**INGENIERO TÉCNICO DE INFORMÁTICA DE GESTIÓN**


# UN ESTUDIO SOBRE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

AUTOR:

JESÚS FRIGINAL LÓPEZ

DIRECTOR:

DAVID DE ANDRÉS MARTÍNEZ

Marzo 2011

# Introducción

La seguridad pasa por entender que uno de los activos más valiosos De forma clásica, la seguridad de los sistemas de información (SI) de las empresas se ha entendido como una rama dependiente del llamado "dpto. de informática", no obstante, de un tiempo a esta parte, se está consiguiendo que la seguridad empiece a concebirse como una filosofía de la propia organización, como pueden ser la calidad, o el respeto al medio ambiente.

El activo más importante de la organización es la información, y no tanto los componentes software o hardware, que pueden ser reemplazados. El cambio de mentalidad es paulatino, pero progresivo. Aun así, en muchas empresas, la alta dirección es reticente todavía a apostar por la seguridad porque no se entiende ésta como una inversión, sino como un gasto. Además, no se percibe la seguridad como un proceso evolutivo. De esta manera, de los gastos en activos informáticos de las organizaciones, los controles tácticos rondan el 90%, mientras que la seguridad estratégica apenas supera el 10%.

La gestión adecuada de la seguridad permite adaptarse a los cambios que vayan apareciendo en el entorno de la organización, ya sean legislativos como la LOPD, las regulaciones sectoriales como Basilea II, o CobIT.

El usuario es el primer agente que rompe la seguridad de los SI dentro de la organización, ya que de poco sirve blindar un sistema con toda la tecnología posible si luego el usuario no es responsable. Por ejemplo, si anota su *password* de acceso al sistema en un *post-it* y lo pega en el monitor a la vista de todo el mundo. O si un comercial almacena en su *pen drive* la información de todos los clientes a los que debe visitar, y luego sale por la puerta sin ningún control.

Las principales amenazas a las que se enfrenta el sistema de información son: La negación del servicio desautorizada, la divulgación de información desautorizada, la mimetización, el uso de recursos no autorizado, la alteración de recursos no autorizada y el repudio de acciones.

Mientras que las principales necesidades de la administración de identificadores son: Los registros de accesos de los usuarios al sistema, el auto-servicio para usuarios finales, es decir, el que un usuario pueda administrar su propia contraseña, los flujos de aprobación de permisos, los bloqueos de usuarios, el uso de una correcta política de contraseñas, el aprovisionamiento de identidades de los usuarios, es decir, saber en todo momento que quien está en el sistema, y la sincronización de cambios de contraseñas. Toda esta gestión es capaz de realizarla el Motor de aprovisionamiento de Oracle

Por otro lado, necesidades a las que se expone la gestión de accesos son: la autenticación de usuarios, el control y unas buenas políticas de acceso, independizar las aplicaciones de la autenticación, Single Sing-on independiente del tipo de aplicación, es decir, un usuario por empleado, no un usuario por empleado por aplicación.

Estas prácticas son muy recomendables, pues conllevan que las auditorias se realicen de una forma más ágil y eficaz.

En resumen, éstos son los retos a los que se enfrenta la seguridad de la información en las organizaciones, y cuál es la manera de atajarlos:

| **Amenazas** | **Medidas de seguridad** |
|---|---|
| Suplantación | Autenticación |
| Uso no autorizado | Autorización/Control de accesos |
| Comportamiento sospechoso | Auditoria |
| Apertura de información | Confidencialidad y privacidad |
| Evasión de responsabilidad | Integridad |
| Denegación del servicio | No-repudio |

El presente proyecto se centra en el estudio de las amenazas de la seguridad en los sistemas de información, y las técnicas y metodologías ideadas para poder combatirlas y neutralizarlas.

## *Importancia de la Información*

Cuando se habla de la función informática generalmente se tiende a hablar de

tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información más consistente, etc.

Sin embargo se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la *información*.

Es muy importante conocer su significado dentro la función informática, de forma esencial cuando su manejo esta basado en tecnología moderna, para esto se debe conocer que la información:

1. esta almacenada y procesada en computadoras
2. puede ser confidencial para algunas personas o a escala institucional
3. puede ser mal utilizada o divulgada
4. puede estar sujeta a robos, sabotaje o fraudes

Supóngase por un momento que se sufre un accidente en el centro de cómputo o el lugar donde se almacena la información. ¿Cuánto tiempo pasaría para que la organización este nuevamente en operación?

Es necesario tener presente que el lugar donde se gestiona la información, con frecuencia el centro de cómputo, puede ser el activo más valioso y al mismo tiempo el más vulnerable.

Es muy importante conocer el significado de dos palabras: riesgo y seguridad.

## *Riesgo*

1. Proximidad o posibilidad de un daño, peligro, etc.
2. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.
3. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

## Seguridad

1. Cualidad o estado de seguro.
2. Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo.

Con estos conceptos claros se puede hablar de la criminología, que ya ha calificado los "delitos hechos mediante computadora" o por "sistemas de información" en el grupo de delitos difícilmente investigados o encontrados.

## *"Problema de Seguridad"*

A continuación se detalla todos aquellos tipos de conflictos que podrían estar incluidos en el conjunto de problemas considerados como "de Seguridad":

1. Aquellos que comprometen la integridad o la privacidad de los datos almacenados.
2. Aquellos que permiten acceso a recursos supuestamente no permitidos.
3. Aquellos que impiden el acceso a recursos a usuarios legítimos.
4. Aquellos que permiten hacer un mal uso de los recursos informáticos.

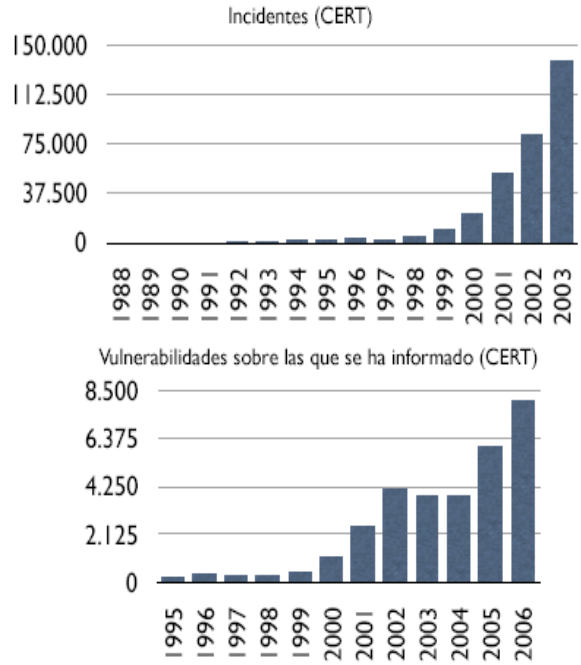
## *¿Los sistemas son seguros?*

Los sistemas no son tan seguros como muchos usuarios piensan. Existe una gran cantidad de factores que hacen que nuestros sistemas se vuelvan vulnerables. Se puede encontrar numerosos ejemplos, entre los más significativos se encuentran los de la lista que aparece abajo:

1. Virus informáticos, Troyanos, Gusanos.
2. Páginas web "hostiles".
3. "Spyware".
4. Entradas en sistemas ajenos.
5. Robo de datos bancarios.
6. Cambio de páginas Web.
7. Ataques DoS a nivel mundial.

Las estadísticas reflejan esta situación de inseguridad generalizada, cuya tendencia parece seguir una trayectoria que asciende peligrosamente a través de los años.

## Estadísticas




Como parte del proceso de recopilación estadística, se recogen vulnerabilidades de una gran variedad de fuentes públicas y se anima a la gente a informar de las vulnerabilidades de las que tengan conocimiento.

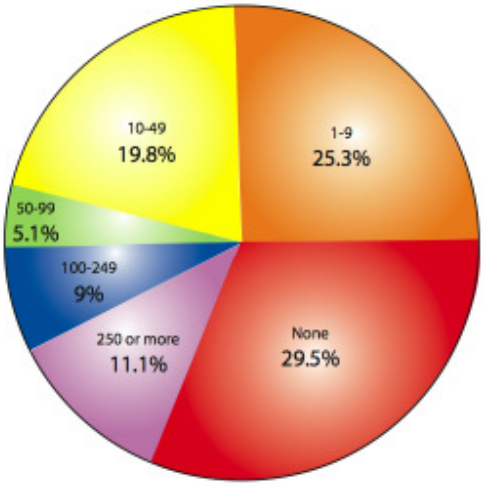
Dado el uso generalizado de herramientas de ataque automático, los ataques contra sistemas conectados a Internet se han convertido en algo tan común que las cuentas recogidas de los incidentes producidos proporcionan poca información con respecto a la valoración del alcance e impacto de los ataques. Por ese motivo en los principios de 2004, se paró de publicar el número de incidentes producidos.

*Un incidente puede implicar un sitio o cientos (o incluso miles) de sitios. También, algunos incidentes pueden incluir actividad durante largos períodos de tiempo.*

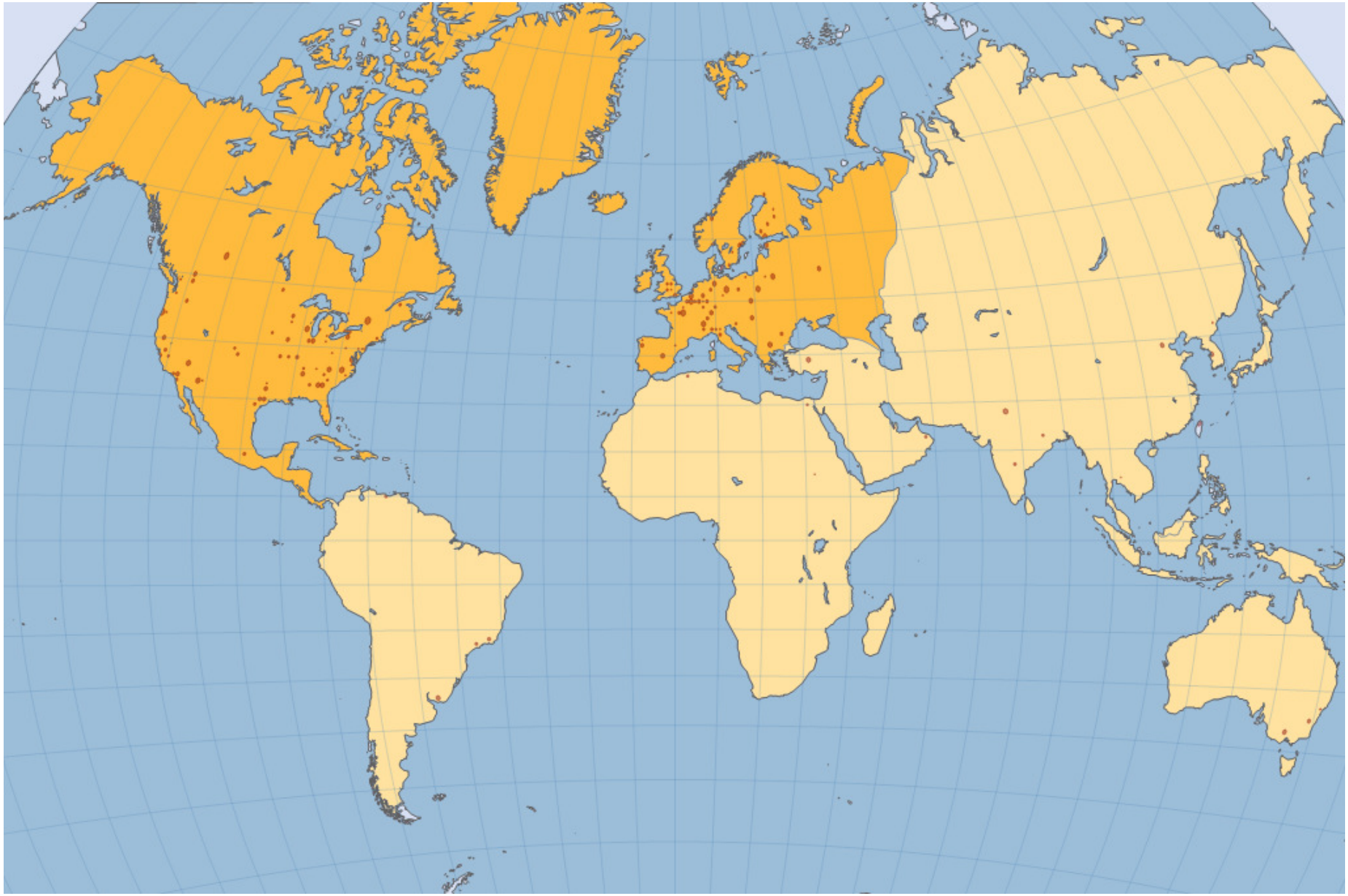
A continuación se muestra la distribución del número de incidentes por organización. Se observa que aunque hay casi una cuarta parte que no registra ningún incidente, hay una gran proporción para la que se detectan 250 incidentes o más, lo cual es alarmante.

