¡Vívelo!
MAYO Día de Internet 17

Tecnología, Seguridad y Empresa

Manual de introducción a la seguridad en el ámbito empresarial

La Suma de Todos
Comunidad de Madrid

MADRID COMUNIDAD DIGITAL

anei
asociacion nacional de empresas de Internet

- **ÍNDICE**

- ***PRÓLOGO***

El concepto de “seguridad integral” se ha consolidado en los últimos años en la empresa respondiendo al amplio espectro de incidencias a las que nos enfrentamos en nuestras compañías en materia de seguridad.

En respuesta se han de diseñar soluciones a las inquietudes de la empresa en este ámbito, desde la perspectiva global.

Es, en este sentido, en el que ANEI promueve este manual reuniendo a los expertos más significativos en cada campo a nivel nacional e internacional; a los que aprovecho para manifestar nuestro sincero agradecimiento, con el fin de animarles a detallar con la amplia experiencia que atesoran, las soluciones que se demandan en el mercado con decisión.

Desde nuestra condición de organización empresarial representante de la industria que cree e invierte en la Sociedad de la Información en España, hemos querido hacer hincapié en que un Internet seguro es posible y al alcance de todos, pero aún más, y este es uno de los propósitos de este manual, la seguridad puede y debe dar respuesta a todas las dudas a las que nos enfrentamos diariamente.

Propuestas realistas y técnicamente solventes hacen de este manual una herramienta indispensable que puede orientar a nuestros empresarios en la correcta aplicación de las nuevas tecnologías en el ámbito de la seguridad, con el objetivo de asegurar su trabajo y ahorrar los altos costes que las deficiencias en este campo pueden acarrear.

Su utilidad práctica y su perfil claramente divulgativo, estamos convencidos, le brindará una excelente acogida.

Miguel Errasti Argal

Presidente de la Asociación Nacional de Empresas de Internet, ANEI

http://a-nei.org

- ***INTRODUCCIÓN***

El año del DNI Electrónico

Arrancar los ordenadores mediante un identificador único, independientemente del Sistema Operativo, es la forma más directa de conseguir el pleno desarrollo del Comercio Electrónico.

El DNI electrónico debe usarse para autentificar el arranque de cualquier equipo informático, independientemente del Sistema Operativo que utilice. De esta forma seremos capaces de paliar el uso indebido de las redes informáticas, y por tanto llegar a tener un desarrollo de Comercio Electrónico tan avanzado, como en EEUU o los países nórdicos. Y es que el desarrollo de las transacciones a través de la Red está totalmente ligado a nuestra capacidad para garantizar la seguridad de las mismas.

Lo mismo ocurre con la e-administración. El desarrollo de servicios al ciudadano desde mecanismos telemáticos, esté ligado a la Seguridad. Porque si yo pido una subvención a través de Internet, el Estado necesita estar seguro de que yo soy, quien digo ser. Por ejemplo desde hace años, en Suecia los ciudadanos realizan todos los trámites relacionados con la Administración de forma telemática. Muchos jóvenes tienen la posibilidad de estudiar gracias a préstamos que proporciona el Estado, y que luego devuelven de forma cómoda a través de Internet, cuando ya están trabajando, independientemente de donde viven, relacionándose con la Administración a través de la Red de una forma “natural” y “eficaz”. Si por ejemplo ya no viven en Suecia, hacen el trámite de devolución cómodamente a través de Internet. Es decir un ejemplo de cómo los ciudadanos se relacionan con la Administración, que es en gran medida a través de Internet.

En España este desarrollo no ha llegado a consumarse por la ausencia de un dispositivo que permita asegurar que quien arranca un ordenador es quien dice ser. Y en último término en Secuware creemos que la mejor manera de autentificar el arranque de un ordenador, es a través del DNI Electrónico, del que se espera esté implantado en el cien por cien de la población española en un plazo de diez años. En nuestro caso, nos gustaría que el DNI Electrónico estuviese implantado antes. Y nos gustaría porque creemos en su efectividad.

¿Qué es el DNI Electrónico?

Un DNI Electrónico es una Tarjeta Inteligente que permite identificar a un usuario cada vez que arranca un ordenador. El hecho de incorporar un chip hace que sea incopiable. Y al estar acompañada de un password, la convierte en un sistema infalible para identificar a la

persona una vez enciende la máquina. El usuario simplemente tiene que introducirlo en el lector de tarjeta de su ordenador, y encenderlo previa introducción de su contraseña.

En Secuware sabemos que el DNI Electrónico daría fin al uso indebido de las Redes Informáticas, sobre todo si fuese ligado a una Tecnología capaz de mantener nuestros ordenadores y dispositivos móviles, libres de la acción de programas maliciosos. El reto es desarrollar una tecnología capaz de blindar los ordenadores, y alargar su ciclo de vida, al menos al triple que en la actualidad. Desde luego el desarrollo de la Sociedad de la Información está también muy ligado al precio del hardware. Queremos que todo el mundo navegue, que todo el mundo realice sus compras y sus trámites administrativos a través de Internet, que todo el mundo esté On Line, pero al mismo tiempo, hacemos de la tecnología un bien de lujo.

Desde Secuware vemos necesario ofrecer al ciudadano un sistema seguro, que le permita utilizar el mismo ordenador durante años, y no le obligue a estar continuamente actualizando sus dispositivos y por tanto abriendo la brecha digital.

El DNI Electrónico es absolutamente el camino a un desarrollo de Internet alineado con los países más avanzados de Europa. El sueño de los gobernantes y del ciudadano es posible. Sólo es necesario asegurarnos de que disponemos de la tecnología capaz de hacerlo realidad.

Carlos Jiménez

Presidente de Secuware

SECUWARE

http://www.secuware.com

- ***CAPÍTULO 1: ORGANIZACIÓN Y GESTION DE LA SEGURIDAD***

"No harán muy grandes cosas los vacilantes que dudan de la seguridad"
Thomas Stearns Eliot

1. Introducción

Uno de los tópicos más extendidos al hablar de la seguridad de la información es asociarla de manera inconsciente a la imagen de un adolescente afanado en reventar, más por placer rebelde que por malicia, los sistemas de autenticación de cualquier compañía, con mayor ahínco cuanto más conocida sea esta por el público. La progresiva facilidad del uso de herramientas de intrusión, unido al auge de las redes inalámbricas, hace que los titulares de los medios de comunicación se centren en los aspectos tecnológicos que, al provenir de un universo oscuro, misterioso e inquietante, muy alejado del usuario y, por ende, del directivo medio de la empresa española, tienen un tirón lúdico y mediático incuestionable.

De esta imagen de tintes románticos y hollywoodienses no resulta evidente inferir la otra realidad que viven las empresas para abordar la protección de su información. Esta otra realidad gira en torno al concepto más amplio de Confianza, de solidez y sostenibilidad de una Gestión de la Seguridad de la Información que inspire un razonable nivel de crédito subjetivo entre mi entorno de trabajo. Para este nuevo edificio debemos incorporar pilares procedimentales, legales y formativos que, aun con menos atractivo público, son de una importancia capital para la traducción de la seguridad a objetivos de negocio. En estos últimos años estamos asistiendo a una evolución de la gestión de la seguridad hacia modelos de gestión más cercanos a la medición sistemática que al parcheo circunstancial, al depender de ello la propia imagen de la organización. Los difusos y precarios límites de la confianza obligan a las organizaciones a diseñar una planificación que les proteja en todos los frentes que el Responsable de Seguridad debe atender. Y la sociedad de la información acoge pensar en clave de riesgo empresarial como la mejor forma de abordar de manera integral lo que está destinado a integrarse en el Cuadro de Mando (Balanced Scorecard), como conjunto de indicadores de la organización mensurables y comparables en el tiempo.

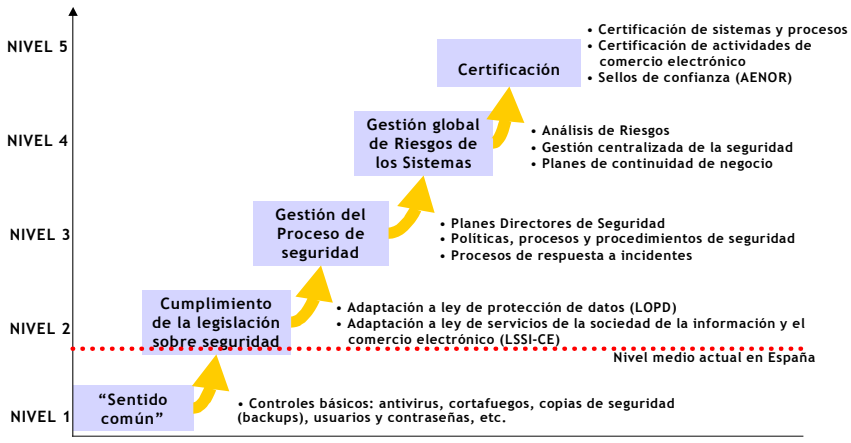
En la época donde los hackers y virus coexisten con los robos físicos, las sanciones legales, los empleados despechados, los desastres naturales y el terrorismo como ingredientes del mismo cóctel explosivo, no es suficiente una visión con enfoque puramente tecnológico, sino que la organización y planificación sistemática de todas las actividades asociadas a la seguridad se añade a las responsabilidades de gestión de la dirección general. En definitiva, se trata de conjugar la tecnología, los procesos y la gente que interviene en ellos en un todo indisoluble.

En la base del problema se encuentra el desconocimiento palmario de los Consejos de Administración sobre la magnitud del problema: en general, las empresas no son concientes de

los descalabros que podrían provocarles la inexistencia de una adecuada gestión de la seguridad de la información. La extensión de los últimos escándalos relacionados con la falta de confianza, en este caso contable, derivados de episodios como ENRON o Parmalat han desencadenado una preocupación, comprensiva de los sistemas de información, sobre el establecimiento de unas normas de gobierno corporativo que aporten un grado de confianza y transparencia necesarias en la gestión de las empresas. [1]

Por otro lado, el único contacto de la mayoría de las organizaciones con la seguridad proviene de su necesidad del cumplimiento a regañadientes de normativas como la Ley Orgánica de Protección de Datos, verdadero catalizador de la seguridad en España, al venir de serie con su "brazo armado", es decir, la Agencia Española de Protección de Datos. Nada como una buena sanción económica, o la percepción de su amenaza cercana, para espabilar las conciencias directivas y percibir de golpe y porrazo que esto de la seguridad es algo más que redes y hackers. Pero, la realidad es que las organizaciones deberían aprovechar el imperativo legal para plantearse el proceso como una oportunidad real para comenzar a gestionar adecuadamente la seguridad de su información.

De este propio proceso de adecuación a la normativa se infieren como siguiente frontera una serie de conceptos como **el análisis de riesgos** o el **establecimiento de métricas**, es decir, el germen de un cuadro de mando más cercano al conocimiento y sensibilidad de la alta dirección de la empresa, contribuyendo a reducir el gap entre tecnología y negocio y enfocando la seguridad como un proceso continuo que tiene un impacto directo en la cuenta de resultados. En hipotético escenario de niveles de madurez de la seguridad, la situación quedaría descrita según el siguiente gráfico:



[1] En este sentido, distintas iniciativas gubernamentales han tomado las riendas de esta tendencia, promoviendo leyes específicas, como la ley Sarbanes-Oxley en los Estados Unidos, que incluye el deber de certificar los controles internos, o la Ley de Transparencia española, que obliga a las sociedades anónimas cotizadas a establecer un sistema de gestión de riesgos e informar anualmente sobre el mismo.

Adicionalmente, la organización de la seguridad adolece de otro problema atávico y difícil de erradicar. Los Departamentos de Seguridad se han visto tradicionalmente como centros de coste, desde el punto de vista de Dirección General. No existe en la mente directiva una vinculación muy clara entre mi gasto en seguridad y los beneficios directos asociados a ese gasto. Esta percepción hace difícil la aprobación de gastos e inversiones en personal, hardware, software, formación, definición y desarrollo de procesos y procedimientos sin una aproximación que no me garantice el retorno de la inversión. La seguridad es un intangible, una sensación subjetiva, difícilmente encorsetable en números y que sólo se cuantifica cuando "ya ha pasado algo". El reto para las organizaciones es responder de antemano al ¿Qué pasa si...? o, dicho de otro modo, al coste que supone la no-seguridad para la organización.

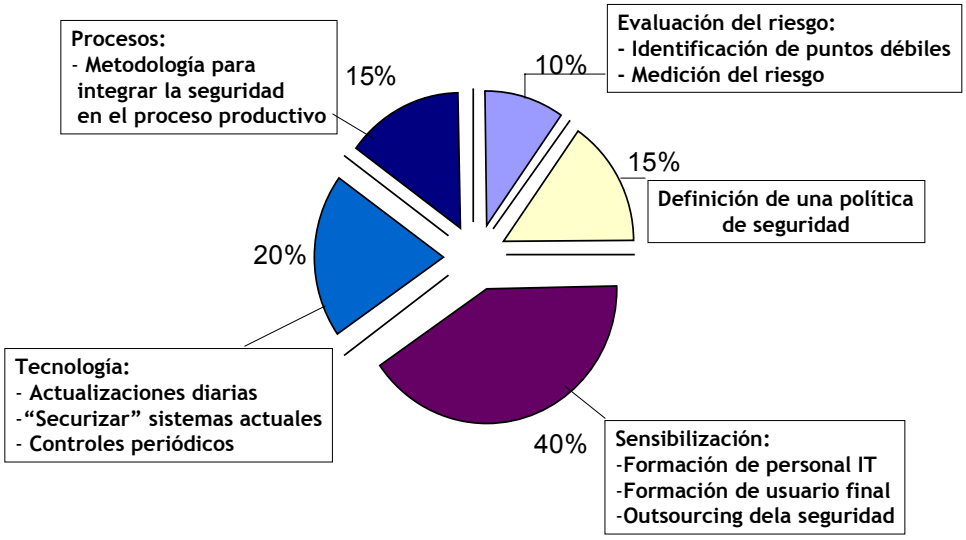
Muy pocas empresas saben exactamente ***cuánto deben gastarse*** en seguridad, al desconocer el valor de los activos que pretenden proteger. También desconocen cual es la probabilidad de que se produzca un impacto económico en sus activos y cual sería el impacto caso de producirse un incidente que afecte a la confidencialidad, integridad y disponibilidad de los mismos. Pocos mimbres para una estructura propensa, por tanto, más a las decisiones emocionales, espontáneas y arbitrarias, cuyo grado de inmediatez es directamente proporcional al impacto sufrido, que a un análisis metódico y racional que priorice la protección de aquellos activos más críticos para el negocio.

Y es que el gasto de seguridad ha venido tradicionalmente asociado a estrategias correctivas, es decir, resultado de buscar una solución a un problema de seguridad ya acaecido en la organización (virus destructivo, intrusión con robo de confidencialidad, sanción de la Agencia Española de Protección de Datos, desastre que requiere de un plan de continuidad de negocio, etc). No es habitual un enfoque proactivo que adopte medidas preventivas antes de que cualquier potencial riesgo se materialice.

De ahí una vez más la necesidad de establecer un sistema de gestión, basado en un análisis previo de los riesgos que afectan a la organización y que cuantifique el valor que significa para el negocio las acciones efectuadas para proteger la información, al tiempo que sirve de correa de transmisión a los altos niveles de la organización.

Uno de los estudios más rigurosos relacionados con la inversión en seguridad de la información arroja unos resultados bastante poco cercanos a la idea de seguridad predominante en el subconsciente colectivo: a la pregunta de cómo gastar 1 dólar en seguridad, la respuesta es que sólo un 20% se destinaría a la protección mediante herramientas tecnológicas, distribuyéndose el resto de la inversión entre el área de procesos, es decir, diseñar y ejecutar una metodología para integrar la seguridad en el proceso productivo (15%), realizar una evaluación del riesgo existente en la organización (10%), la definición de una política de seguridad (15%) y la sensibilización y formación del personal (40%), eslabón más débil por definición de la cadena de la seguridad, en cuanto a que es

ignorante, por lo general, de los riesgos que su actividad supone para su organización. Como se ve, el esfuerzo de la organización debería centrarse fundamentalmente en aspectos procedimentales (40%) y formativos (40%), siendo la parte tecnológica (securización de los sistemas actuales y mantenimiento diario) una parte minoritaria en el proceso de gestión.



Para todo ello, la premisa fundamental es que la Dirección General asuma como suya la responsabilidad de impulsar y liderar la gestión de la Seguridad mediante la realización de una detallada planificación cuyo instrumento básico es el Plan Director de Seguridad.

2. Plan Director de Seguridad de la Información

Partiendo de la premisa: "la seguridad no es un estado, sino un proceso", la correcta gestión de la seguridad es un proceso continuo que requiere ser evaluado, adaptado y mejorado constantemente.

Podemos definir el Plan Director de la Seguridad como la definición, documentación, implantación, ejecución, promulgación y mantenimiento continuo de determinados controles, mecanismos, políticas, auditorías, procedimientos, normas y actitudes cuya única función es mantener permanentemente protegidos con un cierto margen *mínimo y razonable* de confianza los activos físicos o lógicos de una organización ante amenazas externas o internas.

