativos sobre el sistema (no pueden cambiar la configuración)? Limitar el uso de privilegios administrativos, sólo el administrador debe tener poder para configurar las máquinas.

- Si

- No
- NS/NC

36- ¿La configuración de los ordenadores a los que tienen acceso los alumnos impide alteraciones en la misma (salvo necesidades especiales de alguna asignatura)? Emplear aplicaciones como DeepFreezer que impiden que los cambios se hagan efectivos.

- Si
- No
- NS/NC

37- ¿Existe alguna medida de seguridad que impida el acceso a personal del centro no autorizada al tratamiento de los datos? Guardar los ficheros en papel bajo llave. Para dicheros digitales, crear grupos de usuarios sin acceso a la aplicación de gestión (Establecer esta política de seguridad es posible con Active Directory, y un poco más complicado con LDAP).

- Si
- No
- NS/NC

38- ¿Los recursos compartidos en red tienen establecidos los permisos necesarios para impedir accesos no autorizados? Configurar permisos de acceso adecuadamente.

- Si
- No
- NS/NC

39- ¿Se controlan las condiciones de humedad y temperatura del entorno de los equipos informáticos? Instalar equipos de climatización en el entorno de trabajo

- Si
- No
- NS/NC

40- ¿Se controlan las posibles impurezas presentes en el aire (polvo, salinidad [en caso de estar junto al mar],...) presentes en el ambiente? Instalar equipos de climatización/filtrado en el entorno de trabajo

- Si
- No
- NS/NC

41- ¿Existen medidas físicas que impidan la manipulación de los ordenadores? Añadir cerraduras o candados a las cajas de los ordenadores e impedir el acceso a las conexiones de periféricos

- Si
- No
- NS/NC

42- ¿Hay instalado algún tipo de filtro de contenidos? Emplear aplicaciones de control parental.

- Si
- No
- NS/NC

43- ¿Los formularios de admisión y matriculación recogen la información exclusivamente necesaria para realizar estos procesos? Eliminar los items relativos a información innecesaria

- Si
- No
- NS/NC

44- ¿Los formularios de admisión y matriculación recaban el consentimiento de los progenitores / tutores para procesar los datos personales? Incluir una cláusula en el formulario para obtener el consentimiento de acuerdo al Art. 6 de la Ley orgánica de protección de datos de carácter personal 15/1999 de 13 diciembre (LOPD)

- Si
- No
- NS/NC

45- ¿Los formularios de admisión y matriculación informan sobre el titular del fichero de datos y la forma de ejercitar los derechos de anulación, rectificación, corrección y oposición? Incluir una cláusula informativa en el formulario de acuerdo al Art. 5.1 de la Ley orgánica de protección de datos de carácter personal 15/1999 de 13 diciembre (LOPD)

- Si
- No
- NS/NC

46- ¿Los formularios de admisión y documentación adjunta de alumnos excluidos es eliminada? Cancelar dichos datos

- Si
- No
- NS/NC

47- ¿Los formularios de matriculación y documentación adjunta se elimina al término del proceso de matriculación? Cancelar dichos datos

- Si
- No
- NS/NC

48- Al finalizar la etapa escolar del alumno en el centro ¿Se eliminan los datos del alumno (salvo información básica del expediente académico)? Expurgar el expediente académico

- Si
- No
- NS/NC

49- En caso de recopilarse dato médicos (Alergias alimentarias, sueño, discapacidades,…); al finalizar la etapa escolar del alumno en el centro ¿Se eliminan estos datos del alumno? Cancelar dichos datos

- Si
- No
- NS/NC

50- En caso de recopilarse dato por parte del servicio de orientación; al finalizar la etapa escolar del alumno en el centro ¿Se eliminan estos datos del alumno? Cancelar dichos datos

- Si

- No
- NS/NC

51- ¿El fichero de datos personales se encuentra inscrito en el registro de la Agencia Española de Protección de Datos? (En centros públicos este asunto es responsabilidad de la consellería) Registrar el fichero, si se es titular del mismo

- Si
- No
- NS/NC

52- ¿Se ha elaborado el preceptivo documento de seguridad? Elaborar el documento de seguridad, según los criterios de la Agencia Española de Protección de Datos

- Si
- No
- NS/NC

53- Para el tratamiento de datos especialmente protegidos (salud, religión, diversificación curricular,...) ¿Se cuenta con consentimiento expreso? Pedir consentimiento expreso.

- Si
- No
- NS/NC

54- La salida o entrada de datos de carácter personal del centro (que también se aplica a los exámenes) ¿Deja constancia en un registro a tal efecto? Establecer un registro de entrada / salida, se debe conservar 2 años

- Si
- No
- NS/NC

55- Para la destrucción de documentos en papel que contengan datos de carácter personal ¿Se emplean máquinas destructoras o un servicio externo de recogida (que emite el correspondiente certificado de destrucción)? Emplear una máquina destructora y que su existencia sea conocida por todo el personal a fin de que todo documento sea destruido en condiciones de seguridad

- Si
- No
- NS/NC

56- ¿Se realiza la preceptiva auditoría bienal externa o interna del sistema de información? Realizar una auditoría bienal bien sea interna bien sea externa

- Si
- No
- NS/NC

57- ¿El contrato del personal incluye una cláusula de confidencialidad con respecto a los datos de los alumnos? Incluir en los contratos una cláusula alusiva al deber de secreto, según el artículo 10 de la LOPD

- Si
- No
- NS/NC

58- En los casos que es necesaria una cesión de datos no amparada por defecto por la ley (prestación de servicios) ¿Se pide el permiso de cesión correspondiente? Pedir consentimiento expreso y emplear los datos en las condiciones establecidas en el Art. 12 de la LOPD

- Si
- No
- NS/NC

59- En el caso de cesiones internacionales (Ej...: intercambios) ¿Se obtiene el permiso de la AEPD? Pedir consentimiento expreso de los padres / tutores del alumno y el consentimiento de la AEPD y emplear los datos en las condiciones establecidas en el art. 12 de la LOPD

- Si
- No
- NS/NC

60- En caso de realizar una memoria fotográfica y publicarla en Internet (bien en la web del centro, bien en servicios externos) ¿Se pide permiso para ello? Pedir permiso expreso a los padres

/ tutores del alumno/a

- Si
- No
- NS/NC

Comentarios a la encuesta Si desea puntualizar algún aspecto de la encuesta, adelante, háganoslo saber. 

Con la tecnología de Google Docs Informar sobre abusos - Condiciones del servicio - Otros términos

Datos recabados

Han participado cuarenta y dos centros de los cincuenta y cuatro que conforman la muestra. Evidentemente, los datos recabados son insuficientes para extrapolar la situación de los centros escolares de la Comunitat; pero aún así, las vulnerabilidades de este centro recibirán respuesta.

Educación impartida en el centro *

- ☑ Educación Secundaria Obligatoria (18)
- ☑ Bachiller (6)
- ☐ Formación Profesional (18)

Carácter del centro *

- ○ Público (27)
- ◉ Privado-concertado (10)
- ○ Privado (5)

Emplea el sistema "ITACA" de la Conselleria d'educació

- ◉ Si (28)
- ○ No (14)

1- ¿Se realizan copias de seguridad periódicas del sistema de información? Es obligatorio tener un plan de copias de seguridad y realizar las mismas semanalmente o cuando se modifican los datos

- ◉ Si (34)
- ○ No (3)
- ○ NS/NC (5)

2- ¿Se almacenan las copias de seguridad en un edificio diferente o servicio on-line especializado? Es obligatorio y recomendable conservar las copias de seguridad en otro edificio como medida de protección. (Ej: incendios)

- ○ Si (9)
- ◉ No (28)
- ○ NS/NC (5)

3- ¿Se almacenan las copias de seguridad encriptadas/codificadas? Es obligatorio y recomendable conservar las copias de seguridad tan protegidas como sea posible, esto incluye la encriptación de los datos y el almacenaje en lugares de acceso restringido.

- Si (6)
- No (26)
- NS/NC (10)

4- ¿Se verifica que se ha realizado correctamente la copia de seguridad? Es obligatorio y recomendable comprobar la legibilidad de la copias para saber que se podrán emplear para restaurar el sistema.

- Si (21)
- No (11)
- NS/NC (10)

5- ¿Los soportes empleados para las copias de seguridad están debidamente inventariados? Realizar un inventario de los soportes evitando etiquetas alusivas al contenido (v.g.: "Expedientes servicio orientación"), es útil para controlar las copias y no dar facilidades ante posibles accesos no autorizados.

- Si (23)
- No (12)
- NS/NC (7)

6- ¿Se almacenan las copias de seguridad bajo contraseña? Establecer una contraseña para la copia de seguridad sobre el soporte en el que se hace. Ej: guardarla en ficheros 'zip', discos duros con particiones protegidas...

- Si (8)
- No (25)
- NS/NC (9)

7- ¿Cada usuario (no alumnos) conoce sus funciones y obligaciones con respecto al tratamiento de datos de carácter personal? Redactar un epígrafe en el documento de seguridad que establezca los distintos roles, sus funciones y responsabilidades. Quien tiene acceso al sistema, para qué y cuáles son sus obligaciones.

- Si (21)
- No (14)
- NS/NC (7)

8- ¿Existe un registro de incidencias del sistema? Establecer un registro de incidencias que contenga: tipo de incidencia, momento, persona que notifica, a quién notifica y los efectos derivados; de forma que quede constancia y sea posible solucionarlas.