Número de incidentes por organización

*2009 E-Crime Watch Survey*




En la página siguiente se puede ver un mapa del mundo en el que se muestra la distribución de todo tipo de virus en cada área en la actualidad, para un nivel de alerta medio:



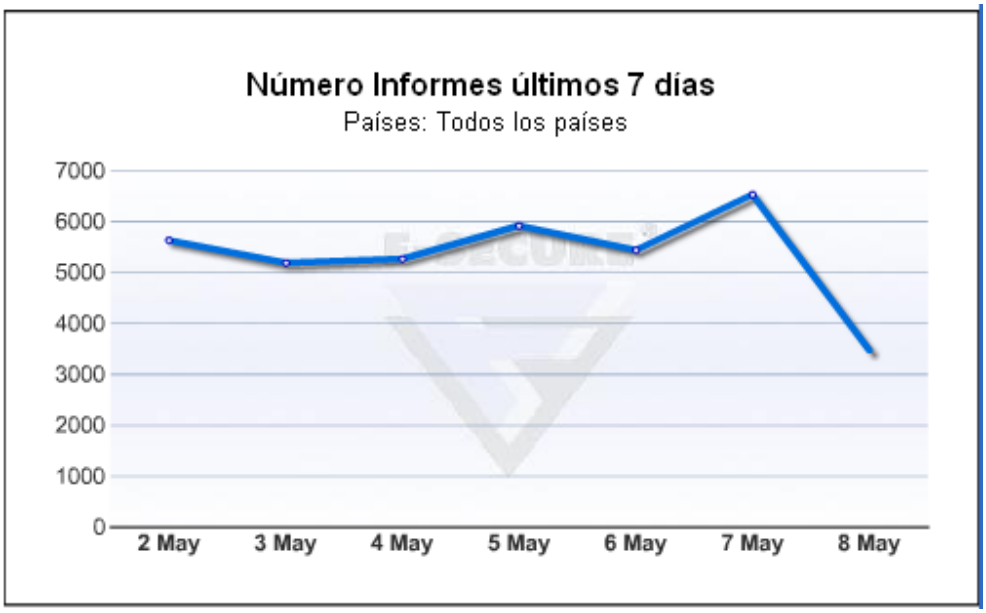
**Nivel de Alerta**: medio

**Período de tiempo**: 1 Mayo 2007
**Infección(es):** Todos los virus
**Área:** El mundo  Abajo se puede observar cuáles son los virus más activos del mundo. La información proviene de fuentes de todo el mundo, que utilizan F-Secure Anti-Virus para proteger sus sistemas.

Virus las últimas 24 horas:

| Lugar | Tendencia | Nombre del Virus | Nivel de Radas | Porcentaje |
|---|---|---|---|---|
| 1 | → | Email-Worm.Win32.Mydoom.m | - | 3,5 % |
| 2 | ↑ | Email-Worm.Win32.Nyxem.e | 2 | 1,1 % |
| 3 | → | W32/Malware | - | 0,9 % |
| 4 | → | W32/Suspicious_F.gen | - | 0,8 % |
| 5 | → | WhenU.SaveNow | - | 0,7 % |
| 6 | ↑ | Virus.Win32.Cheburgen.a | - | 0,7 % |
| 7 | → | Stealth_process | - | 0,6 % |
| 8 | → | Win32.Trojandownloader.Zlob | - | 0,6 % |
| 9 | → | W32/Suspicious_U.gen.dropper | - | 0,6 % |
| 10 | ↑ | Trojan-PSW.Win32.OnLineGames.es | - | 0,5 % |

*Actualizado: 8/5/2009, 12:37:49 PM*


Número Informes últimos 7 días
Países: Todos los países
7000
6000
5000
4000
3000
2000
1000
0
2 May
3 May
4 May
5 May
6 May
7 May
8 May

# ¿Qué es un Sistema de Información?

## *Definiciones*

Oz (2001)
*Todos los elementos que funcionan en conjunto para **procesar datos** y **producir información.***

Saroca (2002)
*Conjunto de **recursos humanos, materiales, financieros, tecnológicos, normativos y metodológicos**, organizado para brindar, a quienes operan y a quienes adoptan **decisiones** en una organización, la **información** que requieren para desarrollar sus respectivas **funciones**.*

Laudon (2001)
*Conjunto de **componentes interrelacionados** que **reúne** (u obtiene), **procesa**, **almacena** y **distribuye información** para **apoyar la toma de decisiones** y el **control** en una **organización**. Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también ayudan a los administradores y trabajadores a analizar problemas, visualizar aspectos complejos y crear productos nuevos.*

De las definiciones anteriores se deduce que un Sistema de Información no requiere necesariamente el uso de las tecnologías informáticas. Ha habido Sistemas de Información antes de que se crearan los ordenadores.

## *Funciones de un Sistema de Información*

1. **Recolección**
   Capturar y registrar los datos. Actúa como el órgano sensorial de la organización.

2. **Clasificación**
   Identificar los datos, agruparos en conjuntos homogéneos, y ordenarlos

teniendo en cuenta la manera en que será necesario recuperarlos.

3 **Compresión**
Reducir el volumen de los datos sin disminuir necesariamente la información que suministrarán a su destinatario.

4 **Almacenamiento**
Conservar físicamente los datos, con su adecuada protección.

5 **Recuperación**
Suministrar el acceso a los datos.

6 **Procesamiento**
Transformar de entradas en salidas a través de los procesos.

7 **Transmisión**
Comunicación entre puntos geográficos distantes.

8 **Exhibición**
Proporcionar salidas de información preparadas de modo que resulte legible y útil a su destinatario.

## *Por qué hay que clasificar la información*

Clasificar la información proporciona un excelente medio de separarla en categorías, con diferentes niveles de protección y sus correspondientes requerimientos. Dado que en el fondo subyace un tema económico, el factor decisivo en la clasificación de la información es la justificación económica de su protección. No obstante, en el correo electrónico, la privacidad ocupa un lugar de privilegio.

El mundo de los negocios está marcado por la obtención de beneficios o pérdidas, lo que significa que la seguridad debe estar justificada en sus costes. Las decisiones de clasificación en el sector privado están marcadas por las consecuencias no sólo de la difusión no autorizada, sino de la destrucción, modificación o falta de disponibilidad de

la información. Esta protección contra pérdida, cambio o indisponibilidad puede ser más importante que la protección contra su difusión. La información es clasificada basándose en las pérdidas financieras que la organización sufriría si tuviera lugar un ataque, bien sea accidental o intencional.

La Administración Pública, por otra parte, en el ejercicio de las competencias que legalmente tiene atribuidas, debe velar por el interés público, así, en consecuencia, la clasificación de la información que maneja vendrá definida por razones de interés público, por intereses de terceros más dignos de protección o cuando así lo disponga la Ley. La protección de la información en la Administración contra pérdida, cambio, indisponibilidad o difusión es de gran trascendencia y no sólo económica, pues un fallo en la misma produciría lesiones en sus derechos a los terceros afectados y podría afectar negativamente a intereses de estado.

## *Categorías de clasificación de la información*

Por todo ello, se establece la clasificación de la información según tres aspectos fundamentales. Un baremo indica la **sensibilidad a la difusión** (confidencialidad), otro hará referencia a la **manipulación fraudulenta** (integridad) y un último señalará la **criticidad** de la información para la operativa de la organización.

Tanto el grado de *sensibilidad* como el de *integridad* marcan el nivel requerido de control de accesos.

El grado de *criticidad* determina los procesos de recuperación y 'backup'. Una información designada como confidencial y no crítica, por ejemplo, sugiere un control estricto en los accesos pero no así en los procedimientos de recuperación. Así, se puede establecer unos procedimientos derivados de la clasificación establecida, de forma que si se requiere total o selectiva confidencialidad, la conexión debe establecerse de la manera apropiada, incluyendo la implementación de claves de trabajo y la negociación de los parámetros de criptografía para la conexión.

Si la integridad de todos los datos del usuario, con o sin recuperación, o la integridad de parte de ellos es un requerimiento, al igual que en caso anterior, debe procurarse

una conexión protegida adecuadamente.

## *Sistemas de Información en el entorno empresarial*

Los sistemas de información se han constituido como una base imprescindible para el desarrollo de cualquier actividad empresarial; estos sistemas han evolucionado de forma extraordinariamente veloz, aumentando la capacidad de gestión y almacenamiento. El crecimiento ha sido constante a lo largo de las últimas décadas, sin embargo, esta evolución tecnológica también ha generado nuevas amenazas y vulnerabilidades para las organizaciones.
La difusión de las noticias relacionadas con la seguridad informática ha transcendido del ámbito técnico al ámbito social, donde regularmente se pueden leer en prensa titulares como:

Evitado el que podía haber sido el mayor robo bancario en Reino Unido [18-03-05]
Fuente: http://delitosinformaticos.com/noticias/111113819358799.shtml

Nueva estafa de phising afecta a Cajamar y Cajamadrid [25-03-05]
Fuente: http://www.elmundo.es/navegante/2005/03/28/seguridad/1112004210.html

La policía detiene a una mujer por participar en una novedosa estafa de un "hacker" [27-04-05]
Fuente:http://www.entrebits.com/noticias/Internet/articulos/n_81085.html

Amenazas como los virus han trascendido del ámbito local, permitiendo crear amenazas que en cuestión de minutos pueden alcanzar a cualquier equipo conectado a Internet.

Las amenazas parecen alcanzar solamente a empresas de renombre internacional como objetivos de los hackers, haciendo que la seguridad se considere de forma tradicional como un apartado oscuro – al igual que la inseguridad –; el ataque de hackers a través de redes que roban secretos de la empresa es un hecho poco frecuente, si se compara con las verdaderas amenazas que habitualmente se materializan en entornos de Pymes: accesos no autorizados a la información, pérdida

de datos por negligencia o por virus, etc., son hechos que se configuran como verdaderas amenazas de la seguridad de la información.

Cuando se aborda la problemática de la seguridad, la organización analiza habitualmente aspectos relacionados con la disponibilidad de los datos, copias de seguridad, mantenimiento de los ordenadores y servidores, mantenimiento de las redes, etc., todos ellos orientados a la disponibilidad de los datos, olvidando otras características que se deben cuidar igualmente como son la integridad y la confidencialidad.

Las dimensiones de la seguridad abarcan los siguientes puntos:

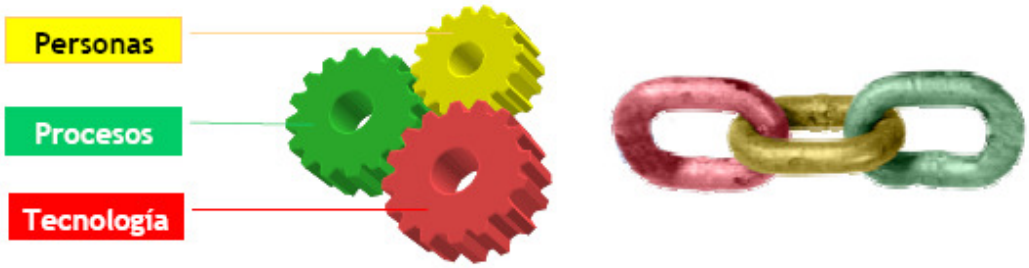
1. Disponibilidad
2. Integridad
3. Confidencialidad
4. Autenticación
5. Trazabilidad

Los aspectos a analizar son amplios y la inversión a realizar es igualmente importante, sin embargo, es preciso definir una estrategia que planifique las actuaciones a realizar, tanto para comprometer recursos económicos como humanos.

Lo importante no es tanto la ausencia de incidentes como la confianza en que están bajo control: se sabe qué puede pasar y se sabe qué hacer cuando pasa. Conocer los riesgos para poder afrontarlos y controlarlos. Para ello es primordial una correcta Gestión de la seguridad.

La gestión de la seguridad viene condicionada por tres elementos que deben funcionar de forma conjunta y coordinada:

1. Tecnología: medidas tecnológicas de protección.
2. Procesos: supervisar el correcto funcionamiento de la tecnología y las personas
3. Personas: utilizan la tecnología y ejecutan los procesos




Esta problemática hace necesaria una estrategia de apoyo a las Pymes y Micropymes, que deben solucionar, en situación de desventaja frente a competidores más grandes, la seguridad de su información y el cumplimiento de sus obligaciones legales.

## ¿Qué es la seguridad?

Aunque no existe una definición exacta, es la capacidad de mantener intacta y protegida la información de sistemas informáticos.

Existen ***cuatro conceptos básicos en seguridad*** que son:

**INTEGRIDAD:** Se define como la característica que previene contra la modificación o destrucción no autorizadas de los activos.

**DISPONIBILIDAD:** Se define como la característica que previene contra la denegación no autorizada de acceso a los activos.

**CONFIDENCIALIDAD:** Se define como la característica que previene contra la divulgación no autorizada de los activos.

**AUTENTICACIÓN:** Se define como la característica de dar y reconocer la autenticidad de los activos (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones.

Se entiende por activos a los recursos del sistema de información o relacionados con

éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Los análisis en materia de Seguridad de los Sistemas de Información, giran alrededor de estos cuatro conceptos. Evidentemente, para ello se debe identificar primero los posibles riesgos y amenazas, y su repercusión en la organización, para después estudiar las posibles medidas que se debe tomar para evitarlos o disminuirlos, tomando la decisión final después de un estudio coste/beneficio de acuerdo con el nivel de seguridad establecido para lograr los objetivos propuestos en esta materia.