En sí mismo es el pilar documental de cualquier estrategia integral de gestión de la seguridad. Incluye un detalle de los activos de la organización susceptibles de gestión, es decir,

de los componentes o recursos de la organización objeto de protección. Una primera división sería entre **activos físicos (tangibles)** o lógicos (intangibles).

Ejemplos de los primeros serían:

- Las propias personas de la organización, el activo más imprescindible para la organización y cuya relación con la información y conocimiento que poseen requiere de una adecuada gestión
- Datos privados de clientes, datos de productos o servicios, datos económicos y financieros, datos privados de empleados, datos de investigación y desarrollo, previsiones de negocio, información estratégica para el negocio, etc.
- Mecanismos y procesos que permiten la continuidad del negocio (infraestructura informática, infraestructura de comunicaciones, infraestructura de almacenamiento de datos, etc)

Las decisiones que marcan el crecimiento y la competitividad de una organización se toman basándose en la información y el conocimiento que dicha organización posee. Es fundamental ***identificar qué activos y procesos son críticos*** para el negocio, así como la información y conocimiento de la que se nutren.

La organización de la seguridad ha de basar su estrategia en ***prevenir*** que la divulgación, manipulación o eliminación de esta información se traduzca en perjuicios económicos, competitivos o de imagen. La información y el conocimiento son los activos más valiosos de una organización (entendiendo el conocimiento como un tipo particular de información). Si se quiere que la organización compita en el mercado con garantías y cumpla con sus previsiones de negocio es necesario proteger la información y gestionarla de acuerdo a una política de estricto cumplimiento.

Esta política debe aplicarse rigurosa y sistemáticamente para garantizar que la información y la capacidad operativa de la organización están protegidos con un cierto margen de confianza aceptable. Los mecanismos, análisis, auditorías, procedimientos y normas de seguridad, derivados de esta política, que contribuyen a proteger la información, implican una inversión de capital, pero las consecuencias de exponer la información y el negocio a los diversos riesgos que los amenazan pueden suponer un coste económico mucho mayor (o pérdida de negocio).

Normalmente, las organizaciones cometen el error de pensar que esta inversión de capital es innecesaria debido a que la probabilidad de que nuestra información se vea amenazada es muy remota. Cada vez más se requieren menos conocimientos técnicos o habilidades extraordinarias para acceder a información restringida que sea crítica para la competitividad de la empresa.

Los **activos intangibles**, como la reputación e imagen de la empresa son cada vez más importantes en la sociedad de la información, al estar directamente vinculados al concepto

de Confianza. Pensemos en la repercusión en el negocio que puede resultar para un banco online la filtración de una vulnerabilidad en su aplicación web o que trascienda una sanción derivada de una infracción de la normativa de protección de datos. En determinados sectores, un incidente de estas características provoca un impacto tan grande en el negocio de la organización como difícilmente cuantificable, por lo que es preciso incidir en los mecanismos de prevención.

3. Beneficios de organizar y gestionar la seguridad

Podemos destacar los siguientes beneficios de una correcta gestión de la seguridad:

- Competitividad: no se da ningún tipo de ventaja a la competencia
- Continuidad y capacidad operativa del negocio garantizada, en caso de desastre, dispondré de los mecanismos adecuados para recuperar la capacidad crítica en el menor tiempo posible
- Fidelización de clientes: la percepción de la Confianza es un intangible que todo cliente exige inconscientemente de sus proveedores. Una adecuada organización y gestión de la seguridad aumenta el prestigió ante los clientes actuales, potenciales y las propias administraciones que, de manera creciente para la adjudicación de concursos públicos o el otorgamiento de subvenciones, valoran el compromiso de las organizaciones con una gestión continua de la seguridad.

La organización de la seguridad debe ser un proceso continuo, sistematizado y comunicado, además de impulsado y liderado por la Dirección General. Sin embargo, en la práctica se observan en la mayoría de los casos, una serie de errores comunes en la organización y gestión de la seguridad:

1. ***Inexistencia de un análisis previo de riesgos*** para evaluar las posibles amenazas que, aprovechando una vulnerabilidad en los activos de la organización, ocasionen un impacto económico en la misma. Es difícil, por no decir imposible, adoptar una visión estratégica y de negocio de la seguridad, cuando no se dispone de ninguna herramienta que determine el valor de los activos que intento proteger. Si no cuantifico y clasifico mis activos no sabré cual es la inversión en seguridad (personal, hardware, software, etc) que deberé mantener para evitar la pérdida, alteración, acceso no autorizado o indisponibilidad de los activos que se deben proteger.
2. ***Asignar una cantidad insuficiente de personal no cualificado*** para la definición, desarrollo y mantenimiento de la seguridad. Por lo general, al considerarse la seguridad como un coste y no como una inversión, los departamentos de seguridad se encuentran tradicionalmente escasamente dotados para realizar sus funciones. Adicionalmente, no se suele proporcionar formación a este personal para que adquieran el conocimiento necesario para realizar esta tarea con garantías.

3. ***Falta de comprensión de la íntima relación entre la seguridad de la información y el crecimiento del negocio*** (las organizaciones suelen entender la necesidad de una adecuada seguridad física pero son incapaces de ver las consecuencias de una pobre seguridad de la información, cuando cada vez más dependen en mayor medida de sus activos lógicos)

4. ***Incapacidad para gestionar los aspectos operativos de la seguridad***. En muchos casos, se procede a la implantación de medidas correctoras y/o preventivas pero no se establecen mecanismos de control y actualización de dichas medidas (las organizaciones identifican la seguridad de la información como un aspecto estático y puntual, no como un proceso dinámico).

5. ***Centrar la responsabilidad de la seguridad de la información únicamente en mecanismos tecnológicos de seguridad*** (muchas organizaciones creen que por el solo hecho de tener instalado un firewall están protegiendo su negocio contra cualquier tipo de ataque, ignorando la posibilidad de una sanción legal por cesión indebida de datos personales, por ejemplo).

6. ***Incapacidad para darse cuenta de la influencia del valor de su información y su reputación en el aspecto económico del negocio.***

7. ***Respuestas reactivas y correctivas a los problemas de seguridad e implantación de soluciones a corto plazo***. No se adopta una estrategia proactiva que prevenga los incidentes de seguridad ni se minimizan los riesgos, sólo se buscan soluciones rápidas según se detectan. Esto, unido a la incapacidad de saber cual es el valor de los activos protegidos, provoca una gestión de la seguridad ineficaz que tiene como consecuencia un consumo de recursos humanos y económicos destinados a la gestión de la seguridad que no corresponde con el necesario.

8. ***Pretender que los riesgos desaparecerán si son ignorados*** (la gestión de la seguridad es un aspecto de baja prioridad para la organización). Esta visión miope es muy habitual en aquellos sectores donde la seguridad no se percibe como un componente crítico para el negocio. Se asume que alguien con el suficiente tiempo y recursos puede comprometer siempre una organización. Al fin y al cabo, se tiende a pensar que si organizaciones como la NASA, Microsoft y los grandes bancos son carne de titular por violaciones de seguridad, es inútil adoptar cualquier estrategia de seguridad que implique un coste para la organización.

   Eso es un argumento tan sólido como decir que no voy a poner un cerrojo a la puerta de mi casa porque existen bandas organizadas con suficientes medios para reventar cualquier dispositivo de seguridad física. Y aunque nunca se pueda garantizar al 100% la seguridad de la información de la organización, el objetivo es minimizar en lo posible, siguiendo criterios de coste-beneficio, los riesgos particulares que amenazan

a una organización, según sus exigencias internas y externas y el sector en el que opere.

La conclusión de todas estas deficiencias es la consideración de la seguridad como un producto o conjunto de productos, no como un ***proceso de gestión continua*** que implica, en la mayoría de los casos, un cambio en la cultura y procesos de la organización. La seguridad no puede ser el resultado de una foto estática, sino que debe mantenerse después de implantada, así como evolucionar y adaptarse a los cambios de la organización y del negocio.

Es evidente que el remedio no debe resultar más caro que la enfermedad. La organización debe asumir el riesgo en caso de que la inversión necesaria para minimizarlo sea mayor que el coste económico o competitivo generado en caso de que se haga efectivo.

De manera informal, se habla de que una organización está expuesta a un cierto riesgo cuando existe una determinada probabilidad de que su información, su conocimiento y su negocio (sus activos lógicos, en definitiva) puedan ser afectados por agresiones o ataques.

Las amenazas que exponen a una organización a estos riesgos provienen de fuentes variadas y en ocasiones insospechadas:

- Competencia (directa o indirectamente a través de terceros)
- Empleados (ya sea por negligencia o de forma malintencionada)
- Clientes descontentos (directa o indirectamente a través de terceros)
- Espías independientes, crackers (chantaje, venta al mejor postor, etc)
- Hackers (con el fin de probar sus habilidades, tomar la infraestructura informática de la organización como base para otros ataques o como almacén de software, ataques masivos sin ningún objetivo en particular, etc)
- Software dañino (virus, troyanos)
- Desastres naturales o energéticos (tormenta eléctrica, corte de energía eléctrica, inundaciones, fallo de refrigeración, etc)

Todos los estudios estadísticos anuales demuestran que los riesgos a los que está expuesto nuestro negocio aumentan constantemente con el tiempo. Y es un problema que afecta a todas las organizaciones. Ignorar esta tendencia o restarle importancia creyendo que a nosotros nunca nos va a afectar no hace sino agravar el problema.

El mayor desafío de una adecuada organización de la seguridad es cambiar de mentalidad:

- La cuestión ya no es si nuestra organización está expuesta a algún riesgo o si existe alguna posibilidad de que alguna vez estos riesgos se materialicen en consecuencias negativas para el negocio.

- Hay que preguntarse no si nuestra organización está expuesta a riesgos sino ***a qué riesgos está expuesta***
- Hay que preguntarse no si alguna vez estos riesgos se harán efectivos sino ***cuándo lo harán*** y tomar medidas preventivas y correctoras para cuando suceda.Es inútil engañarse o ignorar el problema: con el ritmo de crecimiento actual de las agresiones contra la seguridad de las organizaciones, es obvio que tarde o temprano la seguridad de nuestra organización se verá puesta a prueba (si es que no lo ha sido ya). Si queremos evitar las consecuencias de estas agresiones el primer paso es fundamental: mantener una actitud realista y consciente de la existencia de riesgos que constantemente amenazan nuestros activos y la continuidad del negocio.

Una vez sentadas estas bases, queda claro que es necesario proteger la información y el conocimiento de mi organización, ya que son un patrimonio crítico para la competitividad y el crecimiento de mi negocio. También está claro que para proteger de forma adecuada la información es necesario con carácter previo conocer los riesgos a los que está expuesta.

Las siguientes preguntas son:

- ¿Cómo puedo saber a qué riesgos concretos está expuesta mi organización?
- ¿Cómo puedo protegerme ante ellos?

La respuesta es: un procedimiento totalmente regularizado y sistematizado llamado Análisis de Riesgos.

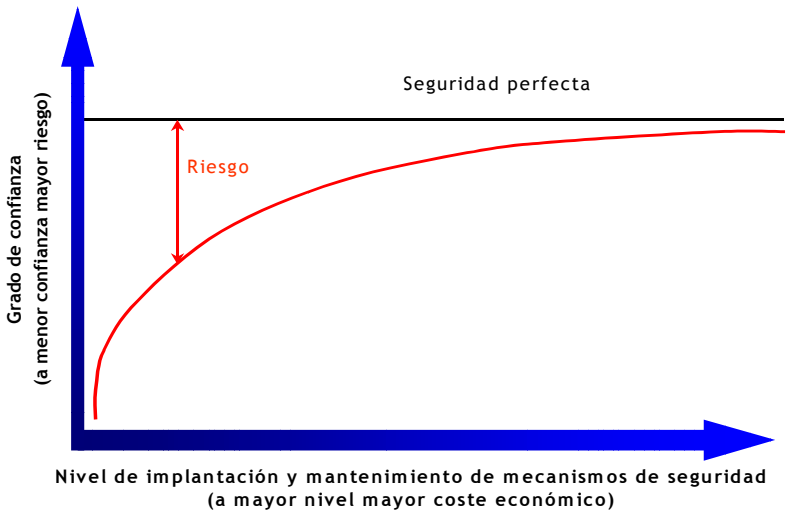
4. ¿Qué es un Análisis de Riesgos?

Un Análisis de Riesgos es, básicamente, un procedimiento de ayuda a la decisión. Sus resultados constituyen una guía para que la organización pueda tomar decisiones sobre si es necesario implantar nuevos mecanismos de seguridad y qué controles o procesos de seguridad serán los más adecuados.Es un paso previo e imprescindible para cualquier estrategia de organización y gestión de la seguridad. Una vez conocidos los riesgos, la organización ya dispone de la capacidad para decidir:

- Qué medidas tomar dependiendo de una serie de factores (costes de la implantación de controles que reduzcan los riesgos vs. costes derivados de las consecuencias de la materialización de estos riesgos)
- Implantar y mantener controles de seguridad que minimicen estos riesgos y los mantengan a un nivel aceptable (lo cual implica inversiones económicas)
- Asumir ciertos riesgos a los que está expuesta la organización ya que las consecuencias acarrean un coste económico y estratégico menor que el coste que sería necesario aportar para reducir dichos riesgosTransferir ciertos riesgos a terceros: bien a proveedores de servicios que prestan un determinado servicio a la organización (relación regulada según los términos de un Acuerdo de Nivel de Servicio) o bien

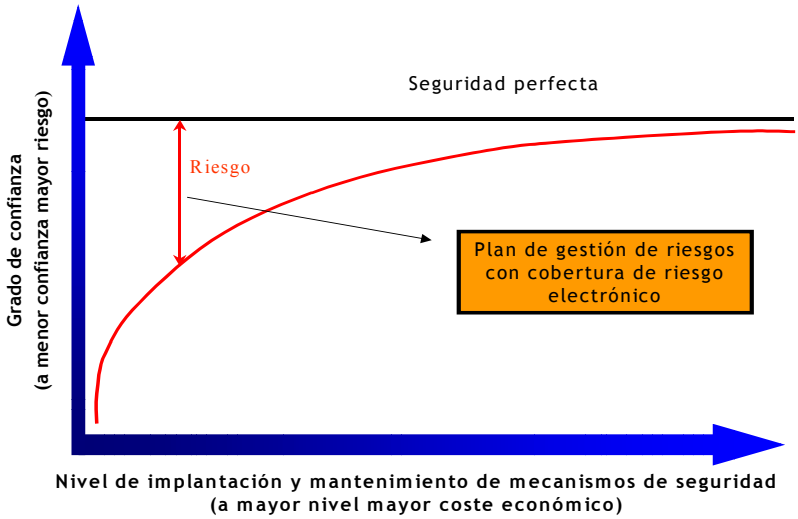
cubrir el riesgo residual mediante la contratación de un seguro de riesgo electrónico.

Por tanto, vemos que el nivel de riesgo al que está sometido una organización nunca puede erradicarse totalmente. Se trata de buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable)



El nivel de riesgo existente después de la implantación de salvaguardas se denomina riesgo residual, y es el que separa a la organización de la “Seguridad Total o Perfecta”. Una cobertura completa desde el punto de vista económico la aportaría un plan de riesgos conjunto, que incluyera la gestión efectiva de los riesgos detectados mediante la implantación de las salvaguardas correspondientes complementado con una póliza de riesgo electrónico que cubriera el riesgo residual.

De hecho, las compañías aseguradoras exigen para la contratación del seguro de riesgo electrónico la existencia de un Plan de Gestión de Riesgos, como prueba del compromiso efectivo de los asegurados sobre la gestión de su seguridad y como base para el cálculo de la prima.



Por el momento, las pólizas tradicionales presentan a este respecto, importantes lagunas de cobertura, la mayoría de las cuales han de solventarse fuera del ámbito de dichas pólizas.

Existen, sin embargo, algunas opciones en el mercado que permiten una amplia cobertura de los riesgos derivados de la seguridad de la información, ofreciendo coberturas para las siguientes garantías:

- Reclamaciones de terceros:
  - Por calumnia y difamación debido a contenidos del correo electrónico o de la web.
  - Por violación de derechos de la propiedad intelectual debido al correo electrónico o a contenidos de la web.
  - Por violación de la confidencialidad o derechos de privacidad (por ejemplo, violación de la ley de protección de datos).
  - Por publicidad engañosa, precios engañosos o temas jurisdiccionales.
  - Por daños a sistemas informáticos y/o registros (por ejemplo, a través del envío de virus o a través de las actividades piratas de empleados).
  - Por pérdidas como resultado de la imposibilidad de acceder a sus sistemas informáticos o como resultado de la pérdida de datos.
  - Por errores u omisiones en el suministro de servicios tecnológicos a sus clientes.
- Reclamaciones de los empleados:
  - Por un entorno de trabajo inapropiado (por ejemplo, cargos por acoso sexual o racial derivados de su actividad electrónica).
  - Por violación de la confidencialidad debido al uso fraudulento de la información de su organización

- Sanciones de la Agencia Española de Protección de Datos:
  - Derivadas del tratamiento de datos personales (sujeta a revisión / auditoria previa satisfactoria por una firma profesional independiente. Como vemos, ***no se trata de que la póliza sustituya a una correcta gestión de riesgos, sino que la complemente.***

A pesar de ser un procedimiento que se puede ejecutar de forma sistemática, en un análisis de riesgos es necesario realizar determinadas tareas y estimaciones de forma totalmente imparcial y objetiva:

- Inventariar los ***activos*** existentes en la organización
- Identificar las ***vulnerabilidades*** presentes en los activos
- Estimar la probabilidad con la que las amenazas pueden explotar las vulnerabilidades de los activos
- Estimar el ***impacto*** en el negocio en caso de que ciertas amenazas se hagan efectivas
- Estimar si se puede asumir el ***riesgo*** o es necesario invertir en la implantación o actualización de controles de seguridad

Si estos factores no se evalúan con total imparcialidad y objetividad, el análisis de riesgos no podrá cumplir su función con garantías, que es ayudarnos a tomar decisiones sobre cómo proteger nuestros activos. Por esta razón, es recomendable que el análisis de riesgos sea ejecutado por un agente externo a la organización.