- Si (18)
- No (16)
- NS/NC (8)

9- ¿Se cambian periódicamente las contraseñas? Cambiar las contraseñas al menos semestralmente y no repetirlas.

- Si (11)
- No (24)
- NS/NC (7)

10- ¿Las contraseñas empleadas contienen caracteres alfanuméricos, caracteres especiales y no incluyen palabras existentes en diccionarios, nombres o datos vinculados al usuario (v.g.: fechas)? Activar un control de contraseñas en las políticas de seguridad del dominio, si se emplea una gestión centralizada tipo LDAP o MS Active Directoy. En otro caso, formar y sensibilizar a los usuarios del valor de la seguridad.

- Si (18)
- No (16)
- NS/NC (8)

11- ¿Es habitual que los usuarios apunten sus contraseñas y dejen el papel accesible? Concienciar a los usuarios de la importancia de no dejar indicios de las contraseñas.

- Si (5)
- No (28)
- NS/NC (9)

12- En los ordenadores en los que se realiza algún tratamiento de datos de carácter personal ¿Se

emplea el protector de pantalla con contraseña para mantener la privacidad? Activar el protector de pantalla protegido por contraseña para evitar miradas indiscretas.

- ○ Si (13)
- ◉ No (25)
- ○ NS/NC (4)

13- Antes de abandonar la mesa de trabajo ¿Se guardan debidamente todos los papeles que contienen datos de carácter personal? Seguir una política de "mesas limpias" y guardar debidamente, por ejemplo, los informes del orientador cuando no está en su mesa.

- ◉ Si (22)
- ○ No (14)
- ○ NS/NC (6)

14- ¿Las cuentas de usuario de ex-empleados son desactivadas o eliminadas al finalizar la relación laboral? Desactivar, y tras un tiempo prudencial, eliminar dichas cuentas.

- ◉ Si (29)
- ○ No (3)
- ○ NS/NC (10)

15- Cuando se remite documentación, en papel, que contiene datos de carácter personal ¿Se entrega en mano o correo certificado? Enviar los documentos por correo certificado, y si es posible, entregarlos en mano.

- ◉ Si (26)
- ○ No (5)
- ○ NS/NC (11)

16- Cuando se remite documentación, en digital, que contiene datos de carácter personal ¿Se emplea una conexión segura ("VPN") o, alternativamente, se envían los datos cifrados? Emplear conexiones seguras como VPN o https para aplicaciones vía web.

- ○ Si (9)
- ◉ No (19)
- ○ NS/NC (14)

17- ¿Existe una persona o personas con formación suficiente para administrar el sistema con soltura? Formar al administrador en las tecnologías empleadas en el centro para poder exprimir al máximo el sistema.

- (•) Si (28)
- ( ) No (9)
- ( ) NS/NC (5)

18- En el caso de documentos en papel que contenga datos especialmente protegidos ¿Están protegidos por una portada con la leyenda "Confidencial" y la lista de personas autorizadas? Disponer una portada que indique la confidencialidad de los datos y los nombres de aquellos que cuentan con permiso para acceder al documento.

- ( ) Si (2)
- (•) No (24)
- ( ) NS/NC (16)

19- ¿Existe alguna limitación al empleo de memorias USB para con los alumnos? Permitir únicamente el uso de memorias controladas por el centro; establecer el escaneo obligatorio con antivirus las memorias de los alumnos o emplear servicios de alojamiento en red pueden ser buenas estrategias.

- (•) Si (16)
- ( ) No (20)
- ( ) NS/NC (6)

20- ¿Existe alguna limitación al empleo de memorias USB en los ordenadores en los que residen datos de carácter personal? Inhibir este tipo de dispositivos en estas máquinas salvo usuarios con permisos elevados.

- ( ) Si (18)
- (•) No (19)
- ( ) NS/NC (5)

21- En caso de distribuir circulares u otros documentos por medio digital ¿Se plantea alguna medida para evitar manipulaciones? Firmar digitalmente los documentos enviados evita manipulaciones y permite identificar al autor sin sombra de duda.

- ○ Si (13)
- ◉ No (21)
- ○ NS/NC (8)

22- ¿Se toma en consideración alguna guía de buenas prácticas en la gestión de TICs (Tecnologías de Información y Comunicación) como la propuesta por la Conselleria d'educació, ISO 20000, ITIL v3,....? Tomar en consideración al menos la guía de buenas prácticas TIC de la Conselleria d'educació

- ◉ Si (13)
- ○ No (2)
- ○ NS/NC (7)

23- ¿El software empleado es legítimo, se han comprado las licencias necesarias? Emplear software Open source, freeware o comprar licencias legítimas evitan problemas de desactualización y aplicaciones infectadas

- ◉ Si (27)
- ○ No (6)
- ○ NS/NC (9)

24- ¿Se actualiza regularmente el software y sistema operativo? Revisar las actualizaciones disponibles semanalmente.

- ○ Si (26)
- ◉ No (9)
- ○ NS/NC (7)

25- ¿Se escanean periódicamente los ordenadores en busca de malware (virus, troyanos, spyware...)? Escanear periódicamente el sistema con aplicaciones detectoras de malware (antivirus...)

- ◉ Si (31)
- ○ No (7)
- ○ NS/NC (4)

26- ¿Se han limitado el empleo de cookies (pequeños ficheros de información que instalan las

webs en el navegador) sólo a webs de confianza? Limitar las cookies a webs de confianza.

- ○ Si (18)
- ◉ No (17)
- ○ NS/NC (7)

27- ¿El personal del centro está sensibilizado con la seguridad informática? Formar al personal poniendo en valor la seguridad informática, consecuencias del incumplimiento de las diferentes políticas y fundamentos de ofimática en general

- ◉ Si (19)
- ○ No (14)
- ○ NS/NC (9)

28- ¿Se toma en consideración alguna guía de buenas prácticas en la gestión de la seguridad informática como la propuesta por la conselleria, ISO 27000,....? Tomar en consideración al menos la guía de buenas prácticas TIC de la Conselleria d'educació

- ◉ Si (14)
- ○ No (22)
- ○ NS/NC (6)

29- ¿El plan de contingencia contempla los activos informáticos? Incluir en el plan de contingencia los activos informático vitales para la continuidad de las operaciones del centro.

- ○ Si (8)
- ○ No (10)
- ◉ NS/NC (24)

30- ¿Los activos informáticos conservan su contraseña por defecto? Cambiar las contraseñas siguiendo la política al respecto, tenga en cuenta que existen web que recopilan las contraseñas por defecto de multitud de productos y fabricantes.

- ○ Si (7)
- ◉ No (18)
- ○ NS/NC (17)

31- ¿Existe un dispositivo que filtre el tráfico ("Firewall") entre Internet y la red local? Establecer un firewall entre la red local e Internet

- Si (31)
- No (5)
- NS/NC (6)

32- ¿Existe un dispositivo que filtre el tráfico ("Firewall") entre los ordenadores accesibles por los alumnos y el resto de la red local? Establecer un firewall entre la red local y las aulas informáticas para aislar los equipos a los que tienen acceso los alumnos y los que contienen información sensible

- Si (32)
- No (5)
- NS/NC (5)

33- En caso de contar con servicios telemáticos en las máquinas del centro (web, plataformas de apoyo a la docencia, correo electrónico) ¿Existe una zona de seguridad intermedia ("DMZ") entre Internet y la red local para los servicios telemáticos del centro? Establecer una zona de seguridad media ("DMZ") para prestar servicios protegiendo la parte más interior de la red local

- Si (5)
- No (15)
- NS/NC (22)

34- ¿Cada usuario (no alumnos) del sistema tiene su propia cuenta de trabajo en el dominio? Crear una cuenta por usuario, emplear soluciones como Ms Active directory o LDAP para simplificar la gestión y centralizar las cuentas en el dominio.

- Si (19)
- No (18)
- NS/NC (5)

35- ¿Los usuarios carecen de privilegios administrativos sobre el sistema (no pueden cambiar la configuración)? Limitar el uso de privilegios administrativos, sólo el administrador debe tener poder para configurar las máquinas.

- Si (36)
- No (2)

- NS/NC (4)

36- ¿La configuración de los ordenadores a los que tienen acceso los alumnos impide alteraciones en la misma (salvo necesidades especiales de alguna asignatura)? Emplear aplicaciones como DeepFreezer que impiden que los cambios se hagan efectivos.

- Si (35)
- No (2)
- NS/NC (5)

37- ¿Existe alguna medida de seguridad que impida el acceso a personal del centro no autorizada al tratamiento de los datos? Guardar los ficheros en papel bajo llave. Para dicheros digitales, crear grupos de usuarios sin acceso a la aplicación de gestión (Establecer esta política de seguridad es posible con Active Directory, y un poco más complicado con LDAP).

- Si (29)
- No (5)
- NS/NC (8)

38- ¿Los recursos compartidos en red tienen establecidos los permisos necesarios para impedir accesos no autorizados? Configurar permisos de acceso adecuadamente.

- Si (32)
- No (3)
- NS/NC (7)

39- ¿Se controlan las condiciones de humedad y temperatura del entorno de los equipos informáticos? Instalar equipos de climatización en el entorno de trabajo

- Si (8)
- No (28)
- NS/NC (6)

40- ¿Se controlan las posibles impurezas presentes en el aire (polvo, salinidad [en caso de estar junto al mar],...) presentes en el ambiente? Instalar equipos de climatización/filtrado en el entorno de trabajo

- Si (6)

- No (30)
- NS/NC (6)

41- ¿Existen medidas físicas que impidan la manipulación de los ordenadores? Añadir cerraduras o candados a las cajas de los ordenadores e impedir el acceso a las conexiones de periféricos

- Si (19)
- No (19)
- NS/NC (4)

42- ¿Hay instalado algún tipo de filtro de contenidos? Emplear aplicaciones de control parental.