## *Elementos de un programa de protección de la información*

En cualquier organización, un programa de protección de la información debe contemplar los siguientes elementos:

1. **Políticas.** Contemplan una descripción de objetivos y estrategias.
2. **Estándares.** Recogen requerimientos más específicos para la consecución de los objetivos marcados. Deben ser suficientemente generales para su amplia aplicación, pero lo suficientemente concretos para poder ser contrastados y evaluados.
3. **Guías.** Incluyen recomendaciones sobre cómo sintonizar con los estándares establecidos.
4. **Procedimientos.** Detallan paso a paso formas de conseguir un resultado final. Los procedimientos son a menudo establecidos con el fin de satisfacer requerimientos de control y deben ser seguidos cuidadosamente para proporcionar el nivel de control requerido.

Las guías y procedimientos son frecuentemente implementaciones específicas de las políticas y estándares. Son necesarios cuando varían los equipos, el software y el entorno proporciona diferentes vías para satisfacer los requerimientos de control. Las guías contemplan sugerencias y no son estrictas. Por el contrario, los procedimientos deben ser seguidos escrupulosamente y estar sujetos a permanente revisión por parte de la dirección.

Hasta este punto, se ha mantenido en un segundo plano el enfoque técnico. Indudablemente, cualquier planificación enfocada a la protección de la información finalmente desemboca en la gestión y administración de mecanismos de seguridad tales como contraseñas, control de accesos y recursos, cifrado de datos, alarmas y notificaciones a los administradores, etc. No obstante, la información y no la tecnología debe ser el punto central de trabajo.

La solución técnica adoptada es un hecho puntual, mientras que la naturaleza y velocidad de los cambios tecnológicos y organizacionales nos llevan irremediablemente a una protección de la información dinámica y flexible. Las características y objetivos deben ser revisados y modificados tan pronto como los cambios lo requieran.

## *Responsabilidades de la seguridad*

Para la gestión adecuada de todos estos recursos, de forma que se garantice la seguridad del sistema, es necesario disponer de una estructura funcional, en base a la asignación de responsabilidades, que se puede estructurar en:

- **Alta Dirección**. Establece y mantiene los presupuestos, personal y procedimientos para asegurar el cumplimiento de la política y su adecuación a los costes.
- **Administradores de seguridad de sistemas**. Implementan estándares y aseguran su cumplimiento para cada sistema sobre el que tienen asignada responsabilidad.
- **Usuarios finales**. Comprende a todas las personas que tienen acceso a los sistemas corporativos y son requeridos en el cumplimiento de los procedimientos recogidos en la política de seguridad.

## *Privacidad de la información*

La mayoría de las personas tiene una idea intuitiva de lo que la privacidad viene a significar, pero puede ser contemplada desde dos vertientes:

1. Un derecho a permanecer invulnerable a los intrusos.
2. Un derecho a decidir qué información personal debe ser comunicada y a quién.

Sin embargo, una compañía debe velar por sus intereses. Alguien puede necesitar, por ejemplo, recuperar la correspondencia de sus empleados en ciertos casos legítimos:

1. Localizar mensajes perdidos.
2. Asistir a los empleados, a petición suya o con su consentimiento, en el desarrollo de sus tareas cuando se encuentran fuera del puesto de trabajo.
3. Analizar la efectividad del sistema de correo electrónico.
4. Iniciar una investigación.
5. Asegurar que los recursos están siendo utilizados con fines laborales y no con fines personales.

## *Razones de la inseguridad*

### En Internet

1. Origen de Internet: Abierta, cooperativa.

   Las implicaciones que tiene el propio concepto de Internet hacen que la red sea inevitablemente insegura. Entre la gran cantidad de usuarios que acceden a la red sin que tenga lugar la aplicación de restricciones exhaustivas, existe una alta probabilidad de que alguno de ellos sea malintencionado y que se aproveche del carácter abierto de Internet para llevar a cabo todo tipo de acciones que perjudican el resto de usuarios.

2. Web: Acceso masivo a personas sin conocimientos. (Deseable, pero peligroso)

   La ventaja que supone el hecho de que Internet esté "al alcance de todos" constituye, paradójicamente, un gran inconveniente. Un usuario que ignora el funcionamiento de elementos básicos puede constituir una amenaza de la misma envergadura (o incluso mayor) que un usuario malintencionado.

3. Nodos no administrados.

## En redes

1 Crecimiento desordenado a medida que surgen necesidades y/o recursos

   Este hecho hace que una red pueda ampliarse de forma desorganizada, dificultando la consideración de aspectos que pueden comprometer la seguridad de la misma.

2 Falta de planificación inicial

   Del mismo modo que el ítem anterior, todo tipo de falta de planificación y organización obstaculiza el hecho de tomar medidas preventivas, e incluso correctivas, en contra de las amenazas.

Obviamente, el hecho de utilizar una conexión a cualquier red en general y a Internet en particular, implica el uso de un ordenador. Por ese motivo, a las razones de inseguridad específicas tanto de las redes como de Internet mencionadas arriba hay que añadirles aquéllas relacionadas con los ordenadores que se detallan a continuación.

## En ordenadores

1. Instalaciones "por defecto" no pensadas para la seguridad.

   La siguiente tira cómica ilustra una crítica a las instalaciones por defecto y sus consecuencias de cara a la inseguridad:


2. Facilitar al máximo todo al usuario, automatización. Seguridad vs. Comodidad.

   En ocasiones se sacrifica la seguridad de un sistema para hacerlo más cómodo o más accesible para el usuario. Sería necesario un análisis detallado de la situación para darle el peso más conveniente a Seguridad y Comodidad, pues no es posible prescindir completamente de ninguna de las dos.

3. Complejidad de los sistemas, interacciones no previstas.

   Las relaciones entre los elementos de un sistema son muy numerosas en cantidad y diversidad. La inmensidad del sistema hace muy complicado prever el efecto de todas sus interacciones, de muchas de las cuales ni siquiera se tiene conocimiento de su existencia.

4. Sistemas "distribuidos"

   Las consecuencias de "distribuir" tienen que ver también con la complejidad de los sistemas y de sus interacciones.

5. Desconocimiento en temas de seguridad por parte de los programadores.

   Gran cantidad de desarrolladores se dedican fundamentalmente a programar con el objetivo de conseguir únicamente la funcionalidad que les ha sido solicitada, sin tomar en consideración aspectos relacionados con la seguridad bien por desconocimiento o bien por cuestiones de tiempo o mera falta de

profesionalidad.

### En usuarios

1. Renuncia por parte de los usuarios a aprender como funcionan las cosas.

   La mayoría de usuarios no tienen el más mínimo interés en conocer el funcionamiento del sistema que usan en sus tareas diarias. En general consideran que invierten suficiente esfuerzo en llegar a saber cómo usar el sistema, a lo que se añade la opinión de que las cuestiones internas del mismo están fuera del alcance de su conocimiento y piensan que de ello ya se encargan otras personas especializadas en el tema.

2. Credibilidad y buena voluntad del usuario.

3. Falta de concienciación.

   Muchas personas tienen la creencia de que "esto no tiene por qué pasarme a mí…"; hasta que un día "pasa", y en ese caso las consecuencias son catastróficas por no haber tomado las medidas pertinentes.

## *Consecuencias*

### Sobre los ordenadores

A continuación se listan una serie de consecuencias de la inseguridad generada por los motivos detallados en el apartado anterior sobre los ordenadores:

1 Denegación de servicio.
2 Eliminación de evidencias.

3 Ejecución no permitida.
4 Acceso a datos ajenos.
5 Modificación de datos ajenos.
6 Ejecución arbitraria.
7 Control total.

## Sobre los usuarios

Los usuarios también se ven claramente afectados por la falta de seguridad en sus sistemas, lo cual suele producir frustración y numerosas de pérdidas que no son únicamente de tipo material.

1. Pérdida de tiempo, sistemas más lentos.
2. Pérdida de trabajo (datos).
3. Pérdidas económicas (robos).
4. Coste de protección y reparación.
5. Deterioro de sistemas vitales.

## *Tipos de problemas*

Cuando se piensa acerca de la vulnerabilidad, se considera una debilidad en un diseño de seguridad, algún defecto que se puede explotar para derrotar a la defensa. En tiempos medievales, la vulnerabilidad de un castillo se basaba en que pudiesen sitiarlo. En términos modernos, un chaleco a prueba de balas podía ser vulnerable a una bala especial, o que tenga como objetivo alguna parte del cuerpo no protegida por el chaleco. De hecho, toda medida de seguridad que se ha inventado ha sido evitada prácticamente en el momento de su creación.

La *vulnerabilidad de un ordenador* es un defecto de seguridad del sistema del computador. La seguridad es la estructura de apoyo que previene el acceso no autorizado al ordenador. Cuando la vulnerabilidad se rompe, la persona que esté

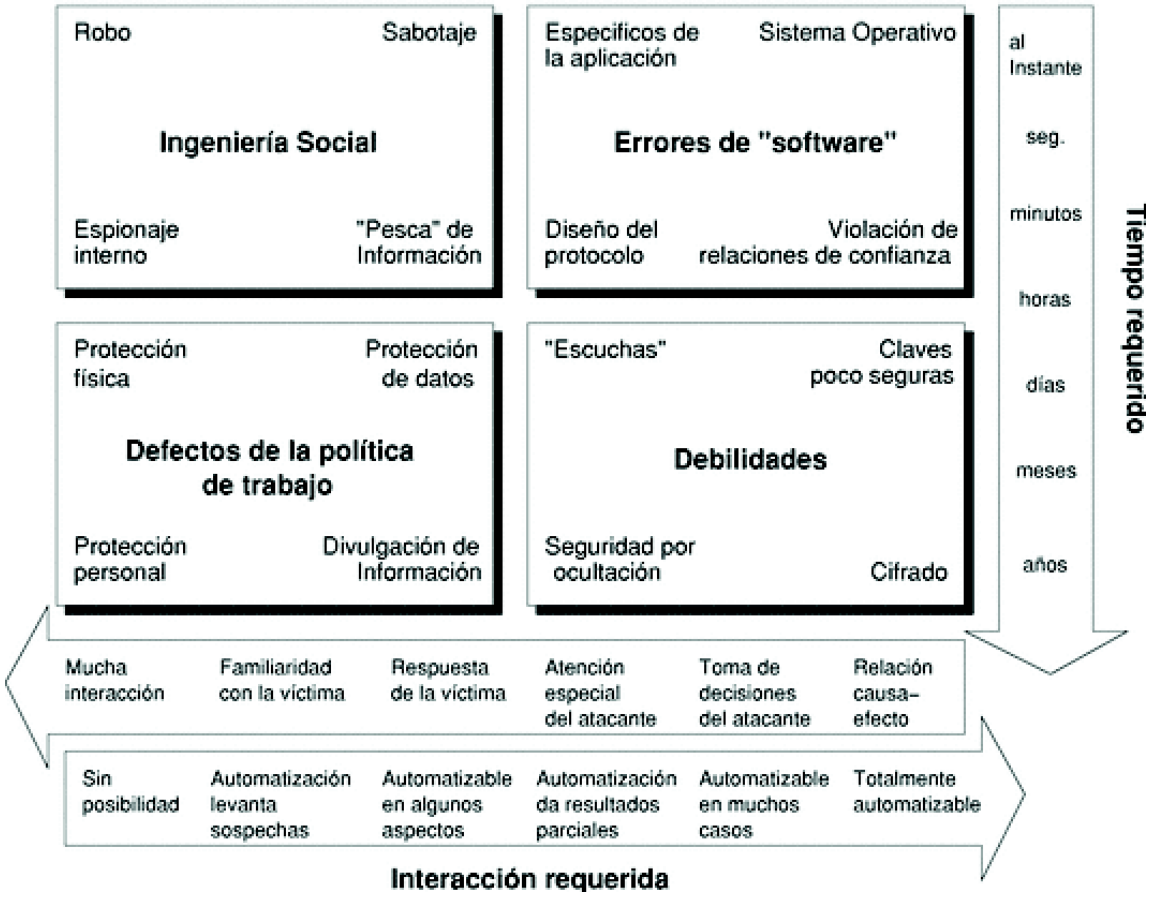
usando la vulnerabilidad ganará una influencia adicional sobre el ordenador que le puede permitir comprometer la integridad del sistema.

Los ordenadores tienen una gama de diferentes defensas, desde contraseñas hasta permisos sobre ficheros. Se puede hacer una clasificación de vulnerabilidades, de forma que sea posible explicar el peligro y la función de cada tipo, y se puedan determinar las mejoras de los caminos de acceso.

Existen cuatro tipos básicos de vulnerabilidades, las cuales hacen referencia dos factores: el que es específico al objetivo de la vulnerabilidad en términos del ordenador o la persona, y el otro es la rapidez con la que actúa la vulnerabilidad. Esta clasificación se puede observar en la tabla:

| | **Afecta a la Persona** | **Afecta al Ordenador** |
|---|---|---|
| **Instantánea** | Ingeniería social | Error de sw |
| **Requiere un tiempo de duración** | Defectos de la política de trabajo. | Debilidades |

El siguiente mapa de vulnerabilidades crea una manera visual de visualizar las situaciones de seguridad que cualquiera se puede haber encontrado y su relación con los cuatro tipos de vulnerabilidades:




## *Crónica del crimen (o delitos en los sistemas de información)*

### Delitos accidentales e incidentales

Los delitos cometidos utilizando la computadora han crecido en tamaño, forma y variedad. En la actualidad, los delitos cometidos tienen la peculiaridad de ser descubiertos en un 95% de forma casual. Se puede citar a los principales delitos hechos por ordenador o por medio de ordenadores estos son:

1. fraudes
2. falsificación
3. venta de información

### Virus informático

El virus informático es un programa elaborado accidental o intencionadamente,

que se introduce y se transmite a través de discos o de la red de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas informáticos. Ejemplo: el virus llamado Viernes 13 o Jerusalén, que desactivó el conjunto de ordenadores de la defensa de Israel y que actualmente se ha extendido a todo el mundo.