El análisis estará orientado a evaluar el nivel de riesgo existente para el cumplimiento dentro de la organización de los siguientes criterios:

Confidencialidad: significa garantizar que un activo sólo será accesible por usuarios o procesos legítimos y autorizados. Comprometer, agredir o atacar la confidencialidad de un activo significa acceder al mismo de forma no autorizada o ilegítima

Integridad: significa garantizar que un activo sólo podrá ser manipulado o modificado por usuarios o procesos legítimos y autorizados

Disponibilidad: significa garantizar la capacidad operativa de un activo en el proceso de negocio de la organización. Comprometer, agredir o atacar la disponibilidad significa impedir que el activo pueda cumplir su función asignada en el proceso de negocio de la organización.

Una vez definidos los principios que debemos respetar en el análisis, es necesario comprender, de manera sencilla, los conceptos formales del análisis de riesgos:

1. ***Activos***: son todos aquellos componentes o recursos de la organización, tanto físicos (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio y conocimiento. Ejemplos de los primeros serían el hardware, software, servicios, documentos, personal, edificios, inventario, tesorería, etc. Entre los activos intangibles, el ejemplo más claro es la imagen / reputación, componente de difícil valoración económica pero de carácter capital en cuanto a la percepción de la Confianza que genera el negocio entre nuestro entorno.

2. ***Amenaza***: es un evento o incidente provocado por una entidad hostil a la organización (humana, natural o artificial) que aprovecha una o varias vulnerabilidades de un activo con el fin de agredir la confidencialidad, integridad o disponibilidad de ese mismo activo o de otros activos de la organización (se dice que la amenaza "explota" la vulnerabilidad del activo). Las amenazas pueden ser externas o internas a la organización y pueden ser deliberadas o accidentales. Ejemplos de amenazas serían los errores humanos / negligencia, el daño intencional / ataque, fraude, robo, fallos de equipos hardware /software, desastres naturales, etc.

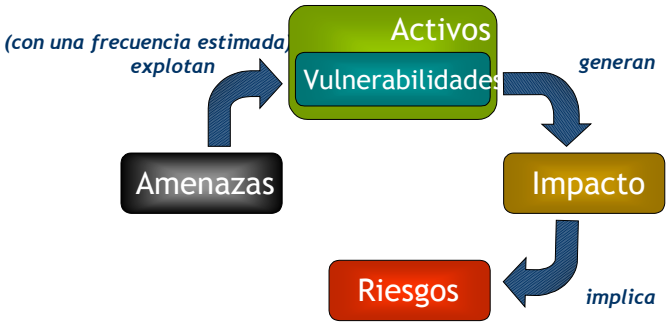
3. ***Vulnerabilidad***: es toda aquella circunstancia o característica de un activo que permite la consecución de ataques que comprometan la confidencialidad, integridad o disponibilidad de ese mismo activo o de otros activos de la organización. Ejemplos de vulnerabilidades serían la falta de conocimientos sobre seguridad del usuario, la falta de funcionalidad de la seguridad (deficiente configuración de un cortafuegos, por ejemplo), elección deficiente de contraseñas, tecnología no probada, transmisión por comunicaciones no protegidas, etc.

4. ***Impacto***: hace referencia a la magnitud de las consecuencias que tiene para el negocio el hecho de que uno o varios activos hayan visto comprometida su confidencialidad, integridad o disponibilidad debido a que una o varias amenazas hayan explotado las vulnerabilidades de estos u otros activos. Al estimar un determinado nivel de impacto es necesario considerar la criticidad de los activos afectados. ***Cuanto más crítico el activo afectado, mayor impacto se producirá en la organización***. Los impactos pueden tener diversa consideración, como por ejemplo:

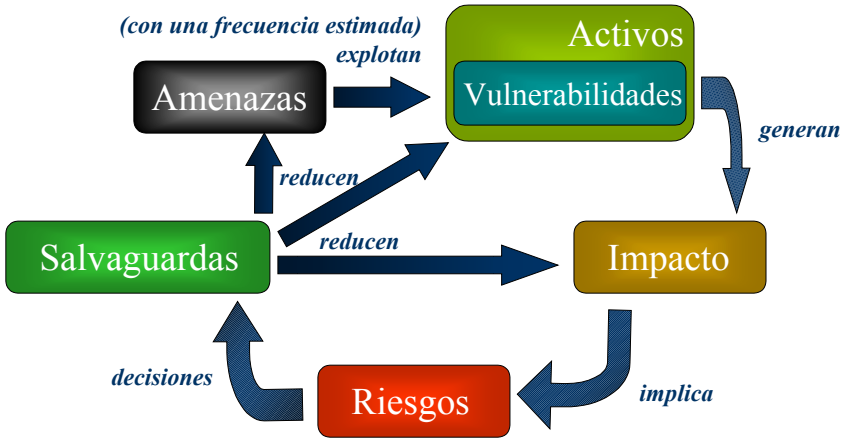
    - Pérdida directa de dinero
    - Sanción por violación de la legislación
    - Pérdida de imagen / reputación
    - Poner en peligro al personal o a los clientes
    - Violación de la confianza del entorno (clientes, partners, proveedores)
    - Pérdida de oportunidad de negocio
    - Reducción de la eficiencia / desempeño operativo

- ❖ Interrupción de la actividad de negocio

5. ***Riesgo***: Se define como la probabilidad de que la organización se vea sometida a un determinado nivel de impacto (determinado a su vez por las consecuencias de la agresión). Su estimación se basa en la combinación de dos factores:La ***frecuencia*** con la que las amenazas consideradas podrían materializarse (estimando la probabilidad de que las amenazas consideradas puedan explotar las vulnerabilidades de los activos)
   - ❖ ***Nivel de impacto*** causado en el negocio en el negocio en caso de que las amenazas consideradas se hagan efectivas. Será mayor cuanto más crítico sea el activo afectado.



6. ***Salvaguardas***: Se define todo control (política, procedimiento, norma, proceso o mecanismo) que contribuye a:
   - ❖ Reducir las vulnerabilidades de los activos
   - ❖ Reducir la probabilidad de que las amenazas puedan explotar vulnerabilidades
   - ❖ Reducir el impacto producido en el negocio por la materialización de amenazas



Las salvaguardas pueden clasificarse como:

- **Proactivas o preventivas**: cuando contribuyen a prevenir que se materialicen los riesgos. Protegen a los activos antes de que estos sufran ataques o agresiones. Ejemplo: los programas de formación para empleados, la definición y difusión de la política de seguridad, la segregación de funciones (al objeto de reducir el riesgo de que una persona este en condiciones tanto de cometer o ocultar errores o fraudes en el transcurso normal de su uso de los sistemas de información)
- **Detectivas**: cuando contribuyen a identificar la amenaza en el momento de materializarse y antes de producir un impacto en la organización. Ejemplos típicos de controles o salvaguardas detectivas son el uso de cortafuegos, el registro de logs, los sistemas de detección de intrusos (IDS), etc.
- **Curativas o correctivas**: cuando contribuyen a eliminar o reducir el impacto negativo de la materialización de una amenaza. También llamadas curativas. “Curan” a los activos después de que estos hayan sufrido ataques o agresiones. Como ejemplos podemos citar las copias de respaldo (back-ups) o los planes de contingencia y continuidad de negocio.

5. Tipos de Análisis de Riesgos

Con carácter previo, y en función de lo explicado en el epígrafe anterior, podemos clasificar los riesgos según la existencia o no con carácter previo de salvaguardas o controles dentro de la organización:

- Riesgo intrínseco: evaluado antes de aplicar las salvaguardas y existente, por tanto, en todas las organizaciones con independencia del sector en el que operen.
- Residual: evaluado después de aplicar las salvaguardas. Es el riesgo que siempre subsiste dado que no existe la Seguridad Total o Perfecta (que, sin embargo, puede ser cubierta económicamente mediante una póliza de seguro de riesgo electrónico)

Una vez identificados los riesgos, el siguiente paso es decidir qué tipo de análisis de riesgos elegir, según la posibilidad o no de cuantificar económicamente los daños producidos en una organización tras producirse un impacto. Esta aproximación nos ofrece dos vías:

1. ***Análisis de riesgo cuantitativo***: Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en ***cifras concretas*** de forma objetiva. Un modelo cuantitativo habitual es aquel en el que las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto, en función de la estimación del coste económico que supone para la organización. Tienen la ventaja de aportar una mayor precisión empresarial al dar como resultado una valoración numérica, que puede ser calculable en el tiempo y como inconveniente principal, la complejidad de su cálculo, especialmente en el caso de los activos intangibles (¿cómo valorar la pérdida de imagen como consecuencia de un incidente de seguridad que ha aparecido en los periódicos?)
2. ***Análisis de riesgos cualitativo***: Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en ***términos subjetivos*** (Impacto Muy Alto, Alto, Medio, Bajo o Muy Bajo). Las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de multitud de factores (pérdidas económicas efectivas, pérdida de conocimiento, pérdida de competitividad, interrupción de negocio, pérdida de imagen, etc). Tiene como ventaja principal su mayor facilidad de cálculo al no implicar una valoración económica y como inconveniente su carácter de apreciación subjetiva.

6. Pasos básicos de un Análisis de Riesgos

El proceso de evaluación de los riesgos de una organización se rige por los siguientes pasos:

1. Realizar o actualizar el ***inventario de los activos*** de la organización y establecer su criticidad en función del papel que tengan asignado dentro del proceso del negocio. En este punto se incluye una valoración preliminar en el que se tienen en cuenta las condiciones de seguridad existentes, identificando los controles o salvaguardas, procedimientos y procesos de seguridad ya existentes en la organización.
2. ***Identificar las vulnerabilidades presentes en los activos*** de forma concienzuda. Este paso es fundamental para conocer la eficacia de las salvaguardas ya presentes en la organización.
3. ***Identificar todas las posibles amenazas*** (internas o externas) que tienen la capacidad de explotar las vulnerabilidades de los activos.***Evaluar el impacto*** que tiene para el negocio la materialización de una determinada amenaza al explotar una determinada vulnerabilidad. Esta estimación del impacto es necesario realizarla para cada pareja amenaza-vulnerabilidad.
5. Estimar para cada una de las parejas amenaza-vulnerabilidad*, la probabilidad que existe de que dicha amenaza explote esa vulnerabilidad* (es decir, estimar la frecuencia con la que la amenaza podría explotar la vulnerabilidad). Las salvaguardas ya presentes en la organización influirán en gran medida en la estimación de estas probabilidades.

   Ejemplo:

   3. **Muy Alta (1): Cuando la amenaza puede materializarse en periodos inferiores a 1 semanaAlta (0,9): Cuando la amenaza puede materializarse en periodos inferiores a 2 meses.Media (0,7): Cuando la amenaza puede materializarse en periodos inferiores a 1 añoBaja: (0,5): Cuando la amenaza puede materializarse en periodos inferiores a 5 añosMuy baja (0,3): Cuando la amenaza puede materializarse en periodos superiores a 5 años**

6. ***Evaluar el nivel de riesgo*** al que está expuesta la organización para cada pareja amenaza-vulnerabilidad, combinando el impacto causado y la frecuencia de ocurrencia. La matriz de riesgos final es un producto de la multiplicación entre el impacto y la frecuencia / probabilidad que se produzca para cada tipo de activo.

Ejemplo de matriz de criterio utilizada para calcular el nivel de riesgo cualitativo

IMPACTO / FRECUENCIA	BAJO	MEDIO	ALTO
BAJA	Nivel BAJO	Nivel BAJO	Nivel MEDIO
MEDIA	Nivel BAJO	Nivel MEDIO	Nivel ALTO
ALTA	Nivel MEDIO	Nivel ALTO	Nivel ALTO

Matriz de criterio para estimación del nivel de riesgo: Ejemplo real

IMPACTO / FRECUENCIA	Muy Alto (50)	Alto (40)	Medio (30)	Bajo (20)	Muy Bajo (10)
Muy Alta (1,0)	Muy Alto 50 * 1,0 = 50	Alto 40 * 1,0 = 40	Medio 30 * 1,0 = 30	Bajo 20 * 1,0 = 20	Muy Bajo 10 * 1,0 =10
Alta (0,9)	Muy Alto 50 * 0,9 = 45	Alto 40 * 0,9 = 36	Medio 30 * 0,9 = 27	Bajo 20 * 0,9 = 18	Muy Bajo 10 * 0,9 = 9
Media (0,7)	Alto 50 * 0,7 = 35	Medio 40 * 0,7 = 28	Medio 30 * 0,7 = 21	Bajo 20 * 0,7 = 14	Muy Bajo 10 * 0,7 = 7
Baja (0,5)	Medio 50 * 0,5 = 25	Bajo 40 * 0,5 = 20	Bajo 30 * 0,5 = 15	Muy Bajo 20 * 0,5 = 10	Muy Bajo 10 * 0,4 = 4
Muy Baja (0,3)	Bajo 50 * 0,3 = 15	Bajo 40 * 0,3 = 12	Muy Bajo 30 * 0,3 = 10	Muy Bajo 20 * 0,3 = 6	Muy Bajo 10 * 0,2 = 2

IMPACTO * FRECUENCIA	NIVEL DE RIESGO
40 < Impacto * Frecuencia <= 50	Muy Alto
30 < Impacto * Frecuencia <= 40	Alto
20 < Impacto * Frecuencia <= 30	Medio
10 < Impacto * Frecuencia <= 20	Bajo
0 < Impacto * Frecuencia <= 10	Muy Bajo

NIVEL DE RIESGO = IMPACTO * FRECUENCIA

Tabla de criterio que establece el nivel de riesgo cualitativo en función de métricas cuantitativas del impacto y la frecuencia (estimación semicualitativa)

Una vez terminado el proceso y en función de los riesgos obtenidos, se debe establecer un plan de acción, en el que se establezca ***qué salvaguardas necesita la organización*** y hacer una planificación para su implantación.

El plan de acción debe contemplar los siguientes aspectos de la Gestión de la Seguridad:

1. Identificar qué salvaguardas serán más óptimas para prevenir aquellos riesgos que no se asuman.

2. Implantar estas salvaguardas o mecanismos que ayuden a prevenir estos riesgos
3. Revisar y modificar en caso necesario los procedimientos establecidos de respuesta a incidentes (es decir, en caso de que se hagan efectivas las amenazas)Revisar y modificar en caso necesario los planes de recuperación ante desastres (planes de contingencia, gestión de crisis)
5. Revisar y modificar en caso necesario los documentos de gestión de seguridad de la organización (política, procedimientos, normas, guías)

Las salvaguardas ayudarán a reducir los riesgos actuales, pero el análisis de riesgos debe establecerse como un ***proceso de carácter cíclico y recurrente*** con el fin de que la organización pueda anticiparse a nuevos riesgos (nuevas amenazas o nuevas vulnerabilidades), comprobar si el impacto o la frecuencia de las amenazas y vulnerabilidades ha cambiado como consecuencia de cambios en el negocio o verificar si las salvaguardas implantadas contribuyen de manera eficaz a reducir los riesgos.

Hasta ahora hemos visto ***QUÉ pasos básicos*** es necesario ejecutar a la hora de aplicar un análisis de riesgos. Sin embargo, queda abierta la cuestión de ***CÓMO se ejecutan*** estos pasos.

La respuesta es: Metodologías de Análisis de Riesgos.

7. Metodologías de Análisis de Riesgos

Existen metodologías perfectamente documentadas, reguladas, sistematizadas y estandarizadas que proporcionan una guía metódica al usuario sobre cómo desarrollar de forma completa un análisis de riesgos. La ventaja de aplicar una metodología reside en que se aplican procedimientos y criterios ampliamente perfeccionados cuya eficacia está sobradamente establecida. Aunque existen otras metodologías utilizadas a nivel mundial (CRAMM, COBRA, etc), la más utilizada en España es ***MAGERIT***.

La Metodología de Análisis y Gestión de Riesgos de las Administraciones públicas, MAGERIT, es un método formal de análisis y gestión de los riesgos que soportan los Sistemas de Información, y de recomendación de las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Magerit ha sido elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática.

Sus objetivos inmediatos son:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociable a él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, en una primera aproximación que se atiene a la acepción habitual del término
- Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados
- A largo plazo, el objetivo de MAGERIT es articularse con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información. Magerit toma como referencia sistemática los siguientes métodos:
    - Los criterios ITSEC (Information Technologies Security Evaluation Criteria)
    - Common Criteria (ISO15408)

La metodología Magerit no debe considerarse como un mero análisis de riesgos, sino que constituye una metodología completa de gestión de riesgos.