- Si (27)
- No (10)
- NS/NC (5)

43- ¿Los formularios de admisión y matriculación recogen la información exclusivamente necesaria para realizar estos procesos? Eliminar los items relativos a información innecesaria

- Si (25)
- No (6)
- NS/NC (11)

44- ¿Los formularios de admisión y matriculación recaban el consentimiento de los progenitores / tutores para procesar los datos personales? Incluir una cláusula en el formulario para obtener el consentimiento de acuerdo al Art. 6 de la Ley orgánica de protección de datos de carácter personal 15/1999 de 13 diciembre (LOPD)

- Si (23)
- No (5)
- NS/NC (14)

45- ¿Los formularios de admisión y matriculación informan sobre el titular del fichero de datos y la forma de ejercitar los derechos de anulación, rectificación, corrección y oposición? Incluir una cláusula informativa en el formulario de acuerdo al Art. 5.1 de la Ley orgánica de protección de datos de carácter personal 15/1999 de 13 diciembre (LOPD)

- (•) Si (16)
- ( ) No (9)
- ( ) NS/NC (17)

46- ¿Los formularios de admisión y documentación adjunta de alumnos excluidos es eliminada? Cancelar dichos datos

- (•) Si (16)
- ( ) No (4)
- ( ) NS/NC (22)

47- ¿Los formularios de matriculación y documentación adjunta se elimina al término del proceso de matriculación? Cancelar dichos datos

- ( ) Si (12)
- ( ) No (11)
- (•) NS/NC (19)

48- Al finalizar la etapa escolar del alumno en el centro ¿Se eliminan los datos del alumno (salvo información básica del expediente académico)? Expurgar el expediente académico

- ( ) Si (17)
- (•) No (9)
- ( ) NS/NC (16)

49- En caso de recopilarse dato médicos (Alergias alimentarias, sueño, discapacidades,…); al finalizar la etapa escolar del alumno en el centro ¿Se eliminan estos datos del alumno? Cancelar dichos datos

- ( ) Si (14)
- ( ) No (6)
- (•) NS/NC (22)

50- En caso de recopilarse dato por parte del servicio de orientación; al finalizar la etapa escolar del alumno en el centro ¿Se eliminan estos datos del alumno? Cancelar dichos datos

- ( ) Si (12)

- ○ No (8)
- ◉ NS/NC (22)

51- ¿El fichero de datos personales se encuentra inscrito en el registro de la Agencia Española de Protección de Datos? (En centros públicos este asunto es responsabilidad de la consellería) Registrar el fichero, si se es titular del mismo

- ◉ Si (16)
- ○ No (4)
- ○ NS/NC (22)

52- ¿Se ha elaborado el preceptivo documento de seguridad? Elaborar el documento de seguridad, según los criterios de la Agencia Española de Protección de Datos

- ◉ Si (9)
- ○ No (12)
- ○ NS/NC (21)

53- Para el tratamiento de datos especialmente protegidos (salud, religión, diversificación curricular,...) ¿Se cuenta con consentimiento expreso? Pedir consentimiento expreso.

- ◉ Si (19)
- ○ No (7)
- ○ NS/NC (16)

54- La salida o entrada de datos de carácter personal del centro (que también se aplica a los exámenes) ¿Deja constancia en un registro a tal efecto? Establecer un registro de entrada / salida, se debe conservar 2 años

- ○ Si (12)
- ◉ No (17)
- ○ NS/NC (13)

55- Para la destrucción de documentos en papel que contengan datos de carácter personal ¿Se emplean máquinas destructoras o un servicio externo de recogida (que emite el correspondiente certificado de destrucción)? Emplear una máquina destructora y que su existencia sea conocida por todo el personal a fin de que todo documento sea destruido en condiciones de seguridad

- Si (27)
- No (7)
- NS/NC (8)

56- ¿Se realiza la preceptiva auditoría bienal externa o interna del sistema de información? Realizar una auditoría bienal bien sea interna bien sea externa

- Si (7)
- No (19)
- NS/NC (16)

57- ¿El contrato del personal incluye una cláusula de confidencialidad con respecto a los datos de los alumnos? Incluir en los contratos una cláusula alusiva al deber de secreto, según el artículo 10 de la LOPD

- Si (11)
- No (9)
- NS/NC (22)

58- En los casos que es necesaria una cesión de datos no amparada por defecto por la ley (prestación de servicios) ¿Se pide el permiso de cesión correspondiente? Pedir consentimiento expreso y emplear los datos en las condiciones establecidas en el Art. 12 de la LOPD

- Si (13)
- No (5)
- NS/NC (24)

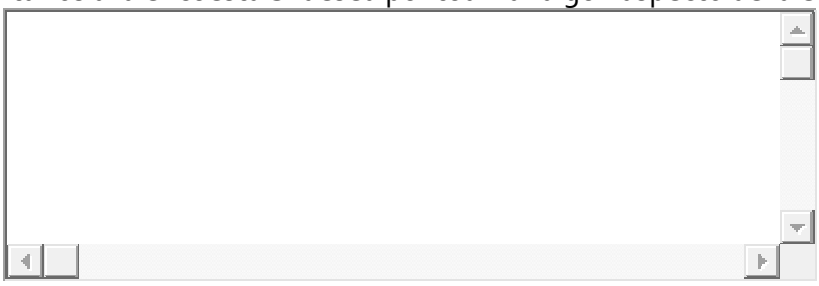
59- En el caso de cesiones internacionales (Ej...: intercambios) ¿Se obtiene el permiso de la AEPD? Pedir consentimiento expreso de los padres / tutores del alumno y el consentimiento de la AEPD y emplear los datos en las condiciones establecidas en el art. 12 de la LOPD

- Si (3)
- No (4)
- NS/NC (35)

60- En caso de realizar una memoria fotográfica y publicarla en Internet (bien en la web del centro, bien en servicios externos) ¿Se pide permiso para ello? Pedir permiso expreso a los padres

/ tutores del alumno/a

- Si (31)
- No (3)
- NS/NC (8)

Comentarios a la encuesta Si desea puntualizar algún aspecto de la encuesta, adelante, háganoslo saber. 

Análisis de datos

Sobre el bloque de preguntas referidas a copias de seguridad, todos los centros disponen de respaldo; si bien veintiocho de ellos tienen implantado el sistema de información ITACA, por lo que en estos casos es la Conselleria d'Educació la responsable de realizar el backup del sistema. Dado que doce centros realizan sus propias copias de seguridad, el interés en este apartado se centra sobre estos. En primer lugar, ninguno declara almacenar los respaldos fuera del edificio que aloja el sistema de información, por lo cual las copias están expuestas a amenazas propias del edificio, como incendios o inundaciones. Se recomienda que no siendo posible el almacenamiento de las copias en otro edificio propiedad del colegio, utilicen servicios on-line que custodien dichas copias en sus centros de datos; y sin perder de vista en ningún caso los requisitos exigidos por la legalidad vigente. Comprobar la integridad de las copias, encriptarlas, establecer contraseñas para el acceso al archivo e inventariarlas debidamente son algunos de esos requisitos sobre los se inquiere en el cuestionario. El resto de centros, los integrados en ITACA, confían en el cumplimento de los ítems planteados o no saben a cerca de ello.

Casi todos los centros encuestados declaran que el personal docente conoce sus funciones y obligaciones con respecto al tratamiento de datos de carácter personal.

En cuanto a la existencia de un registro de incidencias, la mitad dice no disponer del mismo; y otros ocho centros ignoran la existencia de un registro a tal efecto. En el primer caso se recomienda la creación del registro donde constará el tipo de incidencia, el momento de su producción, la persona que realiza la notificación, a quien se le notifica y los efectos que se hubieran producido derivados de la misma.

Veinticuatro centros de la muestra recabada no cambian periódicamente sus contraseñas. Es recomendable un cambio semestral de contraseñas. Adicionalmente, dieciséis de estos centros no emplea contraseñas seguras desoyendo normas básicas como emplear caracteres alfanuméricos, mayúsculas, minúsculas y símbolos; o no emplear datos personales.

La gran mayoría (28 de 42) de los centros niegan o no confirman que se apunten las contraseñas en *post-its* o notas fácilmente accesibles.

Sólo trece de los centros emplean el protector de pantalla protegido por contraseña en ordenadores capacitados para el tratamiento de datos de carácter personal, evitando injerencias no autorizadas. En el caso de papeles sensibles se cambian las tornas. Veintidós centros declaran guardarlos al dejar la mesa de trabajo y otros seis han elegido la opción *no sabe/no contesta*.

Mayoritariamente, se opta por desactivar las cuentas de trabajo de personal cesado. Tres centros reconocen no tener este hábito y diez ignoran esta información.

Once de los encuestados ignoran como se entrega la documentación en soporte papel,

probablemente porque no sea esa la función de la persona que realizó la encuesta. El resto de centros la entregan por un canal de confianza para este medio.

La mayoría de los centros no saben si las conexiones telemáticas con la Conselleria se realizan por canales seguros; o contestan negativamente y los nueve restantes confían en el canal. Al depender este aspecto de los canales telemáticos facilitados por la Conselleria, existe un desconocimiento entre los usuarios sobre la seguridad del mismo, otros la dan por supuesta.