Las primeras referencias de virus con fines intencionales surgieron en 1983 cuando Digital Equipament Corporation (DEC) empleó una subrutina para proteger su famoso procesador de textos Decmate II, que el 1 de abril de 1983 en caso de ser copia ilegal borraba todos los archivos de su unidad de disco.

Al realizar la auditoría se debe estudiar con mucho cuidado lo que significan los virus. Y conocer los diferentes tipos como:

1. Residentes
2. De acción directa
3. De sobreescritura
4. De boot
5. De macro
6. De enlace o directorio
7. Encriptados
8. Polimórficos
9. Multipartitos
10. De fichero
11. De compañía
12. De FAT
13. Gusanos
14. Troyanos
15. Bombas lógicas
16. Virus falsos

Pero como principal punto de partida se debe observar que el sistema:

1. No tenga copias ilegales o piratas.
2. Que no exista la posibilidad de transmisión de virus al realizar conexiones remotas o de redes.
3. El acceso de unidades de disco flexible sea restringido solo a quienes las necesitan.

Es muy importante manejar con discreción los resultados que se obtengan de los aspectos de seguridad, pues su mala difusión podría causar daños mayores. Esta información no debe ser divulgada y se la debe mantener como reservada.

## *Evolución*

1. Ataques "personales" para controlar determinados recursos concretos.
2. Ataques aleatorios para usar recursos como puente. Uso de recursos de disco.
3. Ataques automáticos para realizar DoS distribuidos o bots de IRC.
4. Ataques automáticos sin objetivo particular.
5. Gusanos.
6. Gusanos que buscan salidas de "spam".
7. Ataques tipo "phising" para robo de datos bancarios.
8. Creación de redes de "zombies" para envío masivo de spam/phising.
9. Virus orientados al robo de datos bancarios.

## *Tipos de usuarios*

### Hacker

1. El mundo está lleno de problemas fascinantes esperando a ser resueltos.
2. Jamás se debería resolver un problema dos veces.
3. El trabajo aburrido y repetitivo es malo.
4. La libertad es buena.
5. La actitud no es sustituta de la competencia.

### Otros

1. Nerd

2. Geek
3. Luser
4. Wannabe
5. Crackers
6. Script-kiddies

## *Conceptos básicos*

### Fallos típicos en Sistemas Operativos

1. Cesión de privilegios indiscriminada.
2. Variables de entorno.
3. Enlaces simbólicos.
4. Condiciones de carrera.
5. Desbordamiento.
6. Relaciones de confianza.

### Fallos típicos en clientes

1. Automatización excesiva. Ejecución automática de aplicaciones locales con datos externos.
2. Ejecución automática de código externo.
3. Scripts incluidos en todo tipo de documentos. (Ofimática, HTML, e-mail)
4. Aumento de importancia por el incremento de servicios vía Web. XSS/CSS

## *Medidas de seguridad*

## A nivel de usuario

1. Conocimiento del sistema.
2. Verificación de integridad.
3. Protocolos cifrados.
4. Revisión de registros (”logs”).
5. Paranoia. Evitar ejecución de código externo. Aplicaciones “seguras”.
6. Passwords seguros




1. Sistemas con niveles de acceso. Trabajar sin privilegios especiales. (p.e. MacOS X)
2. Eliminar servicios. (p.e. SNMP)
3. Reglas de acceso, Cortafuegos.
4. Actualizaciones del sistema.
5. Programación segura.

## A nivel de administración

1. Políticas de seguridad.
2. Diseño estricto de la red y los servicios.
3. Barreras de acceso.
4. Copias de seguridad, recuperación ante desastres

**Cortafuegos**

| **Ventajas** | **Inconvenientes** |
|---|---|
| Control de acceso externo. | Dificultad de configuración correcta. |
| Limita alcance de problemas de seguridad en servicios/redes locales. | Dificultad de instalación de nuevos servicios. |
| Limita la posibilidad de utilizar sistemas comprometidos para atacar a terceros. | Problemas con protocolos que usan puertos aleatorios. |
| Limita la posibilidad de extraer información. | Ralentización. |
| | Importancia relativa en máquinas sin servicios y con accesos controlados. |

## *Etapas para Implementar un Sistema de Seguridad*

Para dotar de medios necesarios para elaborar su sistema de seguridad se debe considerar los siguientes puntos:

1. Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.
2. Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información
3. en la organización a nivel software, hardware, recursos humanos, y ambientales.
4. Elaborar un plan para un programa de seguridad. El plan debe elaborarse contemplando:

## Plan de Seguridad Ideal (o Normativo)

Un plan de seguridad para un sistema de seguridad integral debe contemplar:

1 El plan de seguridad debe asegurar la integridad y exactitud de los datos

2 Debe permitir identificar la información que es confidencial

3 Debe contemplar áreas de uso exclusivo

4 Debe proteger y conservar los activos de desastres provocados por la mano del hombre y los actos abiertamente hostiles

5 Debe asegurar la capacidad de la organización para sobrevivir accidentes

6 Debe proteger a los empleados contra tentaciones o sospechas innecesarias

7 Debe contemplar la administración contra acusaciones por imprudencia

8 Un punto de partida será conocer como será la seguridad, de acuerdo a la siguiente ecuación.

$$\text{SEGURIDAD} = \frac{\text{Riesgo}}{\text{Medidas preventivas y correctivas}}$$

Donde:

*Riesgo* (roles, fraudes, accidentes, terremotos, incendios, etc)

*Medidas preventivas* (políticas, sistemas de seguridad, planes de emergencia, plan de resguardo, seguridad de personal, etc)

## Etapas para Implantar un Sistema de Seguridad en Marcha

Para hacer que el plan entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguiente 8 pasos:

1. Introducir el tema de seguridad en la visión de la empresa.
2. Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
3. Capacitar a los gerentes y directivos, contemplando el enfoque global.
4. Designar y capacitar supervisores de área.

5. Definir y trabajar, sobre todo, las áreas donde se pueden lograr mejoras relativamente rápidas.
6. Mejorar las comunicaciones internas.
7. Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
8. Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

## Beneficios de un Sistema de Seguridad

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que el la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

1. Aumento de la productividad.
2. Aumento de la motivación del personal.
3. Compromiso con la misión de la compañía.
4. Mejora de las relaciones laborales.
5. Ayuda a formar equipos competentes.
6. Mejora de los climas laborales para los RR.HH.

# *La Administración De La Seguridad*

## Objetivos

La administración de la seguridad es una función indispensable para el normal funcionamiento de cualquier organización y surge como consecuencia de los aspectos de control de las actividades de gestión.

Los objetivos de esta función son los de asegurar la existencia y el mantenimiento de los niveles de seguridad en:

1. Hardware, software.

2. Personal.
3. Comunicaciones y redes de comunicaciones.
4. Entorno físico.

La administración de la seguridad representa un coste no despreciable en una empresa. Asimismo, puede ser interpretado como restricción a las personas en la forma de hacer sus trabajos. Por ello, es un objetivo primordial reconciliar las labores de administración de la seguridad con aquellas propias de la gestión.

## Funciones

Entre sus funciones están comprendidas las siguientes:

1. Gestión del sistema de seguridad.
2. Gestión de la política de seguridad.
3. Adaptación a las prescripciones legales.
4. Gestión de las tareas de recuperación.
5. Gestión de servicios de seguridad.
6. Determinación y asignación de la protección de la seguridad para el servicio.
7. Asignación y mantenimiento de las reglas para la selección de mecanismos específicos de seguridad para proporcionar el servicio de seguridad requerido.
8. Negociación (local y remota) de los mecanismos de seguridad disponibles.
9. Gestión de mecanismos de seguridad.
10. Gestión de claves.
11. Gestión de criptografía.
12. Gestión firma digital.
13. Gestión de controles de accesos.
14. Gestión de la integridad de datos.
15. Gestión de la autentificación.
16. Gestión de relaciones con TTPs.
17. Gestión de la auditoría de seguridad.
18. Gestión de los eventos a ser registrados.
19. Activación o desactivación de auditorías.
20. Edición de informes.

21. Verificación de adopción de medidas correctoras.
22. Concordancia en la implementación de la tecnología con la política de seguridad adoptada.

En la práctica, estas labores de gestión se materializan en:

1. Controles sobre seguridad crítica.
2. Control sobre los procesos.
3. Conexiones seguras.
4. Alarmas en tiempo real para detectar intrusos, allí donde sea apropiado.

## *Dominios De Seguridad*

El nivel de seguridad en la información es adaptado dinámicamente a una situación dada. Esto nos introduce en el concepto de Gestión Dinámica de los Sistemas de Información y a la necesidad de ser capaces de establecer dominios, en los cuales la seguridad de la información es aplicada homogéneamente.

Los dominios son agrupaciones de usuarios compartiendo algunas de sus funciones. Para algunas actividades, operan como grupos cerrados virtualmente, pero tiene la posibilidad de interoperar con otros dominios, mediante unos requerimientos mínimos, sin pérdida de seguridad o transparencia en el uso.

La noción de dominio de seguridad es aquí importante por dos razones:

1. Es usado para describir la forma en que la seguridad es gestionada y administrada.
2. Puede ser usado como un elemento constructivo en el modelo de seguridad, que involucra distintos elementos bajo distintas autorizaciones en seguridad.

Ejemplos de dominios de seguridad son:

1. Acceso a elementos
2. Operaciones relativas a labores específicas de gestión.

3. Enlaces y comunicaciones.

La política de seguridad recoge los siguientes aspectos concernientes a los dominios de seguridad:

1. Qué se entiende por seguridad en un dominio.
2. Las reglas sobre las cuales se asienta la obtención del dominio.
3. Las actividades sobre las que se aplica.
4. Las reglas de aplicación en las relaciones con otros dominios generales.
5. Las relaciones para su aplicación con otros dominios de seguridad particulares.

## *Administración de los dominios de seguridad*

La gestión y administración de los dominios de seguridad está basada en las similitudes existentes entre dominios. En cuanto a la gestión de relaciones entre dominios, se establece un acuerdo con el fin de obtener el nivel adecuado de seguridad. Los mecanismos actuales que articulan esta administración recogen los siguientes requerimientos:

1. Mecanismos para la gestión, procedimientos y controles entre dominios donde intervenga una TTP.
2. Procedimientos para la creación de dominios, su gestión y control.
3. Desarrollo de una arquitectura común para el trabajo entre dominios.

## *Claves De Seguridad*

Las firmas digitales conllevan la implementación de especificaciones relacionadas con las tres fases de una gestión de claves: incorporación de usuarios, distribución y certificación de claves y mantenimiento operacional (revoques, listas negras, destrucción), que debe ser acordada y aceptada.

En la aplicación de seguridad a cualquier proceso o mensaje, son de especial interés los siguientes aspectos:

1. Aspectos legales e implicaciones (incluyendo aspectos sociales)
2. Definición e identificación del servicio de seguridad a aplicar.
3. Los mecanismos que lo soportan.
4. Los algoritmos y protocolos.

## Servicio de gestión de claves

Los aspectos más generales que se pueden identificar en relación a un servicio de gestión de claves pueden ser:

- *Definición de responsabilidades y obligaciones* para aquellos servicios que proporcionan seguridad en la integridad de comunicaciones y aquellos que proporcionan confidencialidad.
- *Desarrollo de prácticas para la generación, distribución, almacenamiento y destrucción de claves*, con los fines de integridad y confidencialidad, en entornos que poseen diferentes niveles de seguridad.
- '*Escrow Services*'. Algunos de los secretos pueden ser de vital importancia, y pueden requerir ser distribuidos entre partes seguras, de tal manera que ninguna de las partes conozca la totalidad del secreto sino nada más que una mínima parte. Para la completar la totalidad del secreto todas las partes deben aportar su contribución.
- *Mecanismos y criterios de asesoramiento para discernir la conveniencia de los solicitantes de servicios de TTPs*. No todos los potenciales usuarios de una TTP pueden tener las características necesarias (status legal, viabilidad financiera, etc...)
- *Integridad y firma digital.*
- *La relación entre las funciones de gestión de claves, gestión de directorios y certificación* necesita ser clara.
- *Celeridad en la emisión de firma, verificación de veracidad de la firma*, revisión periódica de la veracidad de los signatarios existentes.
- *Eliminación de firmas de la "lista activa" e iniciación de una auditoría para confeccionar una "lista de usos ilegales"*. Esto conlleva una interfase de gestión de claves -gestión de certificaciones.
- *Relaciones de privacidad*.

- *Gestión de los dominios* en los cuales son válidas las claves de confidencialidad. Identificación de los sujetos autorizados en el dominio, distribución de claves a los usuarios autorizados (personas y procesos automáticos).
- *La TTP debe definir dominios por su capacidad de gestionarlos*. Si no pudiera atender su gestión, otra TTP debe soportar la gestión del dominio.
- *Establecimiento del nivel de seguridad del dominio sobre el cual se van a emplear las claves de confidencialidad*. Clasificar desde usuarios vetados al uso, usuarios con acceso físico y lógico controlado hasta usuarios liberados.