Esto significa que un simple análisis de riesgos se limita a la identificación de riesgos y permite decidir cuándo es necesario implantar salvaguardas, pero no ofrece mecanismos para decidir qué salvaguardas son las más adecuadas. Sin embargo Magerit, además de estudiar los riesgos que afectan a los sistemas informáticos, va más allá del simple análisis y recomienda qué salvaguardas son las más apropiadas para reducir la potencialidad de estos riesgos o su posible impacto.

El concepto de salvaguarda en Magerit es muy amplio por lo que sus recomendaciones sobre la selección e implantación de salvaguardas afecta prácticamente a todos los aspectos de la gestión de la seguridad. Todo el modelo Magerit se basa en un conjunto de Guías y un conjunto de Herramientas (I):

- ***Guía de aproximación***: constituye una introducción a los conceptos básicos de la gestión de la seguridad de los Sistemas de Información y esboza los principios fundamentales del modelo Magerit.
- ***La Guía de Procedimientos***: representa el núcleo del método y está orientado a la gestión de los riesgos. Es decir a cómo tratar los riesgos detectados, teniendo en cuenta el avance científico, normativo y normalizador en materia de seguridad de los sistemas de información.Se complementa con la ***Guía de Técnicas***: proporciona las claves para comprender y llevar a la práctica las técnicas especificadas en las tareas a realizar documentadas en la Guía de Procedimientos.

La aplicación del modelo Magerit de análisis y gestión de riesgos consta de cuatro etapas (definidas en el submodelo de procesos), dispuestas en un ciclo iterativo de 4 etapas que constituye la fase de Análisis y Gestión de Riesgos dentro del proyecto global de Gestión de la

Seguridad de los Sistemas de Información.El ciclo de etapas es iterativo ya que después de analizar los riesgos, identificar e implantar funciones y mecanismos de salvaguardas, se puede volver a iniciar el ciclo acudiendo a la fase de análisis de riesgos, pero con la diferencia de que este segundo análisis se realiza con las salvaguardas implantadas.

El ciclo utiliza el producto final de cada etapa como inicio de la siguiente.

Etapa 1: Planificación del Análisis y Gestión de Riesgos

- *Investiga la viabilidad del proyecto*
- *Define los objetivos que ha de cumplir*
- *Define el dominio que abarcará*
- *Planifica los medios materiales y humanos necesarios*
- *Inicia el lanzamiento del proyecto*

Etapa 2: Análisis de Riesgos

- *Identifica, estima y valora los Elementos que intervienen en el riesgo (activos, amenazas, vulnerabilidades e impacto)*
- *Evalúa el riesgo en las distintas áreas del dominio definido en la Etapa 1*
- *Especifica los umbrales de riesgo deseables*

Etapa 3: Gestión de Riesgos

- *Identifica las funciones o servicios de salvaguarda que pueden reducir el riesgo*
- *Selecciona las salvaguardas apropiadas en función de las ya existentes y de las restricciones del proyecto*
- *Estima la eficacia de las distintas combinaciones de salvaguardas*
- *Especifica las salvaguardas definitivas*

Etapa 4: Selección de salvaguardas

- *Identifica los mecanismos de salvaguarda*
- *Selecciona los mecanismos de salvaguarda a implantar*
- *Establece los controles de seguimiento para la implantación*
- *Recopila toda la documentación producida a lo largo de todo el proyecto y elabora los documentos finales*
- *Realiza las presentaciones de los resultados a los diversos niveles*

La Guía de procedimientos de Magerit proporciona una descripción detallada de cada tarea. Para cada una de las tareas, la guía de procedimientos especifica:

- *El objetivo de la tarea*
- *Acciones concretas a realizar*
- *Responsables que intervienen o están afectados por la cumplimentación de las acciones*

•Productos y documentos que se deben obtener como producto de las acciones

•Validaciones y aprobaciones a realizar de los resultados obtenidos

•Técnicas a emplear para llevar a cabo las acciones (tomadas de la Guía de Técnicas de Magerit)

Para conocer más a fondo el modelo Magerit la mejor referencia son las propias Guías de Magerit, sobre todo la Guía de Aproximación, Guía de Procedimientos y Guía de Técnicas. En la siguiente dirección, http://www.csi.map.es/csi/pg5m20.htm, se pueden consultar las Guías Magerit y profundizar sobre la metodología, así como consultar ejemplos de aplicación del modelo y descargarse las herramientas software de soporte MAGERIT.

8. Estándares y normativas de Gestión de la Seguridad de la Información

Como indicamos en el principio de nuestra exposición, el análisis de riesgos tiene como finalidad identificar y calibrar los riesgos a los que está expuesta la organización con el fin de conocer cuándo es necesario implantar salvaguardas.

La gestión de riesgos, además de identificar y evaluar los riesgos, tiene como finalidad añadida ayudar en la selección de los controles o salvaguardas más adecuados para minimizar dichos riesgos.La gestión de la seguridad de la información, además de identificar y evaluar los riesgos y seleccionar salvaguardas, tiene como finalidad añadida la implantación y mantenimiento de estas salvaguardas La gestión de la seguridad de la información tiene como objetivo principal establecer, implantar y mantener unos controles que aseguren una protección adecuada de la confidencialidad, integridad y disponibilidad de la información, conocimiento, recursos y patrimonio de la organizaciónLas metodologías y estándares de la gestión de seguridad de la información permiten acometer este objetivo proporcionando recomendaciones y prácticas de base para que las organizaciones las tomen y puedan adaptarlas y aplicarlas a su propia idiosincrasia. La principal ventaja de basarse en una metodología o estándar para gestionar la seguridad de una organización reside en que se adoptan recomendaciones basadas en las buenas prácticas cuya eficacia está sobradamente establecida, lo cual permite disponer de un punto de partida para responder a la pregunta de... ¿Por donde empiezo?.

Otra ventaja que aportan estos estándares consiste en que se pueden convertir en un criterio universal aceptado por la mayoría de organizaciones con el cual se puede contrastar de una forma absolutamente fiable el nivel de seguridad de una determinada organización. Esta amplia aceptación de una metodología estándar proporciona un criterio a las organizaciones en el que basar la confianza de sus relaciones.La metodología de gestión de la seguridad con más difusión y aceptación en la actualidad es el estándar internacional ISO/IEC 17799. El estándar internacional ISO/IEC 17799 se preparó por la British Standards Institution BSI como BS7799 como resultado de la demandas de la industria, el gobierno y los consumidores británicos de

disponer de un marco que permitiera a las empresas desarrollar, implementar y medir efectivamente las prácticas de gestión de la seguridad y facilitar la generación de la confianza suficiente para el comercio entre organizaciones. Debido a las demandas de organizaciones en otros países, esta norma se elevó para ser establecida como estándar internacional, adoptada por el Comité Técnico Conjunto ISO/IEC JTC 1 Tecnología de la Información, como norma ISO 17799.

En el año 2002, a nivel nacional, el comité espejo AEN/CTN, adaptó al castellano la norma ISO/IEC 17799:2000, dando lugar a la norma UNE-ISO/IEC 17799. ISO/IEC 17799 (en adelante ***ISO17799***) es una norma internacional que constituye un ***código de buenas prácticas de la gestión de la seguridad de la información.***

La propia norma especifica claramente que este código de buenas prácticas únicamente ofrece ciertas pautas y tan sólo debe considerarse un punto de partida para desarrollar la gestión específica de la seguridad de una organización. Su misión no es profundizar en cada aspecto de la gestión de la seguridad sino establecer unas bases a modo de cimientos sobre las cuales cualquier organización pueda desarrollar una sólida y eficaz gestión de la seguridad.

Cada organización debe adaptar estas recomendaciones genéricas a sus propias condiciones y características. No son de aplicación inmediata todos los controles incluidos en la norma, incluso pueden existir algunas de ellas que no sean aplicables a sus particularidades o puede que esas mismas particularidades requieran controles no incluidos en la norma.

La norma ISO/IEC 17799 está compuesta de 10 capítulos, en cada uno de ellos se incluye una selección de controles que están considerados como buenas prácticas en cada una de las áreas:

- Política de seguridad
- Organización de la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Comunicaciones y gestión de explotación
- Control de acceso al sistema
- Desarrollo y mantenimiento
- Plan de continuidad
- Conformidad legal

En cualquier caso, en la norma se especifican ciertos controles aplicables a la mayoría de las organizaciones que constituyen un punto de partida adecuado para implantar la gestión de la seguridad de la información.

Una de las recomendaciones de la norma es situar en el punto de partida el análisis de los ***requerimientos legales, estatutarios y contractuales*** ya que, al ser estos controles de obligado cumplimiento para todas las organizaciones, constituyen una buena fuente y punto de partida, junto con el análisis de riesgos, para la fijación de los requisitos de seguridad.

Como ejemplos de algunos de estos controles podemos mencionar:

- Controles esenciales desde un punto de vista legislativo:
  - Protección de los datos de carácter personal y la intimidad de las personas
  - Salvaguarda de los registros de la organización
  - Derechos de propiedad intelectual
- Controles esenciales para la implantación de la seguridad de la información:
  - ***Documentación de la política de seguridad*** de la información
  - Adjudicación de ***responsabilidades de seguridad***: es importante no sólo que el personal técnico sea consciente de sus diversas responsabilidades en el área de seguridad, sino que todo el personal conozca y cumpla la política de seguridad de la organización, de cuyo incumplimiento pueda derivarse un régimen disciplinario.
  - ***Formación y entrenamiento*** para la seguridad de la información: el mejor modo de transmitir los principios de la seguridad es a través de programas formativos de diverso nivel (usuario final, técnico, ejecutivo)
  - ***Registro de las incidencias de seguridad***: además de procedimiento obligatorio y necesario para una adecuada gestión de la seguridad, cualquier incidente debe estar debidamente documentado, en eventualidades como la realización de actividades ilícitas por un empleado o en el caso de reclamaciones legales efectuadas por terceros ante hechos producidos desde los sistemas de información de la organización. Un buen registro de incidencias es, en cualquier caso, un medio imprescindible para la defensa en todo proceso judicial.
  - Gestión de la **continuidad del negocio**: La posibilidad de que ocurra un desastre, desde catástrofes naturales, pasando por actos de terrorismo, hasta problemas técnicos severos y continuados, como ataques de virus o hackers, hace que las organizaciones necesiten un Plan de Continuidad de Negocio, con la gestión y recursos asociados. Tras la aparición de desastres naturales y actos de terrorismo recientes, los negocios han reconocido más que nunca, la necesidad de que la organización debe estar preparada. Constituye la salvaguarda correctiva o curativa por excelencia.

En cualquier caso, aunque estos controles esenciales se consideran un buen punto de partida, no hay que olvidar que la referencia principal para la selección de los controles

apropiados para una correcta gestión de la seguridad debe seguir siendo el análisis y gestión de riesgos.Adicionalmente, la norma especifica ***8 factores críticos de éxito***, determinados por la experiencia, que son necesarios para que la implantación de la gestión de la seguridad se pueda llevar a cabo con éxito:

- Una política, objetivos y actividades que reflejen los objetivos de la organización
- Un enfoque para implantar la seguridad que sea consistente con la cultura de la organización
- El apoyo visible y el compromiso de la alta dirección
- Una buena comprensión de los requerimientos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo.
- La venta eficaz de la seguridad a todos los directivos y empleados
- La distribución de guías sobre la política de seguridad de la organización y de normas a todos los empleados y contratistas
- Proporcionar una formación y entrenamiento adecuados
- Un sistema integrado y equilibrado de medida que permita evaluar el rendimiento de la gestión de la seguridad de la información, sugerir mejoras y compararse en el tiempo (Sistema de Gestión de la Seguridad de la Información o SGSI). Este sistema implica la necesidad de revisiones
- periódicas para considerar nuevos procedimientos y requerimientos internos, nuevas amenazas y vulnerabilidades y la confirmación de que las medidas de control aplicadas siguen siendo eficientes (revisión de la selección de controles)

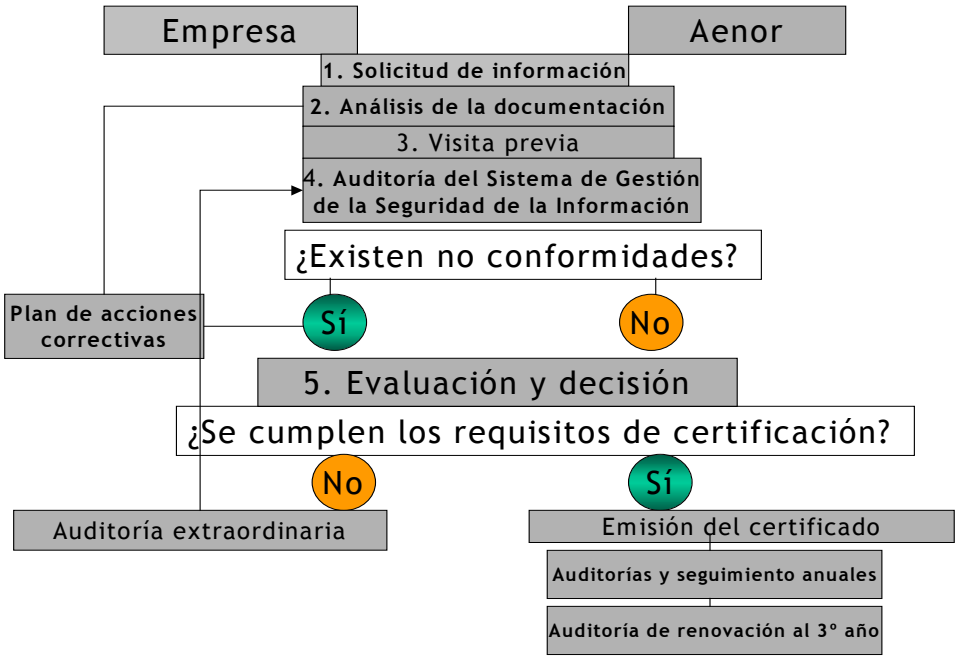
Como vemos, de acuerdo a la norma ISO 17799, las organizaciones deben establecer un sistema de controles, mensurables en el tiempo, para la adecuada gestión de la seguridad de la información. Sin embargo, la norma ISO 17799 aportaba únicamente un marco de conformidad, según el cual las organizaciones adoptaban e implantaban internamente estos controles, pero sin existir un esquema de certificación otorgado por un prestador externo de servicios de certificación. El resultado es que la conformidad no era suficiente para acreditar ante terceros la existencia de una correcta gestión de la seguridad.

Para cubrir esta exigencia del mercado, en el mes de febrero de 2004, la Asociación Española de Normalización y Certificación (AENOR) publicó la ***Norma UNE 71502***, Especificaciones para los Sistemas de Gestión de la Seguridad de la Información, con vocación de ser la referencia aplicable para los procesos de certificación de los Sistemas de Gestión de la Seguridad de la Información (SGSI). La citada Norma establece los requisitos para implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información, dentro de los riesgos identificados por las organizaciones de acuerdo con la Norma UNE-ISO/IEC 17799:2002.

La Norma 71502 fue desarrollada en el seno del Comité Técnico de Normalización AEN/CTN 71 Tecnologías de la Información y más concretamente de su Subcomité SC 27 Técnicas de Seguridad y su principal aportación es que constituye en sí misma un esquema de certificación, lo que permite acreditar ante terceros que las organizaciones están comprometidas en un proceso de mejora continua de sus indicadores de seguridad.

La posesión de esta certificación, sujeta a auditorías periódicas internas y externas, no significa que los sistemas de una organización sean infranqueables, sino que, al incluir la seguridad como elemento fundamental de sus procesos de negocio, se dispone de un sistema para gestionar los riesgos de diferente índole de mi organización (tecnológicos, legales, procedimentales, etc) y tomar decisiones empresariales sobre la manera de afrontarlos (mitigándolos, asumiéndolos o incluso transfiriéndolos a terceros).

Esquema de certificación de AENOR



Asimismo, existen otras metodologías que se pueden considerar alternativas o complementarias, en función del tamaño de la organización y del sector en el que se encuentre. Algunos estándares normativos que es preciso conocer son:

- ***COBIT (Control Objectives for Information and related Technology)*** de la Information Systems Audit and Control Asociation (ISACA), ampliamente aceptado por la comunidad internacional de auditores de sistemas de información como una norma estándar de la auditoria de sistemas. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de organizaciones y auditores.

La amplitud de sus objetivos de control hacen de COBIT una referencia mundial, usada por numerosas organizaciones, especialmente en el entorno estadounidense, como complemento de la norma ISO 17799 y aplicable tanto al establecimiento de unas directrices y fundamentos para proporcionar una investigación consistente sobre los temas de auditoria y control de TI como a la adecuación a los estándares y normativas legislativas en materia de seguridad de la información.

- ***ISO 13335/UNE 71502 (GMITS*** 2): La norma UNE71501 se ha elaborado para facilitar la comprensión de la seguridad de las Tecnologías de la Información (TI), y proporcionar orientación sobre los aspectos de su gestión. Esta estructurada en tres partes: UNE71501-1 que proporciona una visión general de los conceptos fundamentales y de los modelos utilizados en la gestión de la seguridad de la información. La segunda, UNE71501-2, describe los aspectos de gestión y planificación de la seguridad de TI. Va dirigida eminentemente a responsables (directivos).
- Finalmente la UNE71501-3, describe técnicas de seguridad indicadas para quienes se encuentran implicados en actividades de gestión durante el ciclo de vida de un proyecto.