Mayoritariamente los encuestados declaran tener un administrador con conocimientos insuficientes para manejarse con soltura en las tareas al mismo asignadas.

Sólo dos centros emplean portadas en informes o archivos que contengan datos especialmente protegidos (verbi gratia: informes médicos, informes del orientador...) con la leyenda "confidencial" y la lista de personas con derecho a acceder a dicha información.

Únicamente dieciséis centros tienen limitado el uso de memorias USB a los alumnos. En cuanto al personal del centro, dieciocho centros establecen limitación alguna para sus memorias USB estando el sistema expuesto a infecciones víricas o a la toma de datos sin previa autorización.

La mayoría (21/42) de los encuestados no se plantea ninguna medida para evitar manipulaciones en los posibles documentos digitales que ponga a disposición de su comunidad educativa. Este hecho puede deberse a que, probablemente, no utilicen medios digitales para difundir circulares o documentos de similar naturaleza.

La mitad de los encuestados no toma en consideración ninguna guía de buenas prácticas en torno a la gestión de activos informáticos, a los que se unen siete centros que no saben/no contestan este ítem.

Veintisiete elementos de la muestra recogida emplea software debidamente licenciado, y todos ellos salvo uno lo actualiza regularmente. Esto puede desembocar en la persistencia de vulnerabilidades en el software y posibilitar vectores de ataque por ser bien conocidas. Se entiende como más crítico el escaneo regular del sistema en busca de patógenos, dos tercios de los centros así lo hacen.

Los navegadores de diecisiete centros no tienen limitado el almacenamiento de cookies lo que posibilita que cualquier web compile información en torno al usuario, o almacene código ejecutable de aviesas intenciones.

Catorce centros declaran una falta de concienciación del personal sobre la seguridad informática. En estos casos la probabilidad de que un usuario despreocupado desencadene la materialización de alguna amenaza aumenta. El factor humano es el principal problema de seguridad en estos

casos.

Uno de cada dos centros no toma en consideración ninguna guía de buenas prácticas para la gestión de la seguridad del sistema informático, a pesar de que sería beneficioso para los mismos pues serían más conscientes de las amenazas y conocería posibles soluciones.

En la mayoría de los casos se ignora si los activos informáticos están contemplados en el plan de contingencia, o puede ser que ni exista ese plan. Diez centros directamente dan una respuesta negativa. Todo esto, a pesar de lo recomendable que parece a primera vista tener un plan en caso de un impacto medio-grave sobre el sistema.

Siete centros mantienen las contraseñas por defecto de sus activos, y otros diecisiete no lo saben. Todo ello a pesar de que conociendo la marca y modelo del producto sea muy fácil encontrar su contraseña por defecto en la red de redes.

Cinco centros están faltos de *firewall* entre Internet y la red local; con el peligro que esto conlleva. Adicionalmente, tres cuartos de los encuestados dispone de un *firewall* adicional para aislar la parte de la red local accesible al alumnado y la parte de la red local que da soporte al personal docente y administrativo, parte en la cual se realiza el tratamiento de los datos de carácter persona.

Se desconoce, en veintidós de los casos, si la topología de la red dispone de una zona de seguridad media (DMZ) que proteja los servidores que están disponibles desde internet. Para el resto, salvo cinco, de cetros se sabe que no existe dicha zona. Si el centro no cuenta con su propio servidor de correo electrónico, o una plataforma de apoyo a la docencia (Moodle, Joomla!,...), u otros servicios web; la implementación de una zona de seguridad media carece de sentido.

Dos tercios de los centros no emplean cuenta de trabajo personales para sus usuarios, usando una cuenta común, cuestión que complica la administración de privilegios ajustada a cada perfil de usuario. Aunque todos coinciden en señalar que los privilegios administrativos se hayan reservados al administrador. En cualquier caso, en caso de incidencias graves no se puede trazar y determinar quienes han sido responsables de las mismas.

En el caso de los alumnos la inmensa mayoría, once encuestados, afirma tener una configuración adecuada para impedir la reconfiguración de los equipos por parte de este colectivo.

Casi la mitad de centros tienen una cuanta de trabajo por usuario, mientras que otra porción similar emplea cuantas compartida. En cualquier caso, sólo en dos centros los usuarios tienen privilegios administrativos.

Cinco de los colaboradores reconocen no tener ninguna medida que impida el acceso al

tratamiento de los datos bien sean esto digitales o en soporte papel; este punto puede tener graves implicaciones si no se pude limitar el acceso a los usuario legítimos y, como se ha dicho anteriormente, la trazabilidad del sistema no es posible; factor que juega a favor del malhechor.

Un cuarto de los centros no sabe si sus recursos compartidos en red están correctamente configurados para evitar abusos sobre los mismos.

Aproximadamente un cuarto de la muestra controla las condiciones de temperatura y humedad de las instalaciones que acogen los equipos informáticos, pero son sólo seis los que controlan las impurezas del aire o el polvo acumulado en el interior de las cajas del equipamiento. Curiosamente, si se instala un sistema de climatización para controlar los primeros aspectos, también se soluciona este último pues el aire de la habitación es filtrado. Las impurezas del aire que pueden incidir en rendimiento de la máquina. Un ordenador con polvo en su interior se calentará más; y si en el aire existen partículas de salitre, los circuitos pueden llegar a verse comprometidos por la herrumbre.

Diecinueve centros no disponen de medidas que impidan la manipulación física de los equipos, dejando a merced de cualquiera la alteración de la configuración hardware.

Cinco centros no saben si dispone de filtro de contenidos. Filtro que garantiza, en la medida de sus posibilidades, el uso de los equipos para fines legítimos. Diez, directamente, niegan su empleo.

En general, se considera que en los procesos de admisión y matriculación la información exigida no es excesiva, y que se realiza de manera conforme a Ley Orgánica de Protección de Datos de carácter personal 15/1999 de 13 de diciembre.

En cuanto a la cancelación los datos tras su proceso para el fin que habían sido recabados, se ignora si existe una política de cancelación de datos personales.

La mitad de los centros ignora si su fichero automatizado se haya inscrito ante la Agencia Española de Protección de Datos, En el caso de haber de desplegado ITACA será responsabilidad de la Conselleria.

Un cuarto de los encuestados dispone del documento de seguridad, mientras que el resto desconoce o niega su existencia.

Dieciséis de los Cuarentaidós centros no sabe si tienen el consentimiento para tratar datos especialmente protegidos.

El preceptivo registro de entrada/salida de soportes que contenga información personal, no se

emplea en diecisiete de los centros. Luego no hay trazabilidad para determinar responsabilidades sobre tratamientos fraudulentos o negligentes de la información.

Tres cuartos de la muestra realiza la auditoría bienal obligatoria sobre el tratamiento de datos de carácter personal, siempre recomendable para detectar áreas de mejora.

Poco más de un cuarto de los centros incluyen una clausula de confidencialidad con respecto a los datos del alumnado, mientras que se desconoce o niega la existencia en los casos restantes.

En los casos que para el funcionamiento del centro se requiere autorizaciones adicionales, bien sea para la prestación de servicios por terceros, bien sea por otras cesiones; se ignora si se pide permiso expreso en la mayoría de los casos. Algunos encuestado no saben si se realiza. Y se da el caso de tres centros que admiten abiertamente que no han recabado consentimiento para realizar una memoria fotográfica del alumnado.

Comentarios recabados:

- Si només hagués Lliurex als ordinadors, hi haurien molts menys problemes amb els sistemes informàtics, seguretat, etc

- Esta encuesta dirigida a centros públicos está totalmente desenfocada...las preguntas deberían ser ¿Vde. como profesor cuenta con un ordenador donde realizar su trabajo o se tiene que ir a utilizar el de su casa? ¿en caso de tenerlo, funciona correctamente? ¿Cuando tiene algun problema con el mismo existe alguien a quien pueda recurrir que se lo arregle? ¿Cuenta con acceso a internet? ¿cuantas veces se cae el acceso a la hora? ...

- Debería ser la conselleria la que se encargara de la mayoría de estas cosas. Pienso que debe ser ella la que debe dictar la mayoría de las instrucciones y normas a seguir y pienso que no siempre lo hace.

- No contestaré més preguntes si l'enquesta no està en valencià, perquè sembla mentida que encara es faça tot en castellà !!

- El dia que feu l'enquesta en valencià la contestaré.

- La ley es una cosa, la realidad otra. No hay recursos para tanta ley. Si se me ocurre pedir una sala especial para los servidores se van a reir de mi desde Valencia hasta la China ... Además la GVA va haciendo cosas, pero no necesariamente con un plan a largo plazo, lo que crea confusión y desánimo.

  Un saludo y buena suerte con el estudio.
  Ah, y no te deprimas con los resultados ;)

- Muchas respuestas las desconozco, pues son tareas que en principio, corresponden a otros empleados: administrativos, secretarios, equipo directivo ... e incluso la misma Consellería

- Existen determinados conceptos que no manejan (AEDP etc.)

- En aquest centre, com en molts altres, no comptem amb cap Coordinador TIC. Les tasques que s'esmenten en el qüestionari que no es realitzen, és a causa de la falta d'informació i de personal especialitzat. Tot i això, hem intentat contestar el número màxim de preguntes.