Los servicios de seguridad que implementados van a permitir contrarrestar las amenazas previamente identificadas, son los siguientes:

1. *Confidencialidad de datos.*
2. *Integridad del mensaje y del contenido.*
3. *Autenticación de entidades, firma digital.*
4. *No repudio - acuse de recibo.*
5. *Control de acceso*

En la tabla siguiente se relacionan las amenazas, los servicios de seguridad y el objeto protegido.

| ***Amenaza*** | ***Servicio de Seguridad*** |
|---|---|
| Divulgación no autorizada de la información | *Confidencialidad de datos* |
| Modificación no autorizada de la información | *Integridad del mensaje y del contenido* |
| Enmascaramiento | *Autenticación de entidades* |
| Repudio del mensaje de origen o del acuse de recibo | *No repudio* |
| Acceso no autorizado a recursos | *Control de acceso* |
| Denegación de servicio | *Control de acceso* |

# Riesgos

## *Confidencialidad De Los Datos*

Su propósito es impedir que nadie que no sea el receptor pueda leer el contenido de un mensaje y, por lo tanto, tener la disponibilidad de divulgarlo. Hablando de un sistema de transmisión de mensajes, se trata de impedir que la información transmitida sea interceptada (leída) por persona no autorizada, y por lo tanto conocer su contenido.
Se trata en definitiva de garantizar que la información sólo pueda ser leida por el usuario o usuarios a los que está dirigida. La confidencialidad por tanto, se puede aplicar en:

1. Información del destinatario.
2. Texto completo.
3. Parte del texto.

La técnica más moderna existente hoy en día que se puede aplicar como una solución muy eficaz, es la **CRIPTOGRAFÍA**, que mediante algoritmos matemáticos y aplicación de claves o contraseñas, y utilizando medios software o hardware, permite transformar el contenido del texto en un conjunto de caracteres no entendibles.

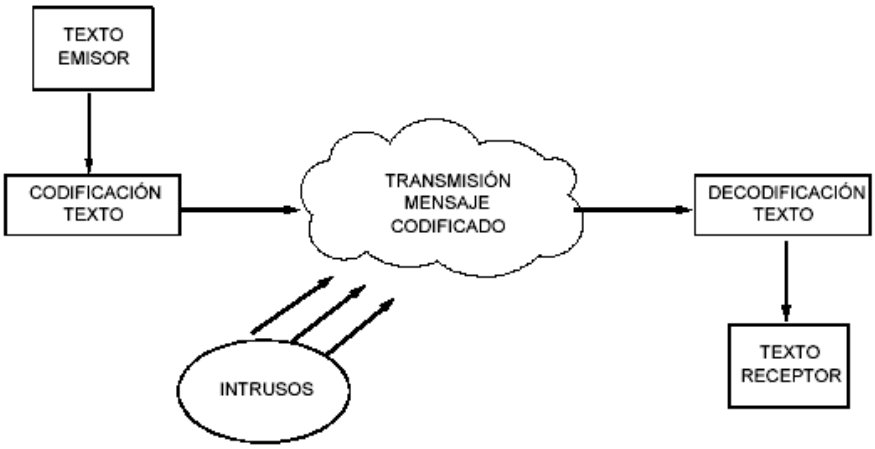
La seguridad se tiene en que se requiere el conocimiento y acuerdo mutuo entre el receptor del mensaje y el emisor, de las claves y utilizar el mismo medio software o hardware para poder cifrar y descifrar el mensaje. Se puede decir entonces que se ha establecido una comunicación segura.

## *Integridad Del Mensaje Y Del Contenido*

Se garantizará a la entidad receptora que el mensaje o información que está recibiendo es exactamente el mismo que le envió la entidad origen. Al mismo tiempo, el receptor tendrá la seguridad de que no ha habido, sobre la información original emitida, ninguna modificación, ni pérdida, ni contenido adicional antes de su recepción.

Para poder lograrlo, nos basamos igualmente en la tecnología de la **CRIPTOGRAFÍA**, pero pudiendo usar esta vez la clave pública y/o la clave privada. Con la utilización de la clave pública, basta que emisor y receptor la conozcan. Si se utiliza ambas, la clave pública y privada, deberá existir algún mecanismo adicional que permita a la entidad

origen transferir la clave secreta al receptor.




Se puede decir que aparte de una comunicación segura, se ha logrado que no haya manipulación del texto en el trayecto emisor - receptor.

## *Autenticación De Entidades*

Garantizará a la entidad receptora que el mensaje que llegó de la entidad emisora, pertenece a quién dice ser. Esto se puede realizar mediante lo siguiente:

1. **AUTENTICACION DE ENTIDAD SIMPLE**: Puede tratarse de la entidad origen de los datos o de la entidad destino.

2. **AUTENTICACION DE ENTIDADES MUTUA**: Ambas entidades comunicantes se autentican una a la otra.

La autenticación debe de realizarse por medio de mecanismos de cifrado y de **FIRMA DIGITAL**, no por un simple mecanismo de intercambio de 'passwords' o de mensajes cifrados del tipo pregunta / respuesta, que son más vulnerables. El empleo de este mecanismo de intercambio de autenticación con tecnologías de certificados puede utilizarse para proporcionar una capacidad de autenticación distribuida de modo que sea posible un tratamiento seguro de la información y una mayor seguridad en la conectividad entre emisor / receptor. Pueden utilizarse diversos mecanismos conjuntamente, que garanticen la Integridad, Confidencialidad, Autenticación y No

Repudio en la transmisión de mensajes vía Correo Electrónico.

## *No Repudio - Acuse De Recibo*

Proporcionará al emisor/receptor de un mensaje, una prueba irrefutable de que el contenido recibido fue el mismo que el del mensaje enviado por el emisor, y que por lo tanto no ha habido modificación del mismo desde el emisor, y se aceptará el mensaje. Para poder proporcionar una confirmación de **NO REPUDIO**, el procedimiento sería el siguiente:

1. El **emisor del mensaje** solicita notificación afirmativa o negativa de la recepción
2. con autenticación no repudiable.
3. El **receptor del mensaje**, emite notificación afirmativa o negativa con no repudio,
4. utilizando el procedimiento de autenticación.
5. El **emisor del mensaje**, cuando recibe la notificación, utiliza los procedimientos
6. de verificación para asegurarse que el emisor de la notificación es el deseado.
7. La presencia de un **CERTIFICADO DE NO REPUDIO**, prueba que el receptor aceptó la notificación de no repudio solicitado por el emisor.

Este servicio protege al emisor/receptor de un documento, de cualquier intento por parte del origen/destino de negar su envío/recepción en su totalidad o en parte del contenido del mismo. Asimismo pretende **dar una validez legal a un documento**, ya que requiere que una persona se responsabilice de contenido del documento estampando su firma digital en él. Estos servicios pueden ser de dos clases:

- Con **PRUEBA DE ORIGEN**. El receptor tiene prueba, demostrable ante terceros, del origen de los datos recibidos.
- Con **PRUEBA DE ENTREGA**. El emisor tiene prueba de que los datos han sido entregados al receptor deseado.

## *Acuse de recibo*

Todas las funciones descritas anteriormente, están dentro de la confirmación de entrega extremo a extremo. Su propósito es poder probar que el contenido del mensaje enviado por la entidad origen fué recibido por la entidad destino. Esta función es similar al concepto de **ACUSE DE RECIBO**.

## *La necesidad del acuse de recibo*

La posición del emisor puede resultar difícil ya que el receptor puede alegar que no recibió mensaje alguno o lo que es lo mismo, negar su existencia. Al emisor sólo le puede quedar la seguridad de que el receptor no le puede alterar el contenido del mensaje. Para que el emisor esté seguro de que el mensaje ha llegado a su destino, aparece la figura del **ACUSE DE RECIBO**. Este se produce en un mensaje del receptor al emisor, de haberlo recibido.

Para que el ACUSE DE RECIBO sea operativo, se debe establecer un plazo de tiempo mínimo en que se produzca el envío del mismo. Es en este punto cuando se invierten las posiciones, pues el receptor no puede justificar que envió el acuse de recibo, se estaría dentro de un círculo cerrado de envíos y contraenvíos de acuses de recibo.

Para solucionar este problema, **se impone la figura de una tercera parte**, siendo a través de su actuación la forma de que se logre que todas las partes tengan prueba plena del origen, contenido y destino de cualquier mensaje que se haya emitido o recibido.

## *Control De Acceso*

Los servicios de seguridad de control de acceso tienen por objeto garantizar que sólo acceden a la información y a los diversos recursos del sistema aquellos usuarios que tienen los derechos para ello. Los mecanismos a utilizar van desde una adecuada gestión de claves de acceso o *passwords* hasta las más complejas técnicas de cortafuegos o *firewall* como se verá más adelante.

## *Medición*

La calidad no es una opción o una característica más, es un concepto de vital importancia para cerciorarnos que todo se hace de la mejor forma posible, es por ello que no se trata como un punto cualquiera más a tratar sino como una obligación que determina el éxito.

Para controlar la calidad de cualquier cosa es necesario tener nociones de referencia que nos puedan cuantificar el valor de lo que se realiza, entiendo valor en un sentido muy amplio, no exclusivamente en el económico. Por lo tanto tener mecanismos para medir el trabajo es la única forma de asegurarse el control de calidad.

Las normas ISO (International Organization for Standarization) nos ofrecen métricas y estándares de actuación cuya finalidad es la coordinación de las normas nacionales, en consonancia con el Acta Final de la Organización Mundial del Comercio, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir con unos estándares comunes para el desarrollo y transferencia de tecnologías. De esta manera, aquellos sujetos que obtengan certificaciones de cumplir estas normas será síntoma de un buen control de calidad otorgando prestigio al trabajo realizado, así pues, es un tema muy importante a tratar por un auditor.

En nuestro caso, se va a tratar la **ISO 27001**:
Es la norma principal de requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones.
Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última.
En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO17799:2005 (futura ISO27002), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.
En España, esta norma aún no está traducida.

# Soluciones

***Auditoría de seguridad de sistemas de información***

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores. La Auditoría Informática se puede definir como "el conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático con el fin de constatar si sus actividades son correctas y de acuerdo a las normativas informáticas y generales prefijades en la organización".

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

La Auditoría Informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información, ésta es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo: informática, organización de centros de información, hardware y software.

La Auditoría del Sistema de Información en la empresa, a través de la evaluación y control que realiza, tiene como objetivo fundamental mejorar la rentabilidad, la seguridad y la eficacia del sistema mecanizado de información en que se sustenta.

Los aspectos relativos al control de la Seguridad de la Información tiene tres líneas básicas en la auditoria del sistema de información:

- Aspectos generales relativos a la seguridad. En este grupo de aspectos habría que considerar, entre otros: la seguridad operativa de los programas, seguridad en suministros y funciones auxiliares, seguridad contra radiaciones, atmósferas agresivas, agresiones y posibles sabotajes, seguridad físics de las instalaciones, del personal informático, etc.

- Aspectos relativos a la confidencialidad y seguridad de la información. Estos aspectos se refieren no solo a la protección del material, el logicial, los soportes de la información, sino también al control de acceso a la propia información (a toda o a parte de ella, con la posibilidad de introducir modificaciones en la misma).

- Aspectos jurídicos y económicos relativos a la seguridad de la información. En este grupo de aspectos se trata de analizar la adecuada aplicación del sistema de información en la empresa en cuanto al derecho a la intimidad y el derecho a la información, y controlar los cada vez más frecuentes delitos informáticos que se cometen en la empresa. La propia dinamicidad de las tecnologías de la información y su cada vez más amplia aplicación en la empresa, ha propiciado la aparición de estos delitos informáticos.

  En general, estos delitos pueden integrarse en dos grandes grupos: delitos contra el sistema informático y delitos cometidos por medio del sistema informático. En el primer grupo se insertan figuras delictivas tipificadas en cualquier código penal, como hurto, robo, revelación de secretos, etc..., y otro conjunto de delitos que ya no es tan frecuente encontrar, al menos con carácter general, perfectamente tipifiados, como el denominado "hurto de tiempo", destrucción de logiciales y datos, delitos contra la propiedad (material, terminales, cintas magneticas,...).

El auditor es el encargado de medir el estado de los servicios de seguridad de la organización, no obstante, para la implementación de dicha seguridad, el auditor puede recomendar técnicas o mecanismos de seguridad aplicables. Así una técnica o

mecanismo de seguridad es la lógica o algoritmo que implementa un servicio de seguridad particular en hardware y software.