8. Estructura organizativa de la Seguridad

Tradicionalmente, las organizaciones han adscrito siempre la figura del Responsable de Seguridad a personal técnico especializado en los aspectos técnicos de la Seguridad. No existe ninguna definición de funciones específicas de la figura del Responsable de Seguridad más allá de su caracterización legal: El Reglamento de Medidas de Seguridad de los ficheros que contengan datos automatizados de carácter personal (Real decreto 994/99, de 11 de junio) define al Responsable de Seguridad como la "persona o personas a las que el Responsable del Fichero (es decir, la organización) ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables".

De esta definición legal sólo se puede deducir que el ***Responsable de Seguridad*** ha de ser un mero ejecutor y coordinador de las políticas definidas y establecidas por la Dirección General, que son los titulares de la "propiedad" de la información y los sujetos responsables de decidir el QUÉ hacer para proteger la información de la organización, quedando el CÓMO en manos de los expertos internos y externos especializados en los distintos ámbitos de la seguridad de la información (tecnológico, procedimental y legal). Esta visión integral contrasta con la miopía actual de la mayoría de las organizaciones y debe ser, de hecho, uno de los factores críticos de éxito para una adecuada gestión de la seguridad de la información.

[2] GMITS: *Guidelines for the Management of IT Security.*

Idealmente, las organizaciones deberían establecer un ***Comité de Seguridad*** de la Información, compuesto por representantes de todas las áreas funcionales y cuya misión sea la definición, comunicación efectiva a los empleados y supervisión de la política de seguridad de la información, velando por que los controles sean razonables, eficientes y aplicables al negocio de la organización. Entre sus ***actividades principales***, podríamos destacar las siguientes:

- **Identificación de los riesgos específicos para el negocio** y estudio y evaluación de controles que especifiquen la relación riesgo-control más adecuada. Los controles implantados seguirán el doble enfoque de valoración del daño potencial de pérdida de información junto con la probabilidad de pérdida de esa información.
- **Elaboración e implantación de la normativa de seguridad interna**, habitualmente recogida en el Documento de Seguridad
- **Asignación de responsabilidades sobre seguridad**: nombramiento del Responsable de Seguridad y fijación de las funciones y obligaciones de cada una de las personas con acceso a la información de la organización.
- **Documentación y comunicación efectiva de la normativa de seguridad**. Resulta fundamental todo esfuerzo por documentar la seguridad de la información, ya que es preciso que los responsables de los activos deben gestionar la seguridad de forma coordinada y teniendo como referencia un objetivo y unas prácticas comunes. Asimismo, los usuarios necesitan una normativa que puedan consultar en cualquier momento, que defina sin ambigüedades qué compromiso espera de ellos la organización en cuanto a seguridad y qué represalias pueden esperar en caso de incumplirla.
- **Identificación y asignación de niveles de autorización** (control de acceso) a la información. Aquí el principio que ha de seguirse es el de "mínimo privilegio", según el cual el personal sólo tendrá acceso autorizado exclusivamente a aquella información que necesite para el desempeño de su trabajo.
- **Selección de asesores especialistas** en los distintos ámbitos de Seguridad de la Información.
- **Contacto con autoridades** legislativas, organismos reguladores, proveedores de servicios de información, operadores de telecomunicaciones
- **Garantía de revisión independiente y periódica de la Seguridad de la Información**, para confirmar no sólo que los controles establecidos siguen siendo eficientes sino que están alineados con los objetivos de la organización.

Al hablar de documentación de seguridad estamos haciendo alusión a la serie de documentos que reflejan el conjunto de valoraciones, actividades, prácticas, decisiones y compromisos que la organización debe afrontar con el objetivo de mantener eficazmente protegidos sus activos (tangibles o intangibles).

Por tanto, los documentos mantienen entre sí una relación jerárquica establecida en función del alcance o grado de generalidad del documento y deben adaptarse perfectamente a las particularidades y procesos de la organización, así como revisarse y actualizarse de forma periódica.

Los ***documentos que permiten construir la gestión de la seguridad de la información*** son:

- ***Política***: Es un documento de alto nivel. Es decir, un documento de gran generalidad que expresa las metas y objetivos de la organización y la aplicación de estos objetivos a cada área de la organización en particular.
  Ejemplo: "Los propietarios de la información son responsables de ofrecer un entorno seguro en el cual dicha información pueda ser mantenida y procesada con integridad"
- ***Estándares***: Son documentos que describen tareas, acciones, reglas o normativas de obligado cumplimiento que dotan a la política de un soporte estructural. Los estándares concretan mediante conceptos específicos el sentido "abstracto" y generalista de la política.
  Ejemplo: " Los propietarios de la información deben asegurar que sus sistemas están limpios de elementos de software destructivos (como por ejemplo virus), que impedirían su correcta operación"
- ***Guías***: Son documentos generales cuyo objetivo es facilitar el cumplimiento de las metas de la política mediante la creación de las condiciones adecuadas en las que se puedan implantar los procedimiento**s**.
  Ejemplo: "Debe instalarse un paquete de software que prevenga y detecte virus en los sistemas y que sea capaz de recuperar información corrompida. Aquellos usuarios que tengan acceso a los sistemas deberán asistir a una jornada de formación sobre virus con el fin de que comprendan las consecuencias de una infección y su responsabilidad a la hora de proteger la información del sistema"
- ***Procedimientos***: Son documentos que describen de forma específica y concreta cómo se implantarán la política, estándares y guías en el entorno operativo de la organización.
  Ejemplos: "Los usuarios de los sistemas no podrán instalar software de dominio público (frecuente fuente de virus) sin la autorización explícita del responsable del sistema. Los usuarios cerrarán sus estaciones de trabajo al finalizar la jornada para prevenir accesos no autorizados y posibles contaminaciones de virus. Los usuarios son responsables de informar sobre cualquier tipo de acceso no autorizado o infección de virus al comité de Protección de la

Información o al Help Desk" a través del procedimiento detallado de gestión de incidencias a disposición de todos los usuarios del sistema.

Asimismo, otra actividad fundamental para una eficaz organización de la seguridad es la clasificación de la información, que atenderá a su mayor o menor carácter confidencial o a su criticidad para el negocio. En este sentido, podemos hablar de tres niveles de información:

- ***Pública***: Información que está disponible para ser distribuida de forma pública a través de canales controlados por la organización. Puede ser una posible vía de riesgo en cuanto a la información que se está ofreciendo a la competencia**.**
- ***Restringida:*** Información destinada al uso exclusivo por parte de los empleados de la organización en el desarrollo rutinario de los procesos del negocio.
- ***Confidencial o Estratégica***: Información, que en caso de ser divulgada, podría violar la privacidad de personas, reducir la ventaja competitiva de la organización o causar un daño significativo al negocio o la imagen de la organización

9. La opción de la externalización de la seguridad de la información

Si algún área de la actividad empresarial queda a priori bajo sospecha al plantearse la opción de externalización, esa ha sido tradicionalmente la de la seguridad de la información. Es evidente que los sectores impulsores de la demanda en seguridad, el sector bancario y el de telecomunicaciones, principalmente, muestran razones "filosóficas" para mantener sus sistemas controlados por personal interno. El principal argumento para esta visión es la reticencia a poner en manos de terceros una actividad compleja y multidisciplinar encargada de la protección de información interna y confidencial, que, para colmo, resulta crítica para el negocio en el caso de muchos sectores.

La reticencia surge del hecho de que, por muy leonino que sea el Acuerdo de Nivel de Servicio (más habitual en su acepción inglesa, Service Level Agreement o SLA) que firme con mi proveedor ¿qué garantías reales puedo tener una organización de que su información se mantenga confidencial en el largo plazo? ¿Es aceptable que una empresa externa tenga acceso a conocer quienes son mis mejores clientes y cuales son sus cifras de facturación? ¿Puedo arriesgarme a que sepa con antelación el plan de negocio del nuevo producto que preveo lanzar al mercado el mes que viene? ¿Y mis proyectos de I+D?

La realidad, sin embargo, nos muestra que numerosas empresas confían ciegamente en su personal interno para la gestión de la información altamente confidencial, y que, probablemente, este personal no dispone en muchas ocasiones del rigor y conocimiento necesario suficiente para proteger sus activos de información del mismo modo que lo hacen las empresas especializadas. Amén de que convertirse de empleado en ex empleado es, en la sociedad actual, cada vez cuestión de (poco) tiempo.

¿Tengo más motivos para confiar en mi personal interno que en una empresa externa, de cuya escrupuloso respeto de su garantía de confidencialidad depende su supervivencia como negocio? La verdad es que no parece que podamos dar una concluyente respuesta positiva a esa pregunta. Con lo que, superada la desconfianza inicial hacia este acceso de mi información por parte de un tercero, la opción de externalización debe ser, cuando menos, considerada en profundidad.

Un adecuado análisis de riesgo nos determinará el grado de exposición de nuestra empresa a las riesgos y amenazas a los que está expuesta, y permitirá disponer de una información adecuada para definir y priorizar nuestras actividades de gestión de la seguridad. Una vez analizados y evaluados los riesgos, la organización debe tomar decisiones sobre su gestión: ¿dispongo de suficientes recursos internos para abordar esta planificación, definición, implantación y mantenimiento de mi Plan Director de Seguridad en condiciones ventajosas de calidad y de coste?. Tal vez sí en alguno de los puntos, pero difícilmente en todos: de ahí que, progresivamente, se observa una tendencia en el mercado a la externalización de, al menos, parte de los procesos de gestión de la seguridad.

Este proceso de externalización es ya una realidad en la auditoría, diseño e implantación de sistemas. Las organizaciones cada vez más buscan propuestas de proveedores que se adhieran y lideren iniciativas basadas en estándares como los propuestos en la sección anterior, de carácter internacional y con el respaldo de la mayoría de las empresas, en detrimento de oscuros procedimientos propietarios de incierto desarrollo futuro.

En el ámbito puramente tecnológico, el crecimiento desbocado de actividad hostil proveniente de virus, troyanos, spyware y demás malware, cada vez más inteligente; intentos de intrusión y rotura de la defensa perimetral, a través de ataques cada vez más avanzados a nivel de aplicación, etc, requiere de unas tecnologías costosas, y de los correspondientes recursos humanos para su gestión, en continua formación.

Estas exigencias hacen viable para muchas organizaciones la propuesta de externalización de servicios de seguridad gestionada. Es evidente que, gracias a las economías de escala que se producen en los modelos de negocio de estos proveedores, resulta más rentable contratar una empresa externa especializada que supervise mi seguridad (para entendernos, un “Prosegur virtual”), que mantener internamente los recursos necesarios, especialmente si lo que se busca es un modelo de servicio 24x7. Las organizaciones comienzan a demandar propuestas de servicios maduros, que vayan más allá del ‘alquiler’ de personal especializado al que nos tiene acostumbrado el sector de las TIC.

Por otro lado, el desarrollo normativo ha sido especialmente prolífico en estos últimos años. (LOPD, LSSI, Ley General de Telecomunicaciones, Ley de Firma Electrónica, etc), lo que demanda igualmente una actualización continua en aspectos de obligado cumplimiento en el sector. La conformidad legal se plantea como necesidad y marco de actuación mínima sobre el

que debe basarse cualquier proyecto de organización y gestión de la seguridad de la información. El conocimiento multidisciplinar, no solo de los aspectos tecnológicos, sino también de los legales, ha de ser una de las variables que es preciso considerar a la hora de evaluar la disponibilidad de personal interno suficientemente formado, o, en la opción de externalización, en la que a la hora de elección de proveedor de servicios de seguridad, ha de ser muy importante la cobertura en el triple eje tecnológico, procedimental y legal.

http://www.tb-security.com

- **CAPÍTULO 2: SEGURIDAD DEL PERSONAL**

1- Introducción

La ISO/TEC 17799:2000 dedica su capítulo 6º a "la seguridad ligada al personal" con el objetivo de reducir los denominados riesgos internos que provienen de errores humanos, robos, fraudes o mal uso de las instalaciones o servicios.

Desde un punto de vista estadístico, se ha considerado que más del 80 % de las amenazas o riesgos a la seguridad de la información en las compañías, proviene de actuaciones de los empleados.

Las empresas luchan por reducir las amenazas procedentes de los empleados, que en ocasiones actúan en desconocimiento del riesgo que generan para la empresa (ignorancia), y en otros supuestos se producen por actuaciones de empleados o exempleados motivadas por el descontento con la entidad (malicia).

Todo ello, unido a los fallos de las medidas de seguridad de las compañías o al mal control de la seguridad, hacen más patente los riesgos humanos producidos.

Las organizaciones intentan hacer frente a esta situación utilizando diversas medidas: desde la implantación en la empresa de toda la normativa legal que les ayude al mantenimiento de la integridad y seguridad de la información, hasta la firma de acuerdos de confidencialidad con sus empleados en los contratos, pasando por el establecimiento de responsabilidades en las políticas de seguridad o la formación de los usuarios en uso correcto de los recursos de la empresa, etc.

Resulta necesario llevar a cabo una función interna de divulgación y sensibilización sobre la seguridad, de forma que su difusión sea efectiva y los empresarios aseguren a sus empleados una formación adecuada en seguridad.

La Política de Seguridad de la Información es una herramienta vital en la organización para concienciar a todo su personal sobre la importancia y criticidad de la información en el funcionamiento y continuidad del negocio.

Así, para la correcta gestión de la seguridad de la información es preciso que existan unas directrices de actuación definidas por la Dirección y dadas a conocer a todo el personal de la entidad, mediante las cuales todos sepan cómo actuar y las repercusiones en caso de incumplimiento. Este enfoque general se plasma en la política corporativa de seguridad de la organización.

La política de seguridad surge como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la

información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

La responsabilidad del cumplimiento de las Normas es de todos los empleados, incluido especialmente del personal directivo que acumula a su responsabilidad como empleado, la de todos los empleados a los que dirige, coordina o supervisa.

Como complemento a la Política y a las Normas de seguridad, se instrumentarán los procedimientos operativos necesarios para su correcta aplicación, detallando los pasos de cada una de las acciones a abordar en los distintos supuestos, los departamentos y personal involucrado, los formularios, mecanismos de comunicación, etc.

La implementación de políticas de seguridad implica ineludiblemente incrementar la complejidad en la operativa de la organización, tanto técnica como administrativa. Basta pensar en la disminución de la operatividad de los usuarios finales (ejemplo de usuarios que para acceder a determinados recursos deben multiplicar sus login – acceso al sistema, acceso a aplicativos determinados -) que consideran esta medida de seguridad como un nuevo impedimento en su labor diaria y como un control adicional del empresario para controlar y establecer responsabilidades en caso de incumplimientos.

Asimismo, la puesta en funcionamiento de la nueva norma de seguridad implicará una nueva tarea para el área técnica (por ejemplo, cambiar los derechos de usuarios), y desde el punto de vista administrativo, la organización deberá notificar fehacientemente a los implicados dichos cambios.

En base a lo anteriormente expuesto, el enfoque de seguridad de la información debe ser coherente con la cultura de la organización, siendo necesarios el compromiso y el apoyo visible de la dirección de la empresa.

Asimismo, debe realizarse una adecuada difusión de la seguridad al personal de la organización (a todos los niveles) y debe ofrecerse orientación sobre la política de seguridad y sobre las normas y estándares a aplicar a los usuarios implicados (tanto internos como externos), proporcionándoles una formación adecuada.

Complementarias a las características expuestas que debe reunir una correcta política de seguridad, es preciso señalar que debe mantener un lenguaje común, libre de tecnicismos y términos legales que impidan una comprensión clara y concisa de los objetivos. Por otra parte, la política debe incluir el rango de los correctivos y la clase de sanciones que se puedan imponer (adecuado y realista procedimiento disciplinario).

Finalmente, la Política de Seguridad como documento dinámico de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes (crecimiento de plantilla, rotación de personal, desarrollo de nuevos servicios, etc.) y

contendrá información de control (fecha de publicación, fecha de entrada en vigor, ámbito de aplicación, si sustituye a una norma precedente o es nueva, etc.)

2. Seguridad en la definición del trabajo y los recursos

La ISO-17799 establece como una buena práctica en la gestión de la seguridad de la información el contemplar la seguridad desde el mismo proceso de selección de personal, incluirse en los contratos, reforzarse mediante la firma de una cláusula de confidencialidad (no divulgación) y seguirse durante el desarrollo de la relación laboral.

Se identifican acciones diferentes para los solicitantes de empleo de la organización (candidatos), proponiendo una serie de filtros en el proceso de selección de personal, y para los trabajadores en plantilla y terceros usuarios (identificados como el personal de empresas contratadas ajenas a la organización) que para el desempeño del trabajo asignado requieran ser usuarios de aplicaciones de tratamiento de información. Estos últimos han de suscribir cláusulas o acuerdos de confidencialidad en el tratamiento de la información.

3. Inclusión de la seguridad en las responsabilidades laborales

Es fundamental en toda organización, para garantizar la seguridad de la información de la entidad, la difusión a todo el personal de las medidas o políticas de seguridad que han sido tomadas desde la dirección de la empresa.