Patrones detectados

Variable de agrupación: modelo administrativo

Como podrá comprobarse en los epígrafes continuos, todos los *clústeres* formados por esta variable de agrupación adolecen de seguridad, salvo pequeñas desviaciones, en los mismos ítems del estudio. El patrón común describe, por un lado, la necesidad de una política de tratamiento de datos más férrea; y por otro, pequeñas configuraciones de medidas técnicas. Sí que es cierto que el clúster "privado" tiene algunas incidencias menos en los ítems del cuestionario, pero en cuestiones más influenciadas por la concienciación que por la propia relevancia del ítem.

Centros públicos (27/42):

Nueve de los centros no cuentan con ITACA lo cual repercute en los ítems sobre copias de seguridad. Este hecho no resulta significativo con respecto al resto de centros públicos, por tanto no es significativo en este patrón.

En doce centros se admite que no está claro el rol de cada usuario en el tratamiento de datos personales, y otros seis no saben-no contestan.

Trece participantes carecen de registro de incidencias contra los ocho que si lo implementan.

Dieciocho centros admiten no cambiar periódicamente las contraseñas y trece que no emplean contraseñas seguras.

Sólo cinco de los veintisiete centros emplean el protector de pantalla protegida por contraseña, por lo tanto, en el caso de los restantes no se protege la información mostrada en las pantallas cuando se abandona el puesto de trabajo; quedando así al alcance de cualquier curioso.

Sólo aproximadamente la mitad de la muestra sigue una política de "mesas limpias" cuando deja su mesa; contra nueve que dicen no seguir esa directiva.

Uno de los centros emplea portadas con la leyenda "confidencial" en documentos que contengan datos de especialmente protegidos ni una lista con las personas que tienen acceso a ese documento.

Nueve de los centros tiene limitación en el uso de memorias USB por parte del personal administrativo y docente, lo que supone una falta de control sobre la entrada y salida de datos personales. Uno menos, limita el uso de memorias USB al alumnado.

Dieciséis centros no establecen ninguna media para impedir la manipulación de la información transmitida por vía telemática.

Sólo ocho toman en consideración guías de buenas prácticas para la gestión del sistema de información.

Trece centros, no percibe la necesidad de configurar las cookies de los navegadores de forma que sólo se permitan para sitios web de confianza.

Sólo en nueve centros se reconoce la concienciación del personal para con la seguridad informática.

Nueve centros consideran alguna guía de buenas prácticas para la gestión de la seguridad informática.

Solamente en cuatro de los casos se sabe si los activos informáticos están contemplados en el plan de contingencia, en contra posición del resto que contestan negativamente a ítem o ignoran dicho plan. Puede ser que en exista dicho plan o que exista bajo otro nombre y no haya comprendido la cuestión.

Únicamente uno de los centros declara tener una zona de seguridad medida (DMZ), esto puede deberse a que los demás no ofrecen servicios telemáticos a su comunidad educativa.

En el caso de trece de los centros el personal no cuenta con una cuenta de trabajo propia, comprometiendo así la privacidad de los datos de cada usuario y complicando la búsqueda de responsabilidades al ser muy complicada la trazabilidad de las incidencias.

Sólo dos de los centros controlan las condiciones ambientales en las que se haya la sala donde están instalados los equipos informáticos; de igual modo, en el caso de control de partículas en el aire.

Catorce de los encuestados no han dispuesto medidas físicas para evitar la manipulación física de los equipos, estando estos expuestos a la alteración de la configuración por parte de cualquier persona.

Siete centros reconocen que sus impresos no informan sobre los derechos de Anulación,

Rectificación, Cancelación y Oposición. Otros siete dicen informar y trece no saben.

La mayoría de centros ignoran la política de cancelación de datos personales y datos personales especialmente protegidos, en la actualidad eso depende de ITACA pero en el caso de expedientes más antiguos previos a la centralización era responsabilidad de centros la cancelación de esos datos; por tanto, pueden hallarse en situación comprometida los expedientes más antiguos.

Únicamente un centro declara contar con el preceptivo documento de seguridad.

La mitad de la muestra ignora si se recaba el consentimiento para el tratamiento de datos especialmente protegidos.

Únicamente en siete centros se ha implementado el obligado registro de entrada/salida.

Ninguno de los centros realiza o sabe si se realiza la auditoría bienal sobre las medidas de seguridad del sistema de información dispuesto para el tratamiento de datos personales.

La respuesta es mayoritaria en cuanto a la ignorancia sobre una cláusula en los contratos del personal que obligue a la confidencialidad de los datos del alumno lado. Así como en el caso de cesiones a terceros en territorio nacional o internacional.

Centros privados/privados-concertados (15/42):

Existen siete centros que si cambian las contraseñas frete a seis centros en los que no se cambian con la periodicidad necesaria las contraseñas; esta medida evita la continua violación del sistema por contraseñas comprometidas aún en el caso de no tener constancia de esta incidencia por parte del administrador. Este mismo centro, declarando seguir las recomendaciones generales para crear contraseñas seguras.

Casi la mitad de los centros de este *clúster* no emplean el protector de pantalla protegido con contraseña para mantener la privacidad del contenido de sus equipos. En cambio es mayoritaria, en el caso de papeles sobre la mesa, una política de "mesas limpias" para cuando se abandona el puesto de trabajo.

Un centro emplea portadas en documentos que contienen datos especialmente protegidos con la advertencia "confidencial" y la lista del personal autorizado para su manejo.

En la mitad de casos se limita la conectividad de memorias USB al personal, siendo ésta una cuestión pendiente de solventar para un tercio de los centros privados; ya que esta falta de

control sobre las entradas y salidas de los datos personales puede derivar en una fuga de datos accidental o intencionada.

La mitad de centros medidas encaminadas a evitar la manipulación de documentos digitales contra un tercio que no lo hacen.

Invirtiendo la proporción anterior, cinco centros toman en consideración alguna guía de buenas prácticas relativa a la gestión de sistemas informáticos, frente a ocho que no lo hacen.

En casi la mitad los centros tampoco se tienen en consideración alguna guía de buenas prácticas en torno a seguridad informática.

Sólo un tercio de la muestra contempla los activos informáticos en un plan de contingencia, mientras que casi todo el resto ignora este punto.

En casi la mitad de centros los activos informáticos conservan su contraseña por defecto.

En algo menos de un tercios de los centros se sabe si tiene configurada una zona de seguridad intermedia (DMZ), aunque tampoco se sabe si realmente necesaria porque la encuesta no recabar la información relativa a los medios telemáticos de los que dispone el centro para apoyar la docencia.

La mitad de la muestra no dispone de cuentas personales de trabajo para el personal docente y administrativo, usando un perfil común para todos ellos con los riesgos que esto entraña; como ya se ha comentado anteriormente.

En a pesar de que seis de los quince centros controlan la calidad del aire de las salas las que están instalados los equipos; sólo cuatro, controla, además, de humedad y temperatura las impurezas del aire.

Casi la mitad declara carecer de documento de seguridad o ignorar si existe.

Un tercio de los centros cuenta con un registro de entrada salida de datos, superado en un centro los que no implementan dicho registro. Cuatro de los quince, no saben si tienen registro o no.

Casi la mitad realizan la auditoria bienal obligatoria, mientras que seis centros no saben si realizan dichas auditorías.

En cuanto a las posibles transferencias a terceros internacionales no sabe si se comunican a la

Agencia Española de Protección de Datos. Mientras que en transferencias a tercero nacionales casi la mitad reconoce no recabar dicho permiso.

Variable de agrupación: tamaño del sistema

Del mismo modo que ha ocurrido con la otra variable de agregación, tampoco el tamaño del sistema se revela como factor significativo para la seguridad de los centros pues todos los *clústeres*muestran vulnerabilidades comunes en su casi totalidad, ligeramente menores en el grupo "Formación profesional"

Sólo Educación Secundaria Obligatoria (18/42):

Casi todos los centros tienen ITACA implantado, por tanto, las cuestiones relativas a copias de seguridad pierden su relevancia.

Más de la mitad de los centros o no saben, o directamente declaran que los usuarios no saben cual es concretamente su rol en el tratamiento de datos.

Sólo cinco centros cuentan con un registro de incidencias.

Algo más de la mitad de los centros no cambia periódicamente las contraseñas, y sólo siete centros observan políticas sobre contraseñas seguras.

Dos tercios de los centros no usa o no sabe si se usa, puede que porque sea elección del usuario y no una política establecida, el protector de pantalla protegido por contraseña. Del mismo modo, tampoco implementas una política de mesas limpias despreocupándose de los documentos que se hallan sobre sus espacios de trabajo.

Los documentos que contienen datos personales especialmente protegidos, no se resguardan en ningún caso empleando una portada con leyenda "confidencial" y el listado de personal autorizado.

Mientras que tres de los centros limitan la conectividad de memorias USB al alumnado, seis hace lo propio con el personal docente y administrativo.

Para la difusión de documentos digitales tipo circular, en caso de realizarse tal difusión, no se toma medida alguna para preservar la integridad salvo en cinco casos.

Catorce de los dieciocho centros dicen no tener en cuenta, o no saben / no contestan, una guía de buenas prácticas para la gestión de activos informáticos. También sucede en el caso de guías de buenas prácticas en la gestión de la seguridad informática.

Únicamente cuatro centros limitan las cookies en sus navegadores. La cifra desciende en una unidad si hablamos de plantillas sensibilizadas con la seguridad informática.

Un centro tiene noticias sobre la vigencia de algún plan de contingencia que contemple los activos informáticos. Y la mitad tampoco sabe si los activos conservan su contraseña por defecto.