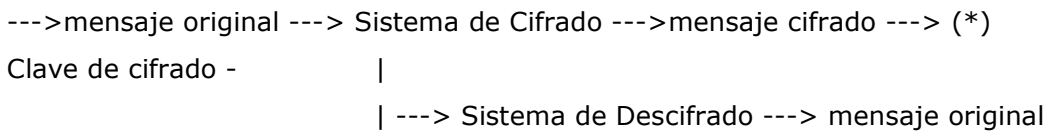
La siguiente tabla expresa la relación entre los servicios de seguridad y las técnicas o mecanismos de seguridad aplicables.

| ***Servicio de Seguridad*** | ***Técnica/Mecanismo de Seguridad*** |
|---|---|
| Autenticación de entidad | *Intercambio de autenticaciones* |
| Autenticación de datos de origen | *Cifrado*<br>*Firma digital*<br>*Función de comprobación criptográfica* |
| Control de acceso | *Lista de control de acceso*<br>*Cortafuegos* |
| Confidencialidad orientada a la conexión | *Cifrado*<br>*Etiquetas de seguridad* |
| Confidencialidad no orientada a la conexión | *Cifrado*<br>*Etiquetas de seguridad* |
| Confidencialidad del flujo de tráfico | *Cifrado*<br>*Relleno del tráfico*<br>*Etiquetas de seguridad* |
| Integridad orientada a la conexión | *Función de comprobación criptográfica*<br>*Funciones hash y cifrado* |
| Integridad no orientada a la conexión | *Función de comprobación criptográfica*<br>*Funciones hash y cifrado*<br>*Firma digital* |
| No repudio, origen | *Firma digital*<br>*Teceras Partes de Confianza* |
| No repudio, destino | *Firma digital*<br>*Terceras Partes de Confianza* |

## *Técnicas de criptografía*

El uso de la criptografía o cifrado puede proporcionar la confidencialidad, tanto de los datos como del flujo/tráfico de información, y puede formar parte o complementar otros mecanismos de seguridad. Aunque la criptografía ha sido utilizada desde muy antiguo desde la aparición de los ordenadores ha adquirido una mayor relevancia, al

facilitarse su uso con estas máquinas.
El sistema genérico es el siguiente:




Los algoritmos de cifrado pueden ser reversibles o irreversibles. Existen dos clasificaciones generales de algoritmos reversibles:

1. *Sistema convencional o simétrico*; donde la clave de cifrado y de descifrado es la misma.
2. *Sistema asimétrico o de clave pública*; en el que existen dos claves, una pública y otra privada. El mensaje se cifra utilizando una y se descifra utilizando la otra y el conocimiento de una de las claves no implica el conocimiento de la otra.

Los algoritmos de cifrado irreversible pueden o no usar una clave. Si usan una clave ésta puede ser pública o secreta.

## *Cifrado y descifrado*

Un método de cifrado, bien sea simétrico o asimétrico, no debe pretender abordar un planteamiento de inviolabilidad absoluta; se busca que el coste de su descifrado 'desleal' a través de un mecanismo externo al proceso de comunicación sea muy costoso, a ser posible en varios ordenes de magnitud, tanto en tiempo como en recursos necesarios.

*ALGORITMO DES (Data Encryption Standard)*. Desarrollado por IBM en 1.977, se basa en un algoritmo que funciona de forma diferente según una palabra clave que se mantiene en secreto, conocida sólo por emisor y receptor. El mensaje M del emisor es codificado por el algoritmo, al que se le introduce como datos de entrada la palabra clave K y el mensaje M; de esta forma obtenemos:

AlgoritmoE(K,M) -- se genera --> C, que es lo que viaja por la Red.
El receptor usando el algoritmo y los datos que conoce, es decir, la clave K y la información que le llega C, obtiene de nuevo el mensaje en claro M.
AlgoritmoR(K,C) -- obtiene --> M.

Los algoritmos usados se basan en operaciones de permutaciones de bits que se realizan de forma muy rápida en los ordenadores; pero muy difíciles de detectar sin conocer la palabra clave K. El problema de mantener una protección con este tipo de algoritmos de clave secreta es la necesidad de tener muchas palabras secretas (tantas como usuarios diferentes con los que se va a comunicar), siendo difícil establecer un sistema de cambio de clave o *password* cada vez que se sospeche que ha sido descubierta.

*ALGORITMO DE CLAVE PÚBLICA (RSA: Rives-Shamir-Adleman, 1.977)*. Se basa en la teoría matemática de la factorización de grupos finitos. En concreto se selecciona como palabra clave un número producto de dos primos muy grandes, uno de los cuales constituye la clave secreta del usuario, mientras que el otro se puede declarar como público.
Existen algoritmos tales que si se les introduce un mensaje M y la clave pública, generan un dato D cifrado, que puede ser descifrado solo conociendo este dato D y la clave secreta; es decir se sigue el esquema:

M --> KPR(M)=D dato que viaja cifrado por la Red y que sólo puede ser descifrado conociendo la clave privada del receptor R al cual va dirigido el mensaje; el cual actuará usando el algoritmo con datos de entrada D y KSR, con los que obtendrá M:

D ----------> KSR(D)= M o lo que es lo mismo:
KPR(M) --->KSR(KPR(D)) = M.
Este algoritmo permite el proceso inverso ; es decir:
KSE(M) ---> KPE(KSE(M)) = M,
siendo KSE= clave secreta del emisor y KPE = clave pública de emisor.

La validez de este algoritmo se basa en que no existe función o algoritmo tal que conociendo la clave pública pueda descifrar la privada y viceversa.

## *Gestión de claves*

Se distingue dos sistemas diferentes de Gestión de Claves:

1 *de Claves Secretas*: Cuando para descifrar un algoritmo sólo es necesario conocer la clave secreta (además del algoritmo en cuestión) es preciso propagar las clave por medios diferentes al camino de comunicación a los que esa clave va a proteger.

2 *de Clave Pública*: Es conveniente enviar la clave pública a una autoridad de certificación (CA), cifrada con la clave pública de esa CA y preferiblemente firmada. Cada vez que se quiera enviar un mensaje a un usuario R, se deba solicitar de nuestra Autoridad de Certificación (CA), o de la CA correspondiente, una certificación de R. Esta operación se puede omitir sólo si se tiene otra certificación válida del usuario (se debe asegurar de que sigue siendo válida, es decir que no ha caducado por haberla modificado el receptor R).

### *Firma digital*

Se basa en el uso de técnicas criptográficas. Se puede implementar tanto con técnicas de cifrado de clave secreta, como con técnicas de cifrado de clave pública. Para evitar la necesidad de conocimiento de claves secretas, se puede elegir la utilización de claves secretas para cifrar y de claves públicas para descifrar. La posesión de una clave privada identifica a un usuario ya que ésta es sólo conocida por el propietario y sólo él puede cifrar con ella.

Todo el mundo puede verificar la identidad de un usuario descifrando con la clave pública los datos cifrados con la privada. Si son iguales la Firma es correcta, en caso contrario se rechaza. Cualquier modificación del documento, de parte de su contenido o de la firma sería detectada automáticamente. El mecanismo de firma digital define dos procedimientos:

1. Firmar una unidad de datos: Utiliza información privada (p.e. única y confidencial) del emisor. Implica tanto el cifrado de la unidad de datos como el

de la producción de un código de control criptográfico asociado a la unidad de datos, utilizando para ello la información privada del firmante como clave privada.

2. Verificar la firma de una unidad de datos: Utiliza procedimientos e informaciones públicamente disponibles, pero a partir de las cuales no se puede deducir la información privada del firmante. Implica la utilización de procedimientos e informaciones públicas para determinar qué firma se ha generado con la información privada del firmante. La característica esencial del mecanismo de firma, es que dicha firma sólo puede haber sido generada con la información privada del firmante. Por lo tanto cuando se verifica la firma, se puede probar que sólo el poseedor de la información privada puede haber generado la firma.

## *Técnicas de seguridad diversas*

**Intercambio de autenticaciones:** Algunas de las técnicas que se pueden utilizar para el intercambio de autenticaciones son:

1. Utilización de información de autenticación, como contraseñas proporcionadas por la entidad emisora y comprobadas por la entidad receptora.
2. Técnicas criptográficas.
3. Utilización de características y privilegios de la entidad.

El mecanismo puede incorporarse en un nivel para proporcionar la autenticación de entidades semejantes. Si el mecanismo no proporciona una autenticación positiva de la entidad, puede producirse un rechazo o la finalización de la conexión, además de una entrada en el programa de auditoría de seguridad y un informe al centro de gestión de la seguridad.

La selección de técnicas de autenticación dependerá de las circunstancias en que deben ser usadas. En la mayoría de los casos se necesitan utilizar con:

1. Marcado de la hora y de relojes sincronizados.

2. 'Handshakes' de dos y tres vías, para autenticación unilateral o autenticación mutua, respectivamente.
3. Servicios de no repudio, conseguidos con firma digital y mecanismos de tercera parte de confianza.

**Funciones hash:** Son funciones matemáticas sin inversa, que aplicadas a un elemento o dato que se transfiere impiden que este sea descifrado. Se utilizan para comprobar la integridad de los datos según un mecanismo por el cual se cifra una cadena comprimida de los datos a transferir mediante una función hash; este mensaje se envía al receptor junto con los datos ordinarios; el receptor repite la compresión y el cifrado posterior de los datos mediante la aplicación de la función hash y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

**Relleno del tráfico:** Los mecanismos de relleno del tráfico se pueden utilizar para proporcionar diversos niveles de protección contra los análisis del tráfico. Se trata de enviar tráfico espúreo junto con los datos válidos para que el adversario no sepa si se está enviando información o qué cantidad de datos útiles se está transfiriendo. Estos mecanismos sólo pueden ser efectivos si el relleno del tráfico está protegido con un servicio de confidencialidad.

**Etiquetas de seguridad:** Los recursos, incluyendo los datos, pueden tener asociadas etiquetas de seguridad, por ejemplo para indicar el nivel de sensibilidad. A menudo es necesario que los datos en tránsito lleven una etiqueta de seguridad apropiada. Las etiquetas de seguridad pueden ser los datos adicionales a los datos transferidos, o pueden ser implícitas, por ejemplo, por utilizar una clave específica para cifrar los datos, o por el contexto de los datos, como su origen o la ruta utilizada. Las etiquetas de seguridad explícitas deben ser claramente identificables, para que puedan ser comprobadas apropiadamente. Además, deben estar limitadas a los datos a los que están asociadas.

## *Control de accesos*

Se trata de proteger los sistemas de informacion, de accesos no permitidos.

Las medidas de seguridad en INTERNET básicamente son:

1. **LA SEGURIDAD DE ACCESOS**. Protección del acceso a nuestros sistemas informáticos y aplicaciones por personas no autorizadas.
2. **LA CONFIDENCIALIDAD DE LA INFORMACIÓN**. Evitar la divulgación, pérdida o alteración del contenido de nuestros ficheros o durante la transmisión de los mismos.

**La implantación de las medidas** de control de acceso ha de tener en consideración los siguientes aspectos:

1 Necesidades por un alto numero de accesos públicos.
2 Restringir el acceso a INTERNET a empleados de la empresa.
3 Mantener la seguridad e integridad de la información.

Véase las principales técnicas de control de accesos:

La tecnología de *Firewalls* o cortafuegos, es relativamente nueva y se ha potenciado al comprobar que una red abierta como es INTERNET ha incorporado un nuevo tipo de usuario no corporativo, y por tanto mas difícil de controlar por las medidas y reglas implantadas en los propios 'host'. Estos cortafuegos, fueron diseñados para impedir a los *Hackers* o intrusos que están utilizando INTERNET, el acceso a redes internas de las empresas. Algunos cortafuegos incluso controlan la información que se mueve por dichas redes.

Pueden ayudar asimismo a prevenir la entrada de virus encapsulados en los paquetes transmitidos con destino a la red empresarial. Se utiliza la expresión cortafuegos para designar pasarelas u otras estructuras más complejas, existentes entre la red propia de la empresa e INTERNET, con la finalidad de restringir y filtrar el flujo de información entre ambas.

Se puede definir la **Tecnología de *firewall* o cortafuegos** como el sistema que controla todo el tráfico hacia o desde INTERNET utilizando software de seguridad o programas desarrollados para este fin, que están ubicados en un servidor u ordenador independiente. Este sistema comprueba que cada paquete de datos se encamine a donde debe, desde la red INTERNET a nuestra red privada y viceversa, al mismo

tiempo que contiene la política de seguridad especificada por el Administrador del Sistema.

**Para prevenir o permitir el tráfico de red, comprueba** el *host*, la red y la puerta desde la cual el paquete es originado o destinado.

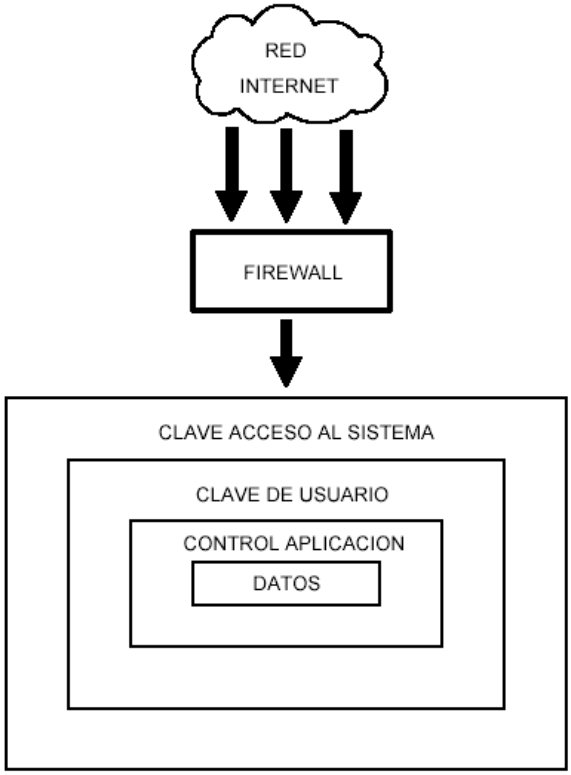
**Para conectar directamente ordenadores de un sistema corporativo en red INTERNET**, existe una aplicación que reside en el servidor para permitir un buen acceso a los servicios INTERNET facilitando al mismo tiempo la mayor seguridad que sea posible. Este servidor **comprueba**:

1. El *host* desde el cual se origina la conexión.
2. El *host* al cual la conexión es solicitada.
3. Los comandos que se producen en la conexión.