En este sentido, es imprescindible que toda organización cuente con procedimientos claramente establecidos, para evitar los riesgos que se pueden producir en la seguridad de sus sistemas.

Las funciones y responsabilidades sobre seguridad de la información, atendiendo a la política de seguridad de la organización deben documentarse por escrito para facilitar su conocimiento y cumplimiento. Así, deberá distinguirse entre una responsabilidad general dirigida a implantar o mantener la política de seguridad establecida en la organización (responsabilidad común para todos los usuarios del sistema) y determinadas responsabilidades específicas y adicionales que sólo serán exigibles a determinados trabajadores que en función del trabajo desarrollado en la organización, requieran acceder a activos particulares y especialmente sensibles o ejecuten procesos o actividades particulares de seguridad (por ejemplo dentro del equipo asignado a la seguridad de la entidad, los administradores de sistemas).

Un ejemplo palpable de este control de seguridad podemos encontrarlo en la normativa legal vigente para la mayoría (por no decir la totalidad) de las organizaciones en materia de protección de datos en España: La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) y el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (en adelante RMS).

En nuestro país, las organizaciones se encuentran ante la necesidad de adaptar la seguridad de sus sistemas de información (limitándose a los ficheros con datos de carácter personal) a la citada normativa vigente.

El artículo 8.2c) del RD 994/1999, tras determinar que el Responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal, y a los sistemas de información, establece que dicho documento debe contener "*las funciones y obligaciones del personal"*. Asimismo, el artículo 9.1 del citado precepto legal determina que *"las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas"...*Una vez publicadas en el documento de seguridad, deberán ser conocidas, aceptadas y respetadas por todo el personal.

Otra de las consideraciones que afectan al tema tratado y que se hace constar de manera especial en esta normativa, es la designación de la figura del Responsable de Seguridad.

En el artículo 2 del Real Decreto 994/1999, se define al Responsable de Seguridad como: *"persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables."*

En el artículo 16 del Real Decreto 994/1999, comprendido dentro del Capítulo III, se establece la obligación de designar un Responsable de Seguridad en las organizaciones que traten datos clasificados como de nivel medio (y alto) y el artículo 15 obliga a que se identifique esta figura en el Documento de Seguridad.

El hecho de forzar la designación de una o varias personas que se ocupen de la implantación y el cumplimiento de los procedimientos de seguridad en el seno de la organización, no debe crear confusión sobre las responsabilidades derivadas del incumplimiento de lo dispuesto en el Reglamento de medidas de seguridad, ya que las sanciones ocasionadas por las infracciones que pudieran producirse no recaerán, en ningún caso, sobre el responsable de seguridad sino sobre el responsable del fichero (la propia organización).

Es importante señalar, que no existe la obligación legal de que el Responsable de Seguridad sea una persona interna de la organización, pudiendo recaer esta responsabilidad, (mediante una adecuada relación contractual) en una persona u organización externa encargada de las labores propias del Responsable de Seguridad.

En cualquier entidad, es indispensable que Responsable de Seguridad (o la persona que se ocupe de la seguridad de los datos) cuente con la cualificación, medios y recursos pertinentes.

Al margen de la coordinación del Responsable de Seguridad, deben ser asignadas al personal correspondiente el resto de responsabilidades en materia de seguridad.

Para cada una de estas funciones debe quedar perfectamente determinado el responsable encargado de su cumplimiento, quién a su vez, deberá ser conocedor de las tareas que le han sido asignadas mediante la difusión de las obligaciones en materia de seguridad.

Todo el personal que trate datos automatizados de carácter personal en la organización (personal de plantilla, contratados externos, personal de mantenimiento, becarios, consultores y asesores externos, etc.) deberá conocer sus implicaciones en materia de seguridad. Sirva como ejemplo la imposibilidad de mantener una adecuada política de actualización de contraseñas o el correcto funcionamiento del registro de incidencias (más abajo analizado) cuando los empleados desconocen las normas establecidas por la organización.

Es fundamental para garantizar la seguridad de la entidad la difusión a todo el personal de aquella parte del documento de seguridad que afecte al desarrollo de su trabajo. Los cursos de formación, campañas de sensibilización, cláusulas contractuales o circulares divulgativas son herramientas que permiten la difusión de las obligaciones en materia de seguridad y que, a su vez, servirán para cumplir con lo dispuesto en el artículo 9.2. del Real Decreto 994/1999, si se incluyen las responsabilidades del personal en caso de incumplimiento.

Como conclusión, establecer que cada vez es más patente, la necesidad (en cualquier organización independientemente del tamaño de la misma) de la designación de responsabilidades entre el personal respecto a la seguridad. En este sentido, es muy recomendable que la difusión de estas responsabilidades se efectúe, más que de forma impositiva, con ánimo de convencer a los empleados sobre la necesidad organizativa y legal de implementar procedimientos de seguridad. En la realidad de muchas empresas, sobre todo en sectores con mucha actividad sindical, la política de seguridad se lleva al marco de la negociación colectiva, buscando un consenso con los empleados que apoye la eficacia del mensaje y que facilite su asimilación. Aspectos como el uso de Internet y del correo electrónico suelen ser delicados, dada su situación alegal, y están sujetas habitualmente a tensiones con las organizaciones sindicales, que ven como tiende a incrementarse el control sobre la actividad de los empleados. Una política de seguridad diseñada para buscar el entendimiento de sus motivaciones mediante el consenso entre los empleados facilita no sólo una mejor comprensión de la misma, sino también un mayor grado de cumplimiento interno.

Adicionalmente, la ISO 17799 determina la conveniencia de formalizar un procedimiento disciplinario para el personal que viole la política y procedimientos de seguridad de la organización. La principal finalidad es el factor disuasor para todos aquellos empleados que pudieran desatender la política y procedimientos de seguridad.

Asimismo, se establece una relación con el apartado de conformidad legal de la norma (relativa a la obtención y retención de medios de prueba) en el sentido de asegurar un correcto tratamiento de situaciones detectadas con empleados sospechosos de incumplimiento.

4. El tratamiento de datos de los empleados y los procesos de selección

La ISO 17799 establece que el personal que tenga asignadas responsabilidades definidas en la gestión de la seguridad de la información debe ser competente para llevar a cabo las tareas necesarias con base en la educación, formación, habilidades y experiencia apropiadas.

Así, se establece como buenas prácticas en seguridad realizar una serie de comprobaciones al candidato en el momento de solicitar trabajo (al igual que el personal temporal o subcontratado)

Por otra parte, respecto a los trabajadores de plantilla fija, también se establece comprobaciones en el momento de promocionarse internamente o solicitar un puesto de trabajo. Dichos controles deben ser más estrictos en función de si el trabajo solicitado implica acceso a información sensible para la organización.

En definitiva, se trata de establecer una política de personal que establezca controles (principalmente comprobaciones y confirmaciones de actitud, experiencia y profesionalidad) para evitar riesgos en la seguridad de la información.

Finalmente, la norma internacional referencia supuestos (conocimiento por los directivos de las circunstancias privadas de su personal que pudieran afectar a su trabajo) que podrían chocar con la legislación vigente en materia de protección de datos, aunque dicha colisión se salva con una mera referencia al cumplimiento de la legislación aplicable en el manejo de dicha información.

Todo lo anterior, da pie a analizar la situación actual del uso de la tecnología en el ámbito laboral, en una doble vertiente:

- En la fase de contratación, (sobre todo en lo relativo al proceso de selección de personal),
- En el desarrollo de la relación de trabajo, en donde por medio del uso de las nuevas tecnologías se produce un aumento del poder de control del empresario sobre la prestación de trabajo y sobre el propio trabajador.

El ordenador se emplea no sólo como instrumento para desempeñar una actividad productiva, sino que al mismo tiempo, servirá de mecanismo de control de la prestación laboral ejecutada por el trabajador.

Es evidente que la introducción de la tecnología informática en la empresa representa una serie de ventajas tanto organizativas como de gestión, pero su utilización ilícita supone un

riesgo para determinados derechos fundamentales de la persona y en especial para el derecho a la intimidad del empleado.

La información va a cobrar una relevancia especial en el proceso de contratación laboral y singularmente en el momento de la selección por el empresario de sus trabajadores.

El empresario que lleve a cabo una gestión informatizada del personal, puede utilizarla para que todos los datos concernientes a un trabajador, o a un candidato (que posteriormente ingresa en la plantilla fija de la organización), desde el momento de su constitución, hasta el momento de su rescisión, sean incluidos en las bases de datos de la empresa.

El empleador debe tener presente los riesgos que esto entraña y la legislación que el Ordenamiento Jurídico proporciona a esta faceta de la intimidad, teniendo en cuenta las intromisiones indeseadas en la privacidad del individuo y su utilización ilegítima.

En el supuesto que nos ocupa, el objeto de este derecho es la facultad del trabajador de conocer y controlar cuantas transacciones y operaciones se realizasen con sus datos, así como la facultad de decidir sobre dichas operaciones a través del otorgamiento informado de su consentimiento, poniendo en sus manos cuantos instrumentos de defensa prevea el ordenamiento, convirtiendo al propio trabajador titular de los datos en el más eficaz garante de su intimidad.

El legislador español ha tenido en cuenta la necesaria protección del tratamiento automatizado de los datos de carácter personal en la fase previa a la contratación laboral, así quedo de manifiesto en la Exposición de Motivos de la ya derogada LORTAD, en cuanto que se afirmaba lo siguiente: "….*el conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona (…) y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como puede ser la obtención de un empleo*…".

Se considera legítimo el derecho del empresario a procurarse la mayor información posible del candidato. Información que permita evaluar en el candidato, si este reúne las aptitudes y la capacidad profesional necesaria para el puesto que quiere que ocupe.

Por tanto, en condiciones normales la finalidad a la que debe responder la recogida de información del demandante de empleo es la valoración de la capacidad profesional del candidato.

El peligro surge cuando la organización en la recogida de información del candidato, obtiene más datos de los necesarios y alcanza aspectos de la vida de los solicitantes de

empleo irrelevantes o no influyentes para la determinación de su aptitud y capacidad profesional.[3]

Es importante que la organización tenga en consideración la existencia de una serie de datos que a efectos de la LOPD, poseen una especial protección: los denominados *"datos sensibles"*. Se trata de datos estrechamente vinculados a la dignidad y personalidad humana, que se encuentran ya garantizados a través de otros derechos fundamentales de la Constitución Española,(en especial los arts. 16 y 18 de la C.E.).

Además, estos derechos son protegidos específicamente en el ámbito laboral, dado que en la práctica habitual de las empresas han sido utilizarlos de forma discriminatoria a la hora de seleccionar a candidato o trabajador:

- El art. 4.2.c) ET determina que en la relación de trabajo, los empleados tienen derecho a no ser discriminados por razones de sexo, raza, ideas religiosas o políticas, afiliación o no a un sindicato, disminuciones físicas, psíquicas y sensoriales
- El art. 17.1 ET establece la nulidad de todo pacto individual o decisión unilateral del empresario que contenga discriminaciones favorables o adversas en el empleo, en materia de retribuciones, jornada y demás condiciones de trabajo.

La LOPD, en el art. 7, bajo el epígrafe *"datos especialmente protegidos",* recoge aquellos datos que el legislador les ha querido dar un trato diferenciado por considerar que merecen una especial protección al vincularse más directamente a la dignidad, personalidad e intimidad de la persona.

Gozan de esa especial protección las siguientes categorías de datos:

1) datos sobre la ideología, religión o creencias
2) datos relativos al origen racial, la salud y la vida sexual.
3) datos personales referentes a infracciones penales o administrativas.

Respecto a los datos de la primera categoría, y trasladado al ámbito laboral, significa que el empresario no podrá investigar este tipo de datos y en el caso de requerirlos, el trabajador podrá negarse a suministrarlos sin que deriven consecuencias negativas de su decisión (adicionalmente, es obligación del empresario advertir de su derecho a no prestar consentimiento -expreso y por escrito- para el tratamiento de los mismos).

En cuanto a las informaciones relativas al origen racial y nacionalidad del trabajador, resulta necesario para el empresario y la Administración conocer la nacionalidad del trabajador, a efectos de la concesión y renovación de los permisos de trabajo y residencia.

[3] El ámbito de aplicación de la LOPD se hace extensivo a los ficheros de datos personales, ya sean automatizados o no. Es decir, esta Ley también se aplica a los ficheros manuales (Disposición Adicional Primera LOPD).

El problema que puede traer a colación la nacionalidad de origen, es el origen racial, así como las convicciones religiosas de los interesados, pudiendo originar actitudes racistas difícilmente verificables.

Con respecto al dato sobre la vida sexual del trabajador, el empresario tiene prohibido investigar, acceder o tratar automatizadamente o no, informaciones relativas a los comportamientos sexuales de sus empleados. Esta información se considera perteneciente a la esfera más intima del trabajador y no da lugar a dudas (como ocurría en el caso anterior) que la convierta en necesaria para el conocimiento del empresario.

Respecto a los datos de salud del trabajador, el legislador ha considerado que se trata igualmente de información sensible y merecedora de una especial protección. En este sentido, el ordenamiento laboral se ha hecho eco de la importancia de la misma y existen distintas normas donde se refleja la obligación de la empresa por garantizar la seguridad y salud de los trabajadores en el desempeño de sus funciones.

La Ley de Prevención de Riesgos Laborales (LPRL) establece en su art. 22, las medidas de vigilancia y control periódico del estado de salud del trabajador, fijando los términos en que deben realizarse dichas medidas.

Respecto a los datos de salud de los trabajadores, que el empresario puede manejar, se trata de información estrictamente necesaria, para los deberes contractuales y la garantía de salud de los mismos. El empresario sólo tendrá acceso a la información de las conclusiones en cuanto a la aptitud de los empleados para el desempeño de su puesto de trabajo, en cuanto a la necesidad de mejorar o introducir las medidas de protección y al desarrollo correcto de las funciones en materia de prevención.

La información que sobre la salud del trabajador se obtiene a través de la realización de controles médicos periódicos pertenece a su esfera privada y el uso que de la misma se haga, puede tener repercusiones para su situación personal y profesional.

La última categoría de datos sensibles es la información referente a las infracciones penales y administrativas. Estos datos se considera que pueden tener un papel importante en el ánimo del empresario.

La LOPD es tajante al excluir la posibilidad de que dichos datos estén incluidos en ficheros privados (sólo pueden estar en disposición de la Administración Pública). Por otra parte, aunque la ley no hace referencia a las infracciones estrictamente laborales del trabajador, sancionadas en base al poder disciplinario del empresario, a falta de mención expresa puede entenderse permitido su tratamiento informático.

En la actualidad es latente la problemática que existe, en cuanto a los riesgos que debe asumir el empresario en el proceso de selección de candidatos y el posterior tratamiento de los datos.

Hay que tener muy presente el principio de calidad de los datos (artículo 4 LOPD), en cuanto a que la información que obtenga el empresario, debe ser adecuada, pertinente y no excesiva en relación con el ámbito y la finalidades legitimas para las que se hayan obtenido. Todo ello, sin olvidar que los datos deben de ser exactos y puestos al día, de manera que sean veraces y respondan a la situación actual de los candidatos y trabajadores.

Esta ultima condición, suele ser olvidada por las organizaciones, en cuanto a la práctica habitual de acumular Currículum Vitae de candidatos y trabajadores, durante un tiempo indeterminado (en ocasiones durante años sin existir procesos de selección), de manera que se mantienen información desactualizada.

Una vez finalizado el proceso de selección, las empresas no deberían mantener los datos de aquellos candidatos que han sido desestimados, en cuanto que la finalidad para la que fueron obtenidos ya ha finalizado.

5. La utilización por los trabajadores de las Tecnologías de la Información y la Comunicación en la empresa

La evolución de las nuevas tecnologías y la comunicación (fundamentalmente Internet) ha motivado el nacimiento de problemas jurídicos hasta ahora inexistentes en las organizaciones. Centrándonos en el uso del correo electrónico e Internet por los empleados en el centro de trabajo, para fines distintos del desempeño de su actividad laboral, pueden señalarse dos problemas coligados entre sí:

1. La legalidad de su uso para fines no empresariales.
2. La legalidad de las medidas de control y revisión del correo electrónico de los trabajadores (como remitentes o destinatarios) por las empresas.

Así, las empresas detectan que sus trabajadores pueden estar utilizando la infraestructura informática implementada con cargo a la empresa, para disponer de conexiones a Internet y correo electrónico con motivos ajenos a la actividad productiva (por ejemplo, búsquedas de empleo, publicidad, ocio, etc.). Esta situación supone un importante coste económico para la entidad, riesgo de perjuicio en la imagen de la empresa, e inclusive un deterioro de la infraestructura informática implantada en la organización, por su anormal funcionamiento (saturación de mensajes personales de los empleados), amén de una puerta de entrada a código malicioso (virus, troyanos, programas espía, *malware* en general)

La propia navegación por Internet lleva aparejados unos riesgos para la seguridad de la organización que justifican el control de la misma; de ahí la extensión de sistemas de control de navegación que registran el uso de Internet de los usuarios, amparándose en la posibilidad de descargarse inadvertidamente códigos maliciosos que pueda causar daños contra la confidencialidad, integridad y disponibilidad de la información (Java, Active X, Javascript, etc).