En dos casos se afirma que existe zona *desmilitarizada* (DMZ) mientras que el resto no disponen, no saben si existe, o no conocen el concepto.

Más de la mitad de los centros no disponen de cuentas personales para los empleados, usando estos cuentas conjuntas.

Dos tercios no controlan la humedad y temperatura en el entorno, y se incrementa en uno si hablamos de controlar las impurezas del aire. Poco más de la mitad también se declara no disponer de medio para impedir la manipulación física de la máquina.

La mitad de los centros tienen dudas respecto a los procesos de cancelación de datos.

La mitad de los encuestados desconocen si se dispone de un documento de seguridad; más un cuarto que afirma no tenerlo. En el caso del registro de entrada salida se repita la historia.

Tres centros si realizan auditorias bienales, tal como obliga el reglamento devenido de la LOPD.

Nueve declaran no saber si los contratos de personal contienen una clausula de confidencialidad; y cuatro lo niegan.

Casi un tercio afirma recabar el consentimiento de los interesados cuando se trata de ceder datos a terceros no previstos en la ley.

Cinco sextos no saben si se obtienen el permiso de la Agencia Española de Protección de Datos para realizar transferencias internacionales, como pueden ser intercambios.

Formación Profesional o Secundaria con Formación Profesional (18/42)

Dos tercios cuentan con ITACA.

Los respaldos en ninguno de los dos casos se almacenan encriptados ni edificios diferentes, pero uno si los guarda bajo contraseña y debidamente inventariados.

Casi en la mitad de los centros los usuarios desconocen su rol con respecto al tratamiento de datos personales.

Casi la mitad carece de registro de incidencias.

Sólo cinco centros cambian periódicamente las contraseñas, pero en ocho centros se observan las recomendaciones generales para formar buenas contraseñas

En catorce centros también adolecen del uso del protector de pantalla con contraseña.

Ninguno de los centros resguarda los documentos con datos especialmente protegidos con una portada con la marca "confidencial" y un listado de usuarios autorizados.

La mitad de los centros limita la conectividad de memorias USB a su alumnado y al personal.

En el caso de dos tercios de la muestra no se contempla medidas para evitar la alteración de documentos digitales difundidos a su comunidad educativa.

Un tercio toman en consideración guías de buenas prácticas en lo relativo a seguridad informática, del mismo modo en gestión de recursos informáticos.

El plan de contingencia en relación a activos informáticos es desconocido para más de dos tercios.

DMZ, cinco sextos o no saben/contestan, o dice no tener; pero como se ha dicho en varias ocasiones, si no prestan servicios fuera de su red local es prescindible.

En la mitad de los centros el personal cuenta con cuentas de trabajo personales.

Tres centros controlan humedad y temperatura del entorno en el que se hallan los equipos, y cuatro vigilan la calidad del aire.

Existe una ignorancia mayoritaria sobre la política de cancelación de datos.

Tres centros han realizado el documento de seguridad correspondiente, lo que supone una sexta parte del total.

Menos de la mitad de los centros cuentan con el consentimiento para tratar datos personales

especialmente protegidos.

Sólo un tercio de los casos cuentan con registro de entrada/salida.

Salvo dos centros el resto ignoran, o no quieren decir, si se cumple con las auditorías bienales.

Casi un tercio pide permiso para la cesión a terceros de datos personales para prestaciones de servicios no establecidos en los limitadores legales. Por el contrario, para cesiones internacionales, en ningún caso se cumple con el trámite de pedir permiso a la AEPD.

Educación Secundaria Obligatoria y Bachiller (6/42)

La mitad de centros ya han implantado ITACA.

Tres de los seis centros disponen de registro de incidencias, cambian periódicamente las contraseñas, y emplean contraseñas seguras.

Tres centros no emplean el protector de pantalla con contraseña, mientras otros tres sí que lo hacen.

Cuatro de los centros no emplean la carátula "confidencial" para documentos con datos especialmente protegidos descrita con anterioridad. El quinto no sabe/contesta al respecto.

La mitad de centros dan vía libre al uso de memorias USB a sus alumnos, empleados, y los riesgos que esta postura conlleva.

Dos tercios coinciden en señalar su desidia por proteger la integridad de los documentos de carácter informativo que puedan distribuir.

Únicamente la mitad toma en consideración guías de buenas prácticas en la gestión de recursos informáticos, y gestión de su seguridad.

Sólo dos de los centros realizan habitualmente labores de actualización del software y el sistema operativo. Y son estos mismos centros los que limitan el uso de cookies a web de confianza.

Tres de los centros no saben/contestan a cerca de la situación de los activos informáticos en el plan de contingencia, y un cuarto contesta negativamente.

Exclusivamente en un centro aseguran que los activos informáticos no mantienen la contraseña *as default*.

Tampoco en este caso los centros disponen de zona de seguridad media, pero tampoco se sabe si es necesaria.

Tres no facilitan cuantas de trabajo personales al personal; mientras otras tres sí que lo hacen.

Tres centros controlan las condiciones ambientales de temperatura y humedad, sólo uno la calidad del aire.

Existen dudas variadas sobre los procesos de admisión, matriculación y cancelación de datos; especialmente en este último. También existen dudas en tres centros sobre si se obtiene consentimiento para tratar datos especialmente protegidos.

Solo dos centros disponen de documento de seguridad.

Exclusivamente dos centros cuentan con registro de entrada/salida de datos personales.

Tres centros no saben si se realizan las auditorías bienales obligatorias, los mismos centros que ignoran si los contratos del personal cuentan con una cláusula de confidencialidad.

Tres centros piden permiso para la cesión de datos a terceros para la prestación de algún servicio, pero sólo uno lo hace en caso de cesiones internacionales.

Posibles soluciones

A tomar en consideración que la Conselleria d'educació es la responsable de las copias de seguridad de ITACA, no tiene sentido recomendar unas directrices para desarrollar un plan de copias en el centro, salvo en aquellos casos que no hayan desplegado ITACA hasta el momento. Para este último caso la mejor opción resulta contratar los servicios de una empresa dedica a las copias de seguridad, así se asegurarán de cumplir con todos los requisitos que marca el reglamento que desarrolla la LOPD

A la hora de configurar la contraseña del protector de pantalla hay que tener en cuenta las recomendaciones generales sobre contraseñas

- Longitud mínima de ocho caracteres.
- Emplear alfanuméricos en mayúsculas y minúsculas, y símbolos.
- No usar datos personales, series o palabras de diccionario.
- No apuntar la contraseña en un lugar inseguro, mejor si no se apunta.

Emplear conexiones seguras para conseguir la confidencialidad requerida. Soluciones como VPN o https son suficientes. Adicionalmente empleando técnicas basadas en firma digital, es posible enviar archivos encriptados por canales no seguros.

Para informes que contenga información sensible de los alumnos, emplear subcarpetas o portadas con la leyenda "confidencial" y la lista de personas autorizada a acceder al informe, de este modo se disuade a los primeros curiosos.

Mediante un Objeto de Política de grupo (GPO) se puede limitar el uso de memorias USB en el dominio. El GPO se aplica sobre unidades organizativa que incluyen equipos y grupos de usuarios. Un GPO puede implementar múltiples políticas. Para este problema en concreto se han desarrollado algunas aplicaciones como DeviceLock de Smartline, DeviceShield de Layton Technology o DeviceWall de Centennial. También a través de un GPO se puede configurar el uso del protector de pantalla con contraseña.

Para emplear firma digital, el centro primero deberá tramitarla en la autoridad de certificación correspondiente. Firmar documento no tiene mayor misterio, a día de hoy los procesadores de texto como MsWord y OpenOffice Wraiter permiten generar la firma fácilmente. Si se desea firmar un pdf, INTECO dispone de una pequeña aplicación que firma y verifica la firma de documentos. Hay que tener en cuenta que un documento digitalmente firmado no puedes ser modificado sin detectarse el engaño.

La actualización del sistema operativo para eliminar bugs es esencial, pues de otro modo perviven las vulnerabilidades del sistema. Por otra parte, la actualización es una operación de mantenimiento sencilla de realizar; salvo complicaciones aportadas por el parche.

Se recomienda restringir las cookies a las webs de confianza de modo que podamos saber cuál es la finalidad del archivo en cuestión. Desde *Panel de control / opciones de internet* se puede realizar el ajuste. En caso de implantar un dominio con Ms Active Directory, esta directiva puede plasmarse en un GPO

En todo centro debería desarrollarse un plan de contingencia que asegure poder continuar las operaciones a pesar de la pérdida parcial o total del sistema de información. Teniendo en cuenta que ITACA centraliza los datos, para continuar con el tratamiento de datos personales sólo requeriría una conexión a Internet y un ordenador con los requisitos mínimos para ejecutar ITACA.

En caso de que el centro preste algún servicio a través de Internet, como correo web o Moodle; contar con una zona de seguridad intermedia es esencial para no comprometer el núcleo de equipos más sensibles, como puede ser el del servicio de orientación.

Incluir una clausula de confidencialidad es preceptivo según el reglamento de desarrollo de la LOPD.

Formar un dominio Ms Active Directory o LDADP simplifica la administración de políticas en e los equipos, aporta trazabilidad a las acciones sobre el sistema de información, privacidad a los usuarios y un mejor ajuste de privilegios.

Es recomendable purificar el aire del entorno de trabajo para evitar males a los equipos. Una instalación de aire acondicionado filtra partículas, controla la temperatura y la humedad. Aún así, es recomendable limpiar periódicamente el interior de las cajas pues la acumulación de polvo es inevitable; los equipo se comportar como verdaderas aspiradoras. La climatización del local puede mitigar este efecto.