Todo ello puede facilitar al Administrador del Sistema la prevención de todas las conexiones desde *host* especificados o de redes en INTERNET. Desde esta puerta de entrada, el sistema puede también prevenirse de aquellos usuarios que a través de comandos añaden un factor de riesgo a nuestra seguridad. Se trata de prevenir, por ejemplo, la exportación de información contenida en el cortafuegos o en los servidores hacia el exterior. Mediante **aplicaciones residentes en el servidor o cortafuegos** el **Administrador del Sistema** puede:

- Definir qué **usuarios tienen palabra clave de acceso** autorizada.
- Configurar las **palabras clave de acceso que deben ser aceptadas por los diferentes hosts** configurados en nuestra red privada.
- **Controlar las cuentas** de aplicación autorizadas.
- **Evitar que la intrusión pueda cambiar la configuración de la aplicación** residente.
- **Controlar los accesos entre la red privada y el servidor** como punto de entrada.
- Llevar un **registro de todas las incidencias** que se produzcan.

BARRERAS DE PROTECCION DE LOS DATOS FRENTE A INTRUSOS INTERNET




**Ambiente propicio para el cultivo del crimen**

En la actualidad se nota que los fraudes crecen en forma rápida, incluso mayor que los sistemas de seguridad. Se sabe que en los EE.UU. se cometen crímenes computarizados denunciados o no por más de 3 mil millones de dólares.

Es importante para el auditor conocer las causas para que se cometan delitos, ya que una vez encontrado el problema se debe observar la raíz para sugerir su solución, entre las causas se puede citar, dos grupos:

**Mayor riesgo**

1. Beneficio personal
2. Síndrome de Robín Hood
3. Odio a la organización
4. Mentalidad turbada
5. Equivocación de ego

6. Deshonestidad del departamento
7. Problemas financieros de algún individuo
8. Fácil modo de desfalco

**Menor riesgo**

1. Beneficio de la organización
2. Jugando a jugar

## *Consideraciones Inmediatas para la Auditoría de la Seguridad*

### Uso de la Computadora

Se debe observar el uso adecuado de la computadora y su software que puede ser susceptible a:

1 tiempo de máquina para uso ajeno
2 copia de programas de la organización para fines de comercialización (copia pirata)
3 acceso directo o telefónico a bases de datos con fines fraudulentos

### Sistema de Acceso

Para evitar los fraudes computarizados se debe contemplar de forma clara los accesos a las computadoras de acuerdo a:

1. nivel de seguridad de acceso
2. empleo de las claves de acceso
3. evaluar la seguridad contemplando la relación costo, ya que a mayor tecnología de acceso mayor costo

### Cantidad y Tipo de Información

El tipo y la cantidad de información que se introduce en las computadoras debe considerarse como un factor de alto riesgo ya que podrían producir que:

1. la información este en manos de algunas personas
2. la alta dependencia en caso de pérdida de datos

## Control de Programación

Se debe tener conocer que el delito más común está presente en el momento de la programación, ya que puede ser cometido intencionalmente o no, para lo cual se debe controlar que:

1. los programas no contengan bombas lógicas
2. los programas deben contar con fuentes y sus ultimas actualizaciones
3. los programas deben contar con documentación técnica, operativa y de emergencia

## Personal

Se debe observar este punto con mucho cuidado, ya que se debe hablar de las personas que están ligadas al sistema de información de forma directa y se deberá contemplar principalmente:

1. la dependencia del sistema a nivel operativo y técnico
2. evaluación del grado de capacitación operativa y técnica
3. contemplar la cantidad de personas con acceso operativo y administrativo
4. conocer la capacitación del personal en situaciones de emergencia

## Medios de Control

Se debe contemplar la existencia de medios de control para conocer cuando se produce un cambio o un fraude en el sistema.
También se debe observar con detalle el sistema ya que podría generar indicadores que pueden actuar como elementos de auditoría inmediata, aunque esta no sea una especificación del sistema.

## Rasgos del Personal

Se debe ver muy cuidadosamente el carácter del personal relacionado con el sistema, ya que pueden surgir:

1. malos manejos de administración
2. malos manejos por negligencia

3. malos manejos por ataques deliberados

## Instalaciones

Es muy importante no olvidar las instalaciones físicas y de servicios, que significan un alto grado de riesgo. Para lo cual se debe verificar:

1. la continuidad del flujo eléctrico
2. efectos del flujo eléctrico sobre el software y hardware
3. evaluar las conexiones con los sistemas eléctrico, telefónico, cable, etc.
4. verificar si existen un diseño, especificación técnica, manual o algún tipo de documentación sobre las instalaciones

## Control de Residuos

Observar como se maneja la basura de los departamentos de mayor importancia, donde se almacena y quien la maneja.

## Establecer las Áreas y Grados de Riesgo

Es muy importante el crear una conciencia en los usuarios de la organización sobre el riesgo que corre la información y hacerles comprender que la seguridad es parte de su trabajo. Para esto se deben conocer los principales riesgos que acechan a la función informática y los medios de prevención que se deben tener, para lo cual se debe:

*Establecer el Costo del Sistema de Seguridad (Análisis Costo vs Beneficio)*
Este estudio se realiza considerando el costo que se presenta cuando se pierde la información vs. el costo de un sistema de seguridad.

Para realizar este estudio se debe considerar lo siguiente:

1. clasificar la instalación en términos de riesgo (alto, mediano, pequeño)
2. identificar las aplicaciones que tengan alto riesgo
3. cuantificar el impacto en el caso de suspensión del servicio aquellas aplicaciones con un alto riesgo
4. formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera

5. la justificación del costo de implantar las medidas de seguridad

Cuando se ha definido el grado de riesgo se debe elaborar una lista de los sistemas con las medidas preventivas que se deben tomar y las correctivas en caso de desastre, señalando la prioridad de cada uno. Con el objetivo que en caso de desastres se trabajen los sistemas de acuerdo a sus prioridades.

## Consideración y Cuantificación del Riesgo a Nivel Institucional

Ahora que se han establecido los riesgos dentro la organización, se debe evaluar su impacto a nivel institucional, para lo cual se debe:

1. Clasificar la información y los programas de soporte en cuanto a su disponibilidad y recuperación.
2. Identificar la información que tenga un alto costo financiero en caso de perdida o pueda tener impacto a nivel ejecutivo o gerencial.
3. Determinar la información que tenga un papel de prioridad en la organización a tal punto que no pueda sobrevivir sin ella.

Una vez determinada esta información se la debe CUANTIFICAR, para lo cual se debe efectuar entrevistas con los altos niveles administrativos que sean afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que podrían causar estas situaciones.

## Disposiciones que Acompañan la Seguridad

De acuerdo a experiencias pasadas, y a la mejor conveniencia de la organización, desde el punto de vista de seguridad, contar con un conjunto de disposiciones o cursos de acción para llevarse a cabo en caso de presentarse situaciones de riesgo. Para lo cual se debe considerar:

1. Obtener una especificación de las aplicaciones, los programas y archivos de datos.
2. Medidas en caso de desastre como pérdida total de datos, abuso y los planes necesarios para cada caso.
3. Prioridades en cuanto a acciones de seguridad de corto y largo plazo.
4. Verificar el tipo de acceso que tiene las diferentes personas de la organización,

cuidar que los programadores no cuenten con acceso a la sección de operación ni viceversa.

5. Que los operadores no sean los únicos en resolver los problemas que se presentan.

### Higiene

Otro aspecto que parece de menor importancia es el de orden e higiene, que debe observarse con mucho cuidado en las áreas involucradas de la organización (centro de cómputo y demás dependencias), pues esto ayudará a detectar problemas de disciplina y posibles fallas en la seguridad.

También se puede ver que la higiene y el orden son factores que elevan la moral del recurso humano, evita la acumulación de desperdicios y limita las posibilidades de accidentes.

Además es un factor que puede perjudicar el desarrollo del trabajo tanto a nivel formal como informal.

### Cultura Personal

Cuando se habla de información, su riesgo y su seguridad, siempre se debe considerar al elemento humano, ya que podría definir la existencia o no de los más altos grados de riesgo. Por lo cual es muy importante considerar la idiosincrasia del personal, al menos de los cargos de mayor dependencia o riesgo.

## *Consideraciones para Elaborar un Sistema de Seguridad Integral*

Como se habla de realizar la evaluación de la seguridad es importante también conocer cómo desarrollar y ejecutar el implantar un sistema de seguridad.

Desarrollar un sistema de seguridad significa: "planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa."

## Sistema Integral de Seguridad

Un sistema integral debe contemplar:

1 Definir elementos administrativos
2 Definir políticas de seguridad
   - A nivel departamental
   - A nivel institucional
3 Organizar y dividir las responsabilidades
4 Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
5 Definir prácticas de seguridad para el personal:
   - Plan de emergencia (plan de evacuación, uso de recursos de emergencia como extintores.
   - Números telefónicos de emergencia
   - Definir el tipo de pólizas de seguros
6 Definir elementos técnicos de procedimientos
7 Definir las necesidades de sistemas de seguridad para:
   - Hardware y software
   - Flujo de energía
   - Cableados locales y externos
   - Aplicación de los sistemas de seguridad incluyendo datos y archivos
8 Planificación de los papeles de los auditores internos y externos
9 Planificación de programas de desastre y sus pruebas (simulación)
10 Planificación de equipos de contingencia con carácter periódico
11 Control de desechos de los nodos importantes del sistema:
12 Política de destrucción de basura copias, fotocopias, etc.
13 Consideración de las normas ISO 14000

## Consideraciones para con el Personal

Es de gran importancia la elaboración del plan considerando el personal, pues se debe llevar a una conciencia para obtener una autoevaluación de su comportamiento con respecto al sistema, que lleve a la persona a:

1. Asumir riesgos
2. Cumplir promesas

3. Innovar

Para apoyar estos objetivos se debe cumplir los siguientes pasos:

## Motivar

Se debe desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo, así como su impacto a nivel empresarial, de cargo y individual.

## Capacitación General

En un principio a los ejecutivos con el fin de que conozcan y entiendan la relación entre seguridad, riesgo y la información, y su impacto en la empresa.

El objetivo de este punto es que se podrán detectar las debilidades y potencialidades de la organización frente al riesgo.

Este proceso incluye como práctica necesaria la implantación la ejecución de planes de contingencia y la simulación de posibles delitos.

## Capacitación de Técnicos

Se debe formar técnicos encargados de mantener la seguridad como parte de su trabajo y que esté capacitado para capacitar a otras personas en lo que es la ejecución de medidas preventivas y correctivas.

## Ética y Cultura

Se debe establecer un método de educación estimulando el cultivo de elevados principios morales, que tengan repercusión a nivel personal e institucional.

De ser posible realizar conferencias periódicas sobre: doctrina, familia, educación sexual, relaciones humanas, etc.

# Casos prácticos

Para conseguir la información que se detalla a continuación, se ha hecho uso de herramientas de auditoría como entrevistas y encuestas usando la metodología vista en el temario de la asignatura de *auditoría y gestión de sistemas*.

## *La Casa del Alumno*

La Casa del Alumno, es un edificio dotado de múltiples servicios e instalaciones que permanece abierto las 24 horas, los 365 días del año.

La Casa del Alumno está ubicada en la zona centro del campus del Vera, y linda por el oeste con la Biblioteca General. Acoge las instalaciones y los servicios de Delegación de Alumnos y la Asociación de Antiguos Alumnos, junto con otras asociaciones de alumnos.

El edificio cuenta con una superficie total de 5.200 metros cuadrados, distribuidos en cuatro plantas construidas en torno a diversas terrazas. Dispone de aulas para cursos, talleres y conferencias; salas generales para el estudio y el trabajo; aulas informáticas, y variados espacios para la atención y la participación.

Entre otros servicios, la Casa del Alumno, equipada con tecnología inalámbrica de voz y datos, aloja una ludoteca con billar, futbolín y una variada colección de juegos de mesa, una asesoría jurídica, un laboratorio fotográfico y una sala de ensayos.

Actualmente la Casa del Alumno dispone del siguiente material informático:

- 51 equipos de aula
- 4 equipos multimedia
- 6 equipos técnicos
- 12 equipos slip

- 6 impresoras en red
- 4 impresoras locales
- 1 plotter local

- 1 plotter en red
- 1 impresora-fotocopiadora OCÉ
- 1 servidor DELL (servidor de impresión)
- 6 scanners locales

- 2 servidores

Los programas de los que disponen los usuarios en los equipos de la Casa del Alumno, tanto en las aulas como en despachos y demás, son de uso general dentro de la UPV, y aquellos que requieran licencia de uso, si la UPV dispone de ella y se puede acceder a sus instaladores, también están. Respecto a programas de licencia libre tipo GPL, se elige aquellos que se adecuen más a las necesidades de los usuarios.