En este orden de ideas y como aspecto relevante, cabe destacar la vía de riesgo que se introduce en las organizaciones por el uso de programas de intercambio de ficheros P2P que principalmente causan un perjuicio económico en la empresa por consumo de ancho de banda no justificado. Por ello, se recomienda la prohibición expresa de instalación de cualquier programa informático sin la debida justificación y previa autorización del Departamento de Informática.

Las soluciones habituales adoptadas por las empresas consisten en establecer medidas de control y prevención del uso abusivo del correo electrónico e Internet (revisión periódica de los e-mails enviados y recibidos, establecimiento de alertas o restricciones de acceso en correos o en la navegación por Internet que se activan por el uso de palabras concretas, etc.)

En este sentido se plantea el siguiente problema: Ante la falta de un pronunciamiento legal específico y la existencia de jurisprudencia dispar e inclusive contradictoria, surgen problemas jurídicos relativos a la constitucionalidad de las medidas de control empresarial y la legalidad de las medidas disciplinarias (sanciones o despido) que puedan derivarse al poder constituir una vulneración del derecho a la intimidad y al secreto de las comunicaciones del trabajador.

En realidad, cualquier empresa gestiona sus ordenadores a través de un sistema de red. Estos sistemas contienen servidores de corro electrónico para gestionar el correo interno y externo de la empresa. Es decir, cuando se crea y se manda un correo, éste pasa siempre por el citado servidor, donde se almacena, filtra y se distribuye (utilizando la información de control del correo). Este mismo proceso se realiza con el correo entrante en la empresa (actualmente ya no sólo se guarda la información de control del mensaje, sino también su contenido, realizando sobre el mismo procesos de filtrado). Para un completo control, simplemente es necesario instalar un software en el servidor de correo, con programas configurables en función de las necesidades de la empresa. Así, se fijan las normas a seguir y los filtros a aplicar (cada norma establecida se traslada al programa como una condición o criterio de búsqueda)

Los filtros pueden ser de cualquier tipo: dirección de remitente o destinatario determinado, un dominio (empresa de la competencia, etc.), la dirección IP, que el mensaje contenga determinada palabra clave (por ejemplo: currículo, sexo, bomba, proyecto, confidencial, etc.), el tamaño, el formato del fichero anexado (mp3, avi, pdf, exe, ect.), la presencia de virus...

Así mediante estos filtros, cuando se detecta el cumplimiento de las condiciones preestablecidas, automáticamente se ejecuta la correspondiente acción prediseñada (bloqueo del envío, envío de copia del correo al buzón del superior jerárquico, etc. (normalmente, los filtros utilizados exceden de la mera función de inspección o control estadístico sobre el uso o frecuencia de la utilización del correo).

No debe olvidarse la figura del Administrador o encargado de los servidores de correo que mediante un perfil de superusuario, tiene acceso a los archivos log y puede acceder a las

cuentas de correo sin conocimiento del trabajador afectado (violaciones de derechos de trabajadores).

En la relación empresa-trabajador, la Ley otorga al empresario el poder de dirección y control de la actividad, permitiéndole adoptar las medidas oportunas para comprobar el cumplimiento de las obligaciones laborales del trabajador.

Los medios son propiedad de la empresa y están puestos a disposición de los trabajadores exclusivamente para el desarrollo de la actividad empresarial. Pero los actos realizados como organizador y propietario de los medios de la empresa, deberán tener como límite el respeto de los derechos fundamentales del empleado.

La potestad del empresario de adoptar medidas de vigilancia y control para verificar el cumplimento de las obligaciones del trabajador, reconocida en el artículo 20.3 del Estatuto de los Trabajadores, viene limitada por el respeto a la dignidad humana.

Entre los derechos fundamentales de la persona reconocidos en la Constitución, en estos supuestos, entran en juego dos relacionados entre si:

a) Derecho a la intimidad personal.

b) Derecho al secreto de las comunicaciones.

El derecho fundamental a la intimidad personal consagrado en el artículo 18 de la Constitución se configura como derecho vinculado a la propia personalidad, derivado de la dignidad de la persona, que reconoce el artículo 10.1 de la Constitución y que ha sido entendido por el Tribunal Constitucional como el reconocimiento de "*la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana*".

Asimismo, el artículo 18.3 de la Constitución garantiza el secreto a las comunicaciones: "*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*". El bien constitucionalmente protegido es la libertad de las comunicaciones y la reserva sobre la comunicación emitida, con independencia del contenido de la misma, habiendo afirmado el TC que "*el derecho puede conculcarse tanto por la interceptación en sentido estricto como por el simple conocimiento antijurídico de lo comunicado*".

Así, cualquier medida de control o vigilancia del empresario que suponga una restricción de la intimidad, debe cumplir un doble requisito:

- que la medida esté estrictamente relacionada con el desarrollo de la actividad empresarial
- que no exista otra medida alternativa menos lesiva para la privacidad del trabajador.

La doctrina del TC ha sido muy clara al mantener que "*el ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir en ningún caso a la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador, ni a la sanción del ejercicio legítimo de tales derechos por parte de aquél*". Y también se ha reiterado que en los casos en que se planteen conflictos donde haya derechos fundamentales en juego, debe ponderarse, mediante la aplicación del principio de proporcionalidad, si la medida respeta el derecho. Ello supondrá analizar si la medida es adecuada para conseguir el objetivo que se pretende, y si no existe otra medida que pueda alcanzar el mismo objetivo sin producirse tal restricción del derecho.

El ordenador es instrumento de la empresa, no pudiendo ser usado para fines personales, pero esto no impedirá garantizar el respeto al derecho del trabajador a mantener su intimidad.

Se considera que los mensajes de correo electrónico del trabajador son "efectos particulares", pese a no existir pronunciamiento de los Tribunales.

A la luz de la interpretación del artículo 18.3 CE, puede afirmarse que el correo electrónico es un medio de comunicación amparado por el derecho fundamental al secreto en las comunicaciones , ya que se trata de un "canal cerrado" que genera expectativas de secreto (para acceder al mensaje se precisan una serie de acciones conscientes dirigidas a su apertura (por parte del destinatario) o interceptación (por terceros)

Por el hecho de ser el correo electrónico un medio de comunicación, debe tener la necesaria protección frente a la intromisión externa. Además existen elementos que exteriorizan el carácter privado del correo electrónico en la empresa (contraseña o clave de acceso personal). En este sentido, pese a no ser incluido en la redacción del artículo 18 CE, se protege el secreto de la comunicación, con independencia del medio utilizado.

Una muestra de la importancia de estos derechos la encontramos en la protección penal que otorga el artículo 197 CP, donde se equipara el correo postal y el electrónico. “El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses."

Este delito puede cometerse en la empresa, pudiendo darse el caso de denuncia penal de un trabajador a su superior jerárquico.

6. Correo Profesional y Correo Particular:

La interceptación ordinaria e indiscriminada del correo electrónico de los trabajadores en las empresas debe considerarse fuera de la legalidad, en base a la doctrina constitucional

anteriormente expuesta. Deberán tener diferente consideración, no obstante, el correo electrónico proporcionado por la empresa (tipo trabajador@empresa.es), y aquel de uso particular del trabajador, contratado por él mismo al margen de su relación laboral con la empresa (tipo trabajador@terra.es, etc.) en horario laboral.

Es claro que el correo proporcionado por la empresa debe destinarse a un uso profesional al considerarse un elemento de trabajo propiedad de la organización, no pudiendo en consecuencia utilizarse para fines particulares, excepto casos concretos y siempre justificados.

La facultad de control de la empresa sobre el correo electrónico deberá limitarse a comprobar si realmente se utiliza el correo electrónico para el fin para el que se destinó, sin más intromisión, que sería a todas luces ilegítima.

En todo caso debe mantenerse la privacidad de los mensajes, sin que un acceso indiscriminado a los mismos sea aceptable. El simple hecho de ser el correo electrónico una herramienta de trabajo proporcionada por la empresa, no es motivo para que la interceptación del mismo sin la debida justificación pueda considerarse lícita. Es decir, por tratarse de una dirección de correo atribuida por la empresa con fines laborales y ser utilizada con finalidad privada, no parece justificable la lectura de un correo electrónico de índole privada, pero si lo es que el uso de herramientas laborales con fines privados pueda ser sancionado por el empresario con su potestad disciplinaria.

El acceder de manera indiscriminada al contenido de los correos salientes o entrantes, no estaría justificado, más que con las garantías de llevarse a cabo durante la jornada laboral y en presencia del representante de los trabajadores, tal como señala el Estatuto de los Trabajadores para los registros en el trabajo (art. 18. "*Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo.*

En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible."

Si la empresa quiere evitar la utilización del e-mail con fines personales o privados, deberá establecer reglas que aclaren que el e-mail de los trabajadores de la empresa es un instrumento de trabajo y que no es un instrumento idóneo para las comunicaciones personales, mediante su adecuada difusión en la política de seguridad.

Respecto al correo electrónico particular del trabajador, la cuestión más importante es determinar si su uso está o no permitido. Es decir, la organización puede imponer (aplicando su poder de dirección) la prohibición de su uso o la restricción que se estimen oportunas,

sancionando los incumplimientos (que podrá abarcar desde una amonestación, suspensión de empleo y sueldo, hasta el despido). Pero tanto si se permite su uso, como si no, cualquier acceso al contenido de los mensajes sería contrario al secreto de las comunicaciones, y solo podría producirse en virtud de orden judicial.

En conclusión, las empresas lo que suelen establecer son unas reglas que aclaren que el e-mail (al igual que el acceso a Internet) de los trabajadores de la empresa es un instrumento de trabajo y que no es un instrumento para uso privado o personal, salvo supuestos excepcionales y tasados previamente. No obstante, puede llegar a posturas intermedias respecto a su uso o la utilización de correos particulares del empleado (fijar una franja horaria del día –hora de comida, etc.- donde o bien se permita al trabajador el uso de correo de empresa con fines privados, o bien se habilite la posibilidad al trabajador de acceder a direcciones de correo contratadas por el titular. Todo ello dictando en una normativa conocida por los empleados con carácter previo.

En este sentido, destacar la doctrina de Don Miguel Ángel Davara, catedrático de la Universidad Pontificia de Comillas, en la IV Semana Internacional de las TIC (junio del año 2004) que durante su exposición manifestó que el Estatuto de los Trabajadores avala el que las propias empresas puedan realizar un control de los medios de los que han dotado al empleado para desempeñar su trabajo, siempre que tenga una justificación clara. Estas inspecciones, tanto de los mensajes de correo electrónico como del uso de Internet, siempre serán lícitas si el trabajador conoce de antemano que se están llevando a cabo. Es en este punto donde es posible encontrar un conflicto entre los intereses del empresario y del trabajador.

7. Uso de acuerdos o cláusulas de confidencialidad.

La fuga de información de las empresas, es un problema habitual a día de hoy y es cada vez más frecuente la utilización de salvaguardas basadas en acuerdos de confidencialidad o no divulgación de la información clasificada como secreta o confidencial.

El deber de fidelidad y el de buena fe, son intrínsecos al contrato de trabajo. No obstante, las empresas insertan o anexan a las condiciones de trabajo suscritas contractualmente con sus empleados, cláusulas adicionales de este tipo. Así, si existe constancia por parte del empresario que han sido vulneradas las responsabilidades asumidas por parte los trabajadores se sanciona con el despido.

Un ejemplo práctico de este tipo de salvaguardas de seguridad de la información, la encontramos en el artículo 10 de la LOPD, donde se plasma el deber de secreto restringido a los datos de carácter personal. En este sentido, la normativa legal establece que el responsable del fichero y quienes intervienen (como empleados o como prestadores de

servicio) en cualquier fase del tratamiento de este tipo de datos, están obligados al secreto respecto de los mismos y al deber de guardarlos.

El empresario como responsable de la información, tiene que adoptar una adecuada política de confidencialidad respecto a los datos de carácter personal con la finalidad de garantizar el obligatorio deber de secreto.

Esta obligación no se acaba en el momento de finalizar las relaciones con el responsable del fichero, sino que subsisten aun después de cancelados o anulados los datos y los ficheros, y tras la finalización del contrato laboral. No obstante, se recomienda limitar el plazo de mantenimiento del deber de secreto recogido en la LOPD como uno de sus principios generales.

Respecto a no empleados (recursos humanos externos o usuarios de terceros) que para prestar un determinado servicio necesitan acceder a este tipo de información, la LOPD amplía el alcance de dicho principio con el artículo 12 del citado precepto legal, donde los requisitos regulados para acceder a datos titularidad de terceros, recoge implícitamente el necesario deber de secreto.

Atendiendo a la ISO 17799, este deber de secreto debe entenderse ampliado a cualquier tipo de información de la organización, pero el contenido de esta buena práctica en seguridad es el mismo que el analizado respecto a la LOPD.

Pese a que lo ideal es firmar las cláusulas de confidencialidad antes de acceder a la información (en el momento de la firma del contrato de trabajo para el personal interno, o en el momento de iniciar el acceso a la información, cuando se trata de recursos humanos externos o usuarios de terceros donde no existe un contrato laboral), aquellas organizaciones que deseen adoptar una correcta gestión de la seguridad de la información deberán realizar acciones a posteriori encaminadas a tal fin.

Es preciso señalar que no resulta operativo el establecer un clausulado tipo para todo el personal de la organización, sino que deberán elaborarse diferentes acuerdos en función del trabajo y responsabilidades asumidas por los trabajadores, debiendo ser revisadas cuando los términos del empleo o contrato cambien.

8. Formación de usuarios

El mundo de la seguridad de la información es cambiante y las amenazas a la seguridad y la tecnología no se detienen. Por este motivo, el aprendizaje de los empleados no debe desatenderse.

Resulta necesario llevar a cabo una labor formativa que sea efectiva, de manera que los empresarios aseguren a sus empleados una formación adecuada en seguridad.

La formación es imprescindible para asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad. No debe olvidarse que la política de seguridad debe ser asequible a todos los empleados porque, en ultima instancia, ellos son responsables de su éxito y deberían recibir formación en procedimientos de seguridad y en el uso correcto de los recursos de tratamiento de información para minimizar posibles riesgos.

Un usuario educado en seguridad es la base de cualquier entorno fiable en la seguridad de la información. Sin una adecuada educación se convierte en el eslabón más débil, que rompe cualquier política de seguridad.

Tal y como se reflejaba en el estudio relativo a la inversión en seguridad de la información expuesto en el Capítulo de "Organización de la Seguridad" del presente manual, el esfuerzo de las entidades debería centrarse fundamentalmente en aspectos procedimentales (40%) y formativos (40%), siendo la parte tecnológica (securización de los sistemas actuales y mantenimiento diario) una parte minoritaria en el proceso de gestión.

Las organizaciones deben promover la formación en seguridad para actualizar el conocimiento, lo cual podría realizarse de diferentes formas: entrenamiento al personal, asistencia a conferencias o foros de seguridad, obteniendo certificaciones o recabando los servicios de educadores de seguridad externos.

Uno de los denominadores comunes a cualquier propuesta de divulgación de la seguridad debe ser el uso de mecanismos que estimulen e incentiven la percepción del mensaje. Además de los programas de formación específicos para cada uno de los niveles de seguridad, un programa de concienciación y sensibilización sobre la seguridad debe incluir elementos humorísticos que hagan más llevadera la asimilación de los mensajes de la seguridad, generalmente prohibitivos y restrictivos en general. Algunos ejemplos de esta tendencia sería el uso de trípticos, posters y gráficos con viñetas humorísticas, mini-aplicaciones desarrolladas en formatos gráficos (flash, por ejemplo), juegos de seguridad con incentivos económicos para los propios empleados, creación del "Día de la Seguridad", etc...Todo ello contribuye a crear un ambiente receptivo y una percepción positiva que, incide, en último término, en la motivación del empleado en el cumplimiento de los procedimientos de seguridad.

Adicionalmente, la difusión y formación deben ser específicas para los distintos perfiles de empleados dentro de la organización, intensificándose en función del trabajo desempeñado y el acceso al tipo de información requerida por el usuario y sus responsabilidades (por ejemplo, un administrador de sistemas no necesita la misma formación en seguridad que un simple grabador de datos).

En este sentido, es importante que los miembros del Área de Seguridad (Departamento TI), o al menos alguno de ellos, posea certificaciones en seguridad no sólo por reflejar

conocimiento de los problemas de seguridad, sino también porque la mayoría de las certificaciones implican cursos de educación o reciclaje continuado para conservar la propia certificación. Así, la organización se garantiza que su personal certificado refresca conocimientos y actualiza las nuevas tendencias en amenazas, tecnología y mejores prácticas en seguridad.

Existen diferentes credenciales de seguridad, aunque la más conocida es la Certified Information Systems Auditor (CISA) que además de requerir una previa experiencia profesional en seguridad, requiere la asistencia anual a un número de horas de formación.

Así, la organización debe proporcionar formación o tomar cualquier tipo de acción para satisfacer dichas necesidades, evaluar la eficacia de las acciones formativas realizadas y asegurarse que su personal se encuentra sensibilizado de la pertinencia e importancia de sus actividades y como contribuyen en el logro de los objetivos de seguridad marcados. Todo ello dentro de un marco de un proceso continuo, que debe ser evaluado y medido en el tiempo, por medio de una serie de métricas relacionadas con la eficacia de la divulgación de la seguridad. Como ejemplos de alguna de estas métricas podemos citar la verificación del porcentaje de usuarios con conocimientos suficientes de la política y procedimientos de seguridad, el ahorro en costes/hora hombre por la reducción de pérdidas por incidentes internos (errores humanos), etc.