El acceso al hardware del sistema debe estar reservado únicamente al personal autorizado para ello, por tanto se deben disponer medidas para evitar manipulaciones fuera de lugar.

Al centralizar la Conselleria d'Educació los datos del alumnado, es esta la responsable de elaborar el documento de seguridad teniendo presente que en el deben figurar los responsables de tratamiento de cada centro y los usuarios autorizado a operar sobre esos datos. El documento de seguridad contiene los protocolos de operación establecidos, por tanto, debe divulgar este documento a los centro para que actúen en consecuencia. En este documento también se establece el modo de realizar las auditorias que dada la naturaleza de ITACA se deberán realizar sobre los sistemas ITACA de la Conselleria y una muestra aleatoria de centros para auditar así todos los procesos de tratamiento.

Elaborar un registro de entrada / salida con los soporte que portan información, así como una declaración de su contenido es obligatorio. El tiempo de guarda de esta información es de dos años. En caso de desastre se puede determinar quién es responsable de una fuga de datos o de

una escritura errónea.

Las vulnerabilidades detectadas pueden agruparse en dos conjuntos: las que requieren soluciones técnicas y las que requieren soluciones funcionales o de políticas. Para el primer grupo se pueden solucionar en su totalidad con la implantación de un dominio y el uso de GPO para implementar las directivas. Para el segundo grupo, se requiere el desarrollo de políticas, protocolos y campañas informativas que cubran los aspectos no técnico problemáticos; por ejemplo: la clausula de confidencialidad, el documento de seguridad o el plan de contingencia.

Conclusión

El presente trabajo ha sido una oportunidad de ejercitar los conocimiento adquiridos en la carrera, tanto técnicos como de gestión de proyectos. La incertidumbre sobre cuál es el desarrollo correcto y el desconocimiento en materia de auditoría han causado muchos momento de reflexión antes de avanzar.

Por otra parte, existe una frustración fruto de la dificultad para conseguir participación en la encuesta que nutre de datos este proyecto; no solo en línea, sino la negativa a la participación presencial. Una mayor cantidad de dato hubiera posibilitado ver con mayor claridad una distribución normal sobre las respuestas de los ítems.

Durante la ejecución del proyecto he aprovechado para realizar dos curso ofertados por el Centro de formación permanente que creo que eran de interés para este trabajo: "Fundamentos de la seguridad de la información: certificación ISO/IEC 27002" y "Curso de auditor interno ISO 9000". Yo creo que algo me han aportado para hacer este proyecto.

La complejidad técnica de las soluciones ha sido menor de lo esperado a priori pues todo es solucionable con las herramientas administrativas para un dominio Ms Active Directory o LDAP

Finalmente, tratar de realizar una auditoría sin experiencia no ha sido sencillo. En qué aspectos fijar la atención, como preguntar y como evaluar los elementos del sistema son cuestiones que aún se me escapan de las manos. Tampoco se ponderó correctamente la influencia de ITACA sobre los elementos del cuestionario, pues la implantación de este sistema anula algunas cuestiones.

Creo este proyecto cumple con su cometido de ejercicio académico, pero que pasará sin pena ni gloria. Teniendo en cuenta las circunstancias, podría haber fracasado totalmente.

> ***"Si todos los usuarios mejoraran sus contraseñas esta noche, y no las dejaran apuntadas en un sitio fácil de encontrar, mañana amaneceríamos, de repente, en un mundo mucho más seguro."***
>
> ***Kevin D. Mitnick, El arte de la intrusión p. 349***

Anexos

etsinf
Escuela Técnica Superior de Ingeniería Informática

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Sol.licitud d'Aprovació de PFC TIPUS B

Solicitud de Aprobación de PFC TIPO B

Dades Personals de l'Alumne/Datos Personales del Alumno

Cognoms/Apellidos:	Villalta Frutos	Nom/ Nombre:	Javier
DNI: 44154993-F	Correu electrònic/Correo electrónico: javilfru@inf.upv.es		Telèfon/Teléfono: 615 722 756

Dades del Projecte/Datos del Proyecto

Títol/Título: *Vulnerabilidades comunes en sistemas de información escolares y posibles soluciones*

Titulació/Titulación: *Ingeniería informática*

Dades/Datos del Director o Codirector/a del PFC de la ETSINF(1)

Nom/Nombre: Eva María Cutanda García

Departament/Departamento: DOE

(1)Qualsevol professor que imparteixi docència en la ETSINF./Cualquier profesor que imparta docencia en la ETSINF.

Dades del Codirector/a del PFC/ Datos del Codirector/a del PFC

Nom/Nombre:……

Departament/Departamento:…… ……

Si no és professor de la ETSINF/Si no es profesor de la ETSINF(2):

D.N.I.:…… E-mail:……Telèfon/Teléfono:……..

"D'acord amb la Llei orgànica 15/1999 de 13 de desembre de Protecció de Dades de Caràcter Personal i STC 292/2000, l'informem que les seues dades seran incorporades a un fitxer automatitzat amb una finalitat exclusivament administrativa. L'interessat podrà dirigir-se a la E.T.S. d'Enginyeria Informàtica com a responsable dels fitxers, per a exercir el seu dret d'accés, rectificació, cancel·lació i oposició. El fitxer es troba en el sistema informàtic de la UPV en El Camí de Vera s/n. / De acuerdo con la Ley orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal y STC 292/2000, le informamos de que sus datos serán incorporados en un fichero automatizado con una finalidad exclusivamente administrativa. El interesado podrá dirigirse a la E.TS. Ingeniería Informática como responsable de los ficheros, para ejercer su derecho de acceso, rectificación, cancelación y oposición. El fichero se encuentra en el sistema informático de la UPV en el Camino de Vera s/n"

Si ☐ No ☐ (marque el que desitge)(marque lo que desee) done el meu consentiment a la utilització de l'esmentada informació als fins anteriorment indicats / doy mi consentimiento a la utilización de la citada información a los fines anteriormente indicados.

Sign./Fdo. ……

(2) Haurà d'acreditar la titulació (Fot. Títol) / Tendrá que acreditar la titulación (Fot. Título)

Documentació a adjuntar/ Documentación a adjuntar

Descripció del Projecte (en full a banda, entre dues i tres pàgines)/Descripción del Proyecto (en hoja aparte, entre dos y tres páginas)

Valéncia, 28 de Junio de 2011

V.P. Director/a PFC de la ETSINF VºBº Director/a PFC de la ETSINF	Sign. Alumne/a Fdo.Alumno/a	Aprovació direcció centre Aprobación dirección centro
		Sign. centre / Fdo. Centro

Vulnerabilidades comunes en sistemas de información escolares y posibles soluciones

Abstract

Este proyecto puede ser descrito, a groso modo, por dos macro fases. Por un lado, el estudio de las vulnerabilidades presentes en los sistemas de información escolares seleccionados como representación del total de centros docentes. Y por otro lado, tras el análisis de los resultados, la proposición de soluciones lo más sencillas posibles a la vulnerabilidades más comunes.

Descripción desarrollada

Sobre el método de encuesta y la muestra seleccionada

Mediante una batería de preguntas se auditarán diferentes aspectos del sistema de información, en adelante SI, como configuraciones, diseño de red o políticas de seguridad. Las auditorías se realizarán principalmente vía telemática entre colegios de las tres provincias de la Comunitat Valenciana. Alternativamente, se realizarán algunas auditorias presenciales para asegurar un mínimo de datos. En este último caso, los centros seleccionados estarán localizados en área metropolitana de la ciudad de Valencia o poblaciones cercanas para facilitar el desplazamiento.

El análisis de los datos

En cuanto al análisis de datos, se ordenarán los items de la encuesta, que indican posibles vulnerabilidades, en función de su relevancia. Se entiende que a mayor número de centros afectado mayor será la relevancia del item. En la primera fase del análisis se considerarán todos los centros como iguales, y en una segunda fase se analizarán por clústeres; de esta forma se podrá deducir si las variables de agrupación influyen en la seguridad del SI. Son variables de agrupación a estudiar:

- El tamaño del SI: en función de que formaciones imparte el centro.

- El carácter del centro: público o privado.
- La implantación del sistema Ítaca.

Se inferirán posibles patrones, combinaciones de items, en función de la influencia de las variables de agrupación.

Proposición de soluciones

Con respecto a la proposición de soluciones, a priori, se definirá una solución por cada item para ofrecer un feedback inmediato a los centros escolares al finalizar la batería de preguntas. Tras el análisis de los datos propondrán soluciones a los patrones inferidos, sin perder de vista el binomio calidad-coste.