En cuanto a los programas de software privado, se accede a sus instaladores y licencias gracias al recurso \\izar2\aplicaciones, y a las que se puede acceder cualquier miembro de la comunidad. No obstante, hay algunas aplicaciones que solamente pueden instalar aquellos técnicos de aula que son PAS, y a las que los alumnos no se puede acceder, sobre todo si se trata de aplicaciones tan comunes y solicitadas como el MS Office, el sistema operativo MS Windows o cualquier otra aplicación de Microsoft.

Actualmente se hace uso de directivas de grupo y grupos de usuarios de la Unidad Organizativa (UO) de la UPV, grupos gestionados gracias al ASIC, pero debido a restricciones que imponen porque los alumnos sólo disponen de permisos de lectura sobre dicha UO, y los becarios que realizan las labores de técnicos de aula son alumnos, se están buscando alternativas a los grupos de usuarios, siendo prioritario el grupo de sancionados.

Otro tema de seguridad que se lleva a cabo es la vigilancia de los programas que utilizan los usuarios. Para ello se realizan consultas a los ordenadores para conocer las aplicaciones que está ejecutando el usuario, y para aquellas que muestran indicios de ser software malicioso, bien porque no están permitidas o no cumplen algunos requisitos, se avisa al usuario de que no se le permite usar dicha aplicación. En caso de insistencia o reincidir, es sancionado automáticamente.

Respecto a la seguridad exterior, la protección de la Casa del Alumno está dentro de la zona segura de la UPV, y para más protección se dispone de un cortafuegos en el ASIC que impide cualquier intrusión desde el exterior y un mayor control de los accesos al exterior desde la red interna del edificio. En cuanto a permisos de usuarios, todos los usuarios pueden ejecutar programas pero no instalar. Solamente el administrador local de cada PC y los becarios del área de informática, tanto colaboradores como coordinadores, tienen permisos de administración en todos los equipos de la Casa del Alumno, incluidas las asociaciones con sede en la Casa del Alumno.

## *Una herramienta de seguridad desarrollada en el ITI, el TigerWeb*

El Instituto Tecnológico de Informática es un Centro Tecnológico especializado en Investigación, Desarrollo e Innovación en tecnologías software. Fue.creado en 1994 a iniciativa del IMPIVA, la UPV y un grupo de empresas del sector informático. Está constituido como una asociación sin ánimo de lucro.

Su misión es la mejora y mantenimiento de la posición competitiva de las empresas del sector informático nacional mediante la I+D+i y la prestación de servicios avanzados.

Cuenta con una larga experiencia en la realización de proyectos de investigación, nacionales e internacionales, en colaboración con empresas e instituciones.

**¿Qué es?**

Es una herramienta de análisis de seguridad perimetral en redes IP. Mediante una extensa serie de pruebas sobre máquinas que disponen de una dirección IP externa, busca potenciales vulnerabilidades que puedan ser utilizadas por usuarios malintencionados para acceder, corromper, destruir o impedir el acceso a dichos sistemas. Como resultado del análisis genera un informe en castellano del estado de la seguridad de los sistemas analizados.

**Estructura de TigerWeb**

La herramienta es accesible desde una interfaz web personalizable con la apariencia corporativa de la **empresa** usuaria. Se compone de un motor de análisis desde donde se realizan una serie de pruebas (Actualmente más de 2000) sobre las IP seleccionadas. Cuenta con una base de datos de vulnerabilidades permanentemente actualizada y utilidades para verificar si las vulnerabilidades están presentes o no en un sistema determinado. De los datos resultantes del análisis y de la base de datos de vulnerabilidades, se genera un informe del estado de la **seguridad** de los sistemas frente ataques externos. En el informe se describen las pruebas de **seguridad** realizadas, y el resultado obtenido de ellas, detallando tanto las vulnerabilidades encontradas, como soluciones y recomendaciones para subsanar las deficiencias, referencias técnicas a las vulnerabilidades, así como sitios web con información

adicional, descargas para actualizaciones, etc. Además de estas informaciones, se proporciona el código CVE y/o Bugtraq asignado a la vulnerabilidad.

**Modalidades del servicio**

Las empresas tecnológicas pueden utilizar TigerWeb de forma puntual o periódica, de diferentes formas:

Como marca blanca personalizada con la imagen de la empresa en modalidad:

- Máquina alojada en el ITI
- Máquina alojada en la empresa (En desarrollo)

Como parte de una consultoría a realizar por la empresa asociada o en su caso con el ITI.

**Metodologías de Consultoría de Seguridad Informática**

**Tipos de Consultoría**

El objetivo es transferir una metodología y certificar su utilización. Son un complemento a las auditorias de LOPD y LSSI realizadas por las consultorías jurídicas y de empresa.

Nivel Básico: Técnicas básicas de seguridad informática.

Nivel Medio: Básico+Políticas de seguridad informática+Formación integral+Técnicas avanzadas de seguridad informática.

Nivel Alto: Medio+Plan estratégico y plan de contingencia+Técnicas de seguridad informática en tiempo real.

De seguridad del perímetro: Análisis previo+Ejecución TigerWeb+Interpretación de resultados.

**Intrudec**

Sistema de detección de Intrusos IDS de host y de red para entornos Unix y Windows. Se basa en una combinación de herramientas de libre distribución, herramientas del sistema y herramientas propias. *Esta en proceso de desarrollo*.

**Otros Servicios**

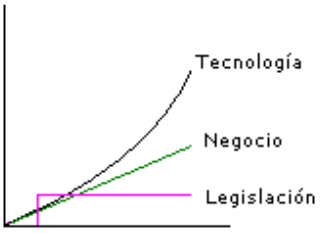
Seguridad en sistemas inalámbricos y móviles - Sistemas de Alta disponibilidad y Tolerancia a fallos - Tecnologías firewall y VPN - Sistemas de gestión de certificados web y firma electrónica...

# Conclusiones

De forma clásica, la seguridad de los SI de las empresas se ha entendido como una rama dependiente del llamado "dpto. de informática", no obstante, de un tiempo a esta parte, se está consiguiendo que la seguridad empiece a concebirse como una filosofía de la propia organización, como pueden ser la calidad, o el respeto al medio ambiente.

La seguridad pasa por entender que uno de los activos más valiosos de la organización es la información, y no tanto los componentes software o hardware, que pueden ser reemplazados. El cambio de mentalidad es paulatino, pero progresivo. Aún así, en muchas empresas, la alta dirección es reticente todavía a apostar por la seguridad porque no se entiende ésta como una inversión, sino como un gasto. Además, no se percibe la seguridad como un proceso evolutivo. De esta manera, de los gastos en activos informáticos de las organizaciones, los controles tácticos rondan el 90%, mientras que la seguridad estratégica apenas supera el 10%.

La gestión adecuada de la seguridad permite adaptarse a los cambios que vayan apareciendo en el entorno de la organización, ya sean legislativos como la LOPD, las regulaciones sectoriales como Basilea II, o CobIT.




La seguridad de los SI en una organización no puede seguir el ritmo de la evolución tecnológica porque implicaría una inversión económica muy importante, y muchas veces innecesaria, pero tampoco puede avanzar al ritmo de la legislación, que en muchas ocasiones va muy por detrás de la realidad tecnológica. La seguridad debe avanzar al ritmo del crecimiento del negocio, adecuándose a las necesidades que vayan apareciendo en la organización.

Con todo esto, destacan cuatro factores clave para gestionar la seguridad de los SI de una organización:

- Una fuerte componente organizativa.

- La métrica. Para ser capaz de gestionar la seguridad hay que saber medir el estado del riesgo de la información.
- Mejora continuada. La seguridad se debe entender como un ciclo. No se puede estar seguro al 100%, pero si procurar estar en un nivel adecuado.
- Certificación (AENOR, AP+…). Obtener una certificación sirve para detectar problemas de seguridad y sobre todo para saber responder ante ellos.

Para ayudar a responder ante los problemas en los SI de las organizaciones, se cuenta, cada vez más con la figura del auditor informático. Éste se encarga de evaluar el estado de los SI, de su control y su seguridad. ISACA es la entidad que ofrece las titulaciones más prestigiosas del sector de la auditoría. La posesión de una certificación CISM/CISA garantiza al auditado contar con un profesional con experiencia profesional continua en auditoría.

La radiografía de los SI de las organizaciones de la comunidad valenciana indica que las empresas valencianas están muy por debajo de los niveles de madurez de seguridad recomendados. Muchas empresas ni siquiera identifican sus activos de información, punto clave para alcanzar una seguridad adecuada. Quizás este sea el caballo de batalla de las organizaciones, ya que aunque existen estándares como ROI, que pueden ayudar, nunca existe una fórmula matemática que calcule su valor, y las valoraciones no dejan de ser un tanto cualitativas. Más tarde vendrían los análisis y sólo entonces podría empezar a hablarse de medir el nivel de seguridad en los SI de la organización. El llegar a este punto indica un proceso de educación al dueño de la información. Principalmente hay que saber transmitir confianza e informar hasta que punto la tecnología afecta a su negocio. La seguridad no genera dinero, pero evita sus pérdidas.

# Glosario

***Amenaza:*** Acción o acontecimiento que pueda perjudicar la seguridad. (European ITSEC) Potencial violación de la seguridad del sistema. (ISO 7498-2)

***Análisis de Tráfico:*** Información inferida de la observación del tráfico de datos (presencia, ausencia, dirección y frecuencia). (ISO 7498-2)

***Aseguramiento:*** Confianza que puede tenerse en la seguridad que proporciona un objetivo de evaluación. (European ITSEC)

***Autenticación de Entidad:*** Comprobación de que una entidad es la que se presupone. (ISO/IEC 9798-1)

***Autenticación de Origen de Datos:*** Comprobación de que la fuente de los datos recibidos es la afirmada. (ISO 7498-2)

***Certificación:*** Expedición de una declaración formal que confirma los resultados de una evaluación y el hecho de que los criterios de evaluación han sido correctamente utilizados. (European ITSEC)

***Certificado:*** Claves públicas de un usuario, junto con alguna otra información, infalsificable mediante cifrado con la clave secreta de la autoridad de la certificación que la emite.

***Clave:*** Secuencia de símbolos que controla las operaciones de cifrado y descifrado. (ISO 7498-2)

***Confidencialidad:*** Propiedad de la información que hace que ésta no sea disponible o descubierta a individuos, entidades o procesos no autorizados. (ISO 7498-2) Prevención de la revelación no autorizada de información. (European ITSEC)

***Denegación de servicio:*** Rechazo de un acceso autorizado a los bienes del sistema p retraso en las operaciones críticas en el tiempo. (ISO 7498-2)

***Disponibilidad:*** Propiedad que requiere que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada. (ISO 7498-2) Prevención de una negación no autorizada de información o recursos. (European ITSEC)

***Etiqueta de Seguridad:*** Indicador sensible que está permanentemente asociado con datos, procesos y/u otros recursos OSI protegidos, y que puede ser usado para poner

en práctica una política de seguridad. (ISO 7498-2)

***Firma Digital:*** Datos añadidos a un conjunto de datos o una transformación de estos que permite al receptor probar el origen e integridad de los datos recibidos, así como protegerlos contra falsificaciones. (ISO 7498-2)

***Gestión de claves:*** Generación, almacenamiento, distribución segura y aplicación, de claves de cifrado de acuerdo con una política de seguridad. (ISO 8732 & CD 11166)

***Integridad de datos:*** Propiedad de los datos que garantiza que éstos no han sido alterados o destruidos de modo no autorizado. (ISO 7498-2)

Prevención de la modificación no autorizada de la información. (European ITSEC) ***Mecanismo de Seguridad:*** La lógica o el algoritmo que implementa una función particular de seguridad tanto en hardware como en software. (European ITSEC)

***Notarización:*** Registro de datos por una tercera parte fiable, que suministra posteriores recursos a los mismos y garantiza la exactitud en lo que respecta a sus características como contenido, origen, tiempo y entrega de los datos. (ISO 7498-2)

***Política de Seguridad:*** El conjunto de reglas para el establecimiento de servicios de seguridad. (ISO 7498-2).

***Privacidad:*** Derecho de reclamar una seguridad adecuada y a definir usuarios autorizados de las informaciones o sistemas. (ISO 7498-2)

***Repudio:*** Denegación, por una de las entidades implicadas en una comunicación, de haber participado en todo o parte de dicha comunicación. (ISO 7498-2)

***Servicios de Seguridad:*** Servicios suministrados por uno o más niveles de sistemas abiertos de comunicación que llevan a cabo la seguridad del sistema y las transferencias de datos. (ISO 7498-2)

***Suplantación:*** Pretensión de una entidad de ser una diferente, para así acceder sin autorización a los recursos. (ISO 7498-2)

***Tercera Parte Fiable:*** Autoridad de seguridad, o agente suyo, fiable para otras entidades con respectos a actividades relativas a su seguridad. En el contexto de esta norma, una tercera parte fiable es de confianza para un demandante y/o verificador a efectos de autenticación.

***Vulnerabilidad:*** Debilidad de la seguridad de un Objetivo de Evaluación, debido a errores en el análisis, diseño, implementación u operación. (European ITSEC)

# Bibliografía


Panda Software: http://www.pandasoftware.es/

http://www.iwar.org.uk/iwar/resources/treatise-on-iw/iw.htm

http://www.cert.org/stats/

http://worldmap.f-secure.com

http://www.f-secure.com/virus-info/statistics/

http://www.dilbert.com

http://www.securityfocus.com/archive/1/348092



http://www.securityfocus.com/archive/1/348092