Resumen esquemático de las tareas principales

- Fase 1: Auditoría de centros
    - Estudio de precedentes
    - Elaboración del cuestionario
    - Proposición inicial de soluciones, una por ítem del cuestionario
    - Periodo de auditoría
        - Auditoría telemática
        - Auditoría presencial

- Fase 2: Estudio de soluciones
    - Análisis de datos
        - Inferencia de patrones sobre el conjunto total de datos
        - Inferencia de patrones sobre clústeres
        - Conclusiones sobre influencia de las variables de agrupación
    - Proposición de soluciones a los patrones inferidos

Asignación PFC tipo B

ASIGNACION PFC TIPO B

Estimado alumno/a: JAVIER VILLALTA FRUTOS

Por la presente te remito la información referente a la asignación de tu proyecto final de carrera:

DIRECTOR/A: Eva María Cutanda García

CÓDIGO P.F.C.: DOEEFC-97

TÍTULO: VULNERABILIDADES COMUNES EN SISTEMAS DE INFORMACION ESCOLARES Y POSIBLES SOLUCIONES

Un saludo,

Valencia, a 12 de Julio de 2011

SUBDIRECCIÓN DE ORDENACIÓN ACADÉMICA

‘ etsinf
Escuela Técnica Superior de Ingeniería Informática

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Sol.licitud Avaluació Project Final

Solicitud de Evaluación de Proyecto Final de Carrera

Dades Personals de l'Alumne/Datos Personales del Alumno

Cognoms/Apellidos: Villalta Frutos — Nom/ Nombre: Javier

DNI: 44154993-F

Correu electrònic/Correo electrónico:

Telèfon/Teléfono: 615 722 756

Domicili/Domicilio: Pº Martutene nº98,1º — Població/Población: Donostia-San Sebastián

Codi Postal/Código postal: 20014 — ºProvíncia/Provincia: Gipuzkoa

Dades del Projecte/Datos del Proyecto

Tipus/Tipo: A ☐ Departament/Departamento B ☒ Projectes específics/Proyectos específicos C ☐ Empreses o Universitats/Empresas o Universidades

Codi PFC/Código PFC: DOEEFC-97 — *Data aprobación/Fecha aprobación: 12 de Julio de 2011*

Títol/Título: Vulnerabilidades comunes en sistemas de información escolares y posibles soluciones

Titulació/Títulación: Ingeniería informática

Vau sol·licitar pròrroga?/Solicitó prórroga? Sí ☒ No ☐ Data d'aprovació/Fecha de aprobación: 28 de octubre de 2011

A emplenar pel Director del Projecte / A cumplimentar por el Director del Proyecto

Eva Mª Cutanda García, director del projecte/director del proyecto, ……, codirector del projecte,/codirector del proyecto,

han dejado disponible la memoria del PFC según la normativa(1) y autoritzen la persona interessada perquè sol·licite ser avaluada per:/autorizamos a la persona interesada para que solicite ser evaluada por:

☒ Director(2)

☐ Tribunal(3) en la convocatòria de / Tribunal en la convocatoria de:

☐ febrer / febrero ☐ juliol / julio ☐ setembre / septiembre

Director del projecte/Director del proyecto — Codirector o tutor del projecte/Codirector o tutor del proyecto

València, 30 de diciembre de 2011

Segons la normativa de PFC aprovada en la Comissió Permanent celebrada el dia 10 de juny de 2010 y modificada en sesión celebrada el 14 de abril de 2011/ Segons la normativa de PFC aprovada en la Comissió Permanent celebrada el dia 10 de juny de 2010 y modificada en sesión celebrada el 14 de abril de 2011:

(1) El director ha de deixar disponible en el PoliformaT la memòria del PFC seguint les directrius descrites en l'Annex A de aquesta normativa. / El director debe dejar disponible en el PoliformaT la memoria del PFC siguiendo las directrices descritas en el Anexo A de dicha normativa.

(2) L'alumne, al sol·licitar aquest tipus d'avaluació, renúncia a la part de la qualificació corresponent a l'exposició del PFC. / El alumno, al solicitar este tipo de evaluación, renuncia a la parte de la calificación correspondiente a la exposición del PFC.

(3) El director podrà, si ho desitja, emetre un informe del PFC, que serà deixat disponible així mateix en el PoliformaT. / El director podrá, si lo desea, emitir un informe del PFC, que será dejado disponible asimismo en el PoliformaT.

Documentació a adjuntar/ Documentación a adjuntar

Haurà d'entregar-se, junt amb aquesta sol·licitud/Deberá entregarse, junto con esta solicitud:

☒ Escrit d'autorització de consulta del PFC/ Escrito de autorización de consulta del PFC.

Autorización de consulta

UNIVERSIDAD POLITECNICA DE VALENCIA

Autorización para la difusión de obras digitales a favor del Área de Bibilioteca y Documentación Científica de la Universidad Politécnica de Valencia

D/Dª _____ DNI/Pasaporte núm. _____, autor/a de la obra titulada _____ autoriza a la Universidad Politécnica de Valencia a:

1. Poner para uso privado y/o con fines de investigación y docencia a disposición electrónica la obra anteriormente citada mediante su incorporación a través de cualquier medio y, en particular, a través de Internet, o cualquier otro canal o destino de la información que sea susceptible de adscripción a Internet, así como a través de la televisión digital, por cable o cualquier otra plataforma o forma de transmisión de datos tecnológica –como, por ejemplo, ondas hertzianas, transmisión telemática o transmisión por fibra óptica. La Universidad no garantiza ni asume ninguna responsabilidad por la forma y manera como los usuarios hagan uso posterior de la tesina.
2. Adaptar la obra en la medida en que sea necesario para ponerla a disposición electrónica a través de Internet o a cualquier otra tecnología susceptible de adscripción a Internet, así como incorporar 'marcas de agua' o cualquier otro sistema de seguridad en el formato electrónico de la tesina.
3. El autor/a autoriza la difusión de la obra:
   (marcar la opción deseada)

   ☐ mediante la licencia Creative Commons o similar "Reconocimiento-NoComercial-CompartirIgual", que permite reproducir, distribuir, comunicar públicamente y hacer obras derivadas.

   ☐ mediante la licencia Creative Commons o similar "Reconocimiento-NoComercial-SinObraDerivada", que permite reproducir, distribuir, comunicar públicamente pero no hacer obras derivadas.

   (Estas licencias autorizan en todo caso la reproducción, distribución y comunicación pública de la obra por cualquier persona siempre que mencione la autoría y se realice con fines no comerciales).

   ☐ sin aplicación de ninguna licencia Creative Commons

En ningún caso esta autorización implica una cesión en exclusiva de los derechos de explotación del autor sobre la obra ni impide la explotación normal de la obra a través de las formas habituales. Cuando la tesina se muestre en una base de datos se deberá hacer figurar tanto el nombre del Autor/a como el de la Universidad, así como cualquier otra mención específica y razonable indicada por éste.

La duración de esta autorización entrará en vigor el día de su firma y se entiende por un periodo inicial de 5 años, prorrogables de forma automática por periodos sucesivos de igual duración excepto revocación expresa de la autorización por parte del autor/a de la obra. Esta autorización vincula a los sucesores del autor/a de la obra.

El autor/a declara que es el legítimo propietario de los derechos de autor de la obra cuya autorización concede con este documento. Sin perjuicio de cualquier otro derecho que pueda corresponderle, la Universidad podrá rescindir unilateralmente la presente autorización en caso de que un tercero haga prevalecer cualquier derecho sobre toda o parte de la tesina. En caso de la existencia de cualquier reclamación de un tercero relacionada con la tesina, queda la Universidad exenta de responsabilidad.

Si el documento incluye obras de las cuales el autor/a no es el propietario de los derechos de explotación (fotografías, dibujos, textos, etc.), éste declara que ha obtenido el permiso sin restricción del titular correspondiente para conceder la presente autorización.

En caso de surgir alguna discrepancia en el alcance, interpretación y/o ejecución de la presente autorización, las partes se someten a la competencia de los Juzgados y Tribunales de la Ciudad de Valencia y sus superiores jerárquicos, con expresa renuncia a su fuero, de ser éste diferente.

Valencia, a de de 20

El autor/a

Aprobación de prórroga PFC

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

PRÓRROGA PFC

etsinf
Escuela Técnica Superior de Ingeniería Informática

Estimado alumno/a: JAVIER VILLALTA FRUTOS

Por la presente te remito la información referente a la prórroga de tu proyecto final de carrera:

DIRECTOR/A: Eva María Cutanda García

CÓDIGO P.F.C.: DOEEFC-97

TÍTULO: VULNERABILIDADES COMUNES EN SISTEMAS DE INFORMACION ESCOLARES Y POSIBLES SOLUCIONES

Según la normativa de PFC aprobada por la Comisión Permanente de 10 de junio de 2010, la prórroga será válida únicamente para el curso académico 2011/2012.

Un saludo,

Valencia, a 28 de Octubre de 2011

SUBDIRECCIÓN DE ORDENACIÓN ACADÉMICA

Bibliografía

- *Plan sectorial de oficio a la enseñanza reglada no universitaria*, 29 de diciembre de 2006; Agencia Española de protección de datos.
- *Buenas prácticas TIC*; Conselleria d'Educació.
- Apuntes de la asignatura *Administración de sistemas* curso 2010-2011; Agustón Espinosa Minguet, Andrés Terrasa Barrena, Fernando Ferrer García y Álvaro Alvarez Rodríguez.
- *Linux: administración del sistema*; Iñaki Alegría Loinaz, Roberto Cortiñas Rodríguez y Aitzol Ezeiza Ramos. Editorial Pearson practice hall, 2005. ISBN: 84-205-4848-0.
- *Auditoría de tecnologías y sistemas de información*; Emilio del Peso Navarro, Mar del Peso, Mario G. Piattini Velthuis. Editorial RA-MA, 2008. ISBN: 978-84-7897-849-6.
- *Enciclopedia de la seguridad informática*, Álvaro Gómez Vieites. Editorial RA-MA, 2006. ISBN: 978-84-7897-731-4.
- *El arte de la intrusión*, Kevin D. Mitnick y William L. Simon. Editorial RA-MA, 2006. ISBN: 978-84-7897-748-2