9. Respuesta ante incidencias y malos funcionamientos de la seguridad

El objetivo de esta buena práctica en seguridad se encamina a minimizar los daños provocados por incidencias en seguridad y por malos funcionamientos, al fin de controlarlos y aprender de ellos para limitar su frecuencia, daño y coste de futuras ocurrencias.

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad de la información, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

Como paso previo y punto de partida, debido a que las entidades requieren conocer y recoger cuantas incidencias de seguridad se produzcan sobre el sistema, a tal objeto, se deberá presentar al menos, una lista de lo que se consideran incidencias y malos funcionamientos en seguridad y que serán inexcusablemente registradas por todos los usuarios del sistema (internos o externos). Esta lista inicial podrá (y deberá) ser ampliada con otro tipo de incidencias que pudieran haber quedado omitidas, o que se detecten posteriormente en base en la experiencia en gestionar la seguridad.

El mantener un registro de las incidencias que comprometan la seguridad de la información es una herramienta imprescindible para la prevención de posibles ataques a la seguridad, así como para persecución de los responsables de los mismos.

A continuación se recogen, con carácter general, las directrices que debe contener un adecuado procedimiento de gestión de incidencias:

- Aplicable a cualquier persona que forme parte de la plantilla de la empresa o se halle prestando sus servicios temporalmente en la misma.
- Obligación de informar o notificar inmediatamente al/los responsable/s de Seguridad cualquier anomalía que detecte y que afecte o pueda afectar a la seguridad de la información.
- Información relativa a que el retraso en la notificación de incidencias constituirá un quebranto de la buena fe contractual, sancionable según la normativa laboral aplicable.
- Identificación de los diferentes medidos para notificar incidencias, aunque se recomienda el deber de notificarla además siempre por escrito. A modo de ejemplo, se señalan los diferentes canales de comunicación: comunicación en persona, a través del móvil o teléfono directo, e-mail del responsable de Seguridad designado en la organización.
- El Responsable recibirá las notificaciones de las incidencias y las comunicará a los técnicos internos o externos encargados de la seguridad del sistema. Dicho responsable se asegurará que los técnicos dan respuesta a la incidencia detectada en el periodo de tiempo dispuesto para ello. Además supervisará el trabajo de subsanación de la anomalía detectada (gestionar las incidencias que pudieran producirse, en el menor tiempo posible, garantizando, en todo caso, que la seguridad de la información no se vea alterada en ningún momento)
- Asimismo, es obligación del Responsable de Seguridad mantener un registro de las incidencias en el cual debe constar, al menos, la siguiente información relativa a las mismas:

    - Tipo de incidencia.
    - Momento en el cual se ha producido la incidencia.
    - Persona que realiza la notificación.
    - Persona a quién se le comunica
    - Efectos derivados de dicha incidencia.

Es obligación del Responsable de Seguridad asegurarse de que el registro de incidencias se mantiene actualizado y se guardarán al menos las incidencias de los 12 últimos meses.

- Se recomienda adjunta en el procedimiento un modelo plantilla a utilizar para el registro de incidencias

Atendiendo al genérico procedimiento descrito, resulta de conformidad con el Real Decreto 994/1999, respecto a los ficheros con datos de carácter personal con nivel básico de seguridad.

http://www.tb-security.com

- **CAPÍTULO 3: SEGURIDAD DE LA INFORMACIÓN EN EL PUESTO DE TRABAJO**

"Conoce a tu enemigo y conócete a ti mismo. De esta manera, en cien batallas nunca estarás en peligro". "Cuando no conoces a tu enemigo pero te conoces a ti mismo, tus posibilidades de ganar o perder son iguales" "Si desconoces tanto a tu enemigo como a ti mismo, ten la certeza de que en cada batalla estarás en peligro."

Sun Tzu

El Arte de la Guerra

1. Introducción

El mundo de las telecomunicaciones ha evolucionado muy rápidamente en los últimos años, y en el campo en el cual ha sido especialmente rápido, es el de la informática. Por ejemplo el crecimiento en la capacidad de los ordenadores en los últimos veinte años ha sido imparable. El ordenador personal que usábamos hace doce años era quinientas veces más lento que el que usamos ahora (4MHz vs. 1.7 GHz); tenia un disco duro cuatro mil veces más pequeño (20Mb vs. 80Gb); y tenia ocho mil veces menos memoria RAM (64Kb vs. 512Mb). Por si fuera poco costaba el doble de lo que cuesta ahora (en euros constantes).

El software ha tenido un crecimiento aún más rápido. Microsoft lanzó Windows 3.0 en 1990 utilizando medio millón de líneas de código para su compilación, y cuando diez años más tarde lanzó Windows 2000 se jactaba de ¡25 millones de líneas de código! En resumen: la complejidad del software crece exponencialmente y su la fiabilidad es inversamente proporcional a su complejidad.

Por otro lado durante el vertiginoso desarrollo de la informática no se ha tenido en cuenta un aspecto clave: el usuario. La tecnología ha evolucionado más rápidamente que nuestra capacidad para asimilarla. Debido a que hoy en día una persona que no sabe utilizar la informática tiene difícil encontrar un puesto de trabajo, el usuario adopta la tecnología forzado, sin plantearse los riesgos que supone no conocer la herramienta que utiliza todos los días. En pocas palabras, la complejidad, rapidez y potencia de los sistemas, así como la poca formación de los usuarios, multiplican los problemas de fiabilidad y seguridad.

2. La evolución informática en los últimos años

Hace quince años la informática seguía un modelo centralizado. Un ordenador central daba servicio a varios terminales simples que no tenían capacidad de cálculo. Básicamente consistían en una pantalla y un teclado. En un entorno centralizado de este tipo, las cuestiones de seguridad no había que planteárselas.

Pero en 1975 se creó una pequeña empresa formada por dos estudiantes llamada Microsoft que cambió para siempre el curso de la informática. IBM pensaba lanzar al mercado un ordenador personal, y necesitaba software para hacerlo funcionar. Bill Gates había desarrollado un compilador de BASIC y había llegado a un acuerdo para suministrarlo a IBM pero necesitaba un sistema operativo para que funcionara, así que licenció a una empresa de Redmond un sistema operativo llamado DOS (Disk Operating System).

Los ordenadores que teníamos en 1982 sólo permitían hacer programas en BASIC, no tenian disco duro ni pantalla gráfica. Eran simples, y como daba igual cuántas veces tuviera que reiniciarlo porque no afectaba a otros usuarios, no tenia medidas de protección.

En esa época existía una ley en la informática que decía que para doblar la capacidad de cálculo de un ordenador había que cuadruplicar su precio (Ley de Moore). Esta ley venía a decir que un sistema centralizado siempre sería menos económico que un sistema distribuido. Y crear una red de área local para compartir recursos entre ordenadores personales permitía que un sistema duplicara su capacidad sin cuadriplicar su precio.

El crecimiento del número de ordenadores personales abarató su precio y se mantuvo un crecimiento extraordinario de las prestaciones. El entorno Wintel (Windows+Intel) durante los años 90 se ha convertido en un estándar mundial con más del 94% del mercado mundial de ordenadores.

Microsoft tenía una visión que ha mantenido desde 1985 hasta el año 2000: que existiría un ordenador personal en cada casa y en cada puesto de trabajo, y efectivamente lo ha conseguido.

3. La Seguridad: asignatura pendiente

A finales de los 90 y en esta década, los hábitos de flexibilidad adquiridos por los usuarios han dejado desprotegida a la organización. Los usuarios exigen la misma libertad de acción en la oficina que la que tienen en casa. ¿Cómo negarle al director que se lleve información a casa para seguir trabajando?

El problema es qué pasa si el director mañana se va a la competencia, por ejemplo. Probablemente en el ordenador de su casa tendrá información sensible de su ex-compañía. Pero no solo el director puede hacer esto, sino que cualquier empleado puede copiar información de la empresa utilizando un CD ROM y llevarse gigabytes de información de manera prácticamente indetectable.

Además el Administrador de Sistemas tiene acceso a toda la información de la red informática. ¿Cómo nos protegemos de él? Hay una serie de departamentos como el de personal, administración, la dirección general que manejan información a la que el administrador de sistemas no debería poder acceder.

Según el FBI el 85% de los delitos informáticos tienen que ver con personal interno de la compañía, no con ataques externos. Dentro de la organización existen empleados descontentos, y conocedores de cuáles son los ordenadores que contienen información más sensible. Como personal interno, tienen acceso físico a la misma red que quieren atacar. Sin embargo, el usuario tiende a creer que es Internet el que ha creado los problemas de seguridad, y que fuera de la organización existe un lobo feroz dispuesto a entrar. Es una falsa percepción.

Desde hace mas de diez años, tienen una red informática abierta que permite a cualquiera de los usuarios introducir un virus, robar información o contraseñas, suplantar a otros usuarios y, suplantando al administrador, tener un control sobre toda la información de la organización. Lo que viene a continuación son una serie de reflexiones sobre los problemas de seguridad comunes en las organizaciones.

4. Los virus informáticos

Viernes 13 acaparó medios de comunicación a finales de 1988. Se temía un desastre informático mundial, con todos los ordenadores dejando de funcionar. Ese año Carlos Jiménez, Presidente de Secuware, desarrolló el primer antivirus informático que repartió el ministerio de Economía y Hacienda de forma gratuita. Entonces Jiménez constituyo la empresa *Anyware*, que se convirtió en una de las cuatro empresas del mercado que fabricaban antivirus. Existían en ese momento treinta variedades virus informáticos en el mundo.

En 1990 apareció Windows 3.0 y ya entonces existían 800 virus. Un virus se reproducía lentamente porque no existía una interconexión entre ordenadores que permitiera una infección masiva. Hubo quien publicó libros que explicaban como fabricar un virus paso a paso, pero su difusión era muy limitada.

Sin embargo la aparición en 1995 de Windows 95 acercó Internet a cada ordenador. Entonces existían unos 5.000 virus, pero la información sobre virus se disparó. Cualquiera puede buscar en Altavista la palabra virus y le aparecerán siete millones de páginas con información. Hoy en día existen más de 110.000 virus informáticos y aparecen unos 800 nuevos cada mes. Incluso existen generadores de virus que permiten fabricar virus sin conocer nada de programación.

Internet, y especialmente el correo electrónico facilita que un virus se pueda propagar de forma muy rápida. En mayo del 2000 el virus “I Love You” contaminó decenas de millones de ordenadores en todo el mundo en menos de 12 horas. El efecto dañino de este virus es que intentaba robar contraseñas.

Con las tasas actuales de aparición de virus y con la rapidez de propagación utilizando el correo electrónico, un antivirus resulta inútil actualmente. A día de hoy sólo hay una alternativa para la protección efectiva frente a los virus: la firma digital de código.

5. La Firma Digital

Un antivirus tradicional detecta los virus que conoce a través de una base de datos con identificadores para los virus conocidos, la cual es necesario actualizar periódicamente, y así incorporar los nuevos. Su funcionamiento es el siguiente: cuando vamos a utilizar un programa, que hemos descargado de Internet, o recibido por correo electrónico, el antivirus comprueba si contiene un identificador de la base de datos, y si no contiene un virus conocido, permite operar con él.

El problema es que a la velocidad a la que se crean los virus actualmente, es probable que el programa que queramos hacer funcionar contengan un virus que todavía no haya sido registrado por nuestro antivirus. El resultado ya lo conocemos, es la infección de nuestro ordenador, nuestra herramienta principal de trabajo.

Sin embargo en el mundo físico no actuamos así. Desde que nacemos, vamos construyendo nuestra estructura de confianza. Nuestros padres nos enseñan en quién debemos confiar y nos enseñan que no hablemos con desconocidos. Nadie invitaría a su casa para jugar con sus hijos a un desconocido con el que se cruza por la calle. No tiene porque pasar nada malo, pero la mayor seguridad es la precaución.

Esa es la estrategia futura para resolver los virus: confiar en aquellos programas que conoce. Una organización utiliza software corporativo, que ha comprado y que ha elegido como el que mejor se adapta a sus necesidades. Además tiene soporte sobre ese software

corporativo, y si alguno de los usuarios esta utilizando software no corporativo, lo más probable es que sea ilegal o no deseado, como un juego, un programa pirata, un virus, un caballo de Troya, etc. Para resolver el problema de los virus de manera definitiva hay que autorizar lo que se conoce (el software corporativo) y desconfiar del resto (no interesa, tanto si es un virus como si no).

Y la manera de autorizarlo es a través de la Firma Digital de aquellos programas que un usuario está autorizado a usar, es una estrategia restrictiva, pero válida en una Organización. Este sistema además resuelve el hecho de que el usuario siempre tenga programas no autorizados (juegos, música mp3, DivX, video, etc.). Quizás por ello seria menos aplicable a usuarios domésticos. Aunque en nuestro caso, no nos importaría firmar digitalmente el software que viene con un ordenador que acabamos de comprar, sabiendo que si funciona hoy, va a funcionar siempre, sin que un virus o por error, borre un programa o deje de funcionar sin saber el motivo.

6. El mercado de la seguridad en España

En febrero del 2002, IDC publicó un informe sobre la seguridad en España que merece la pena comentar. De forma clara, la seguridad es un sector con perspectivas interesantes de crecimiento en un momento en el que las empresas de telecomunicaciones están sufriendo reestructuraciones importantes.

La previsión del mercado global de la seguridad en España es de una tasa de crecimiento anual del 29,7%, que es superior al crecimiento estimado para Europa 28,1%.

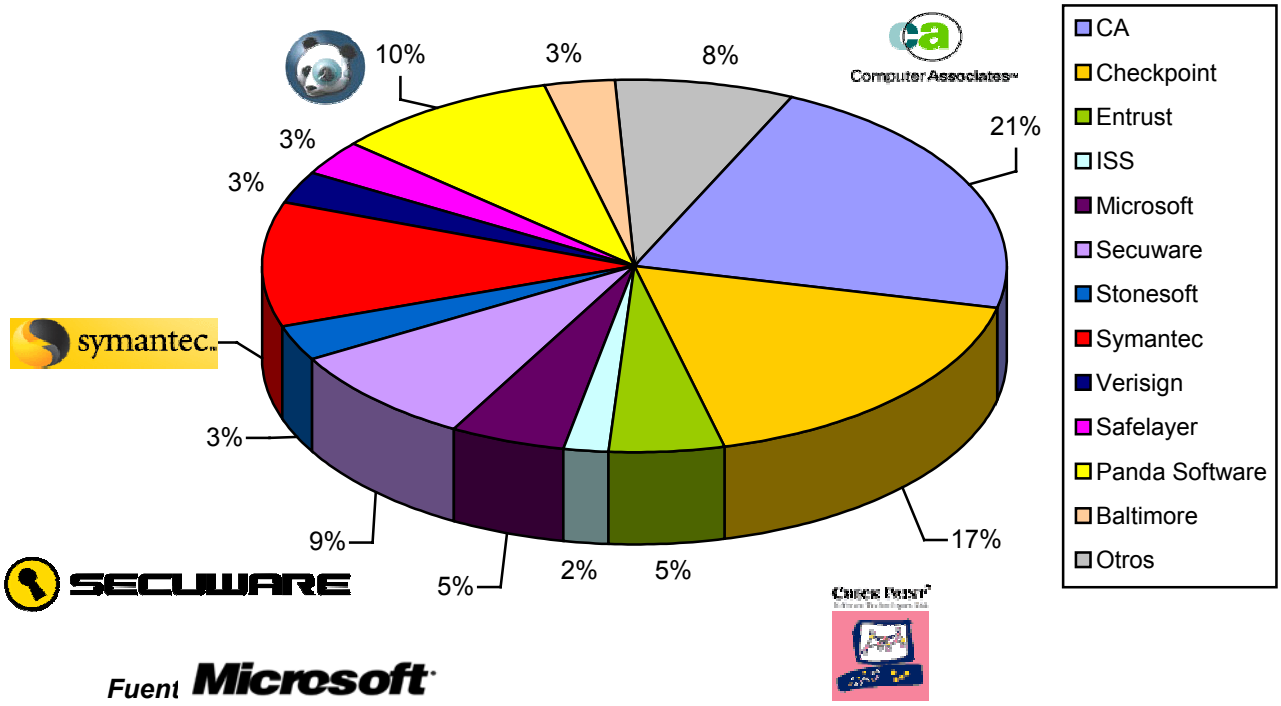
Mercado Total de la Seguridad en España

(Millones de Euros)

	2000	*2001*	*2002*	*2003*	*2004*	*2005*	*Crecimiento 2000-2005*
Software	47	57.2	73.1	91.6	111.3	135.9	23.7%
Hardware	16.5	26.6	42.9	64.6	88.4	113.8	47.8%
Servicios	54	67	78.1	116.1	144.5	177	26.8%
Total	117.5	150.8	194.1	272.3	344.2	426.7	29.7%

Fuente: IDC,2002

Los principales fabricantes de software de seguridad en España son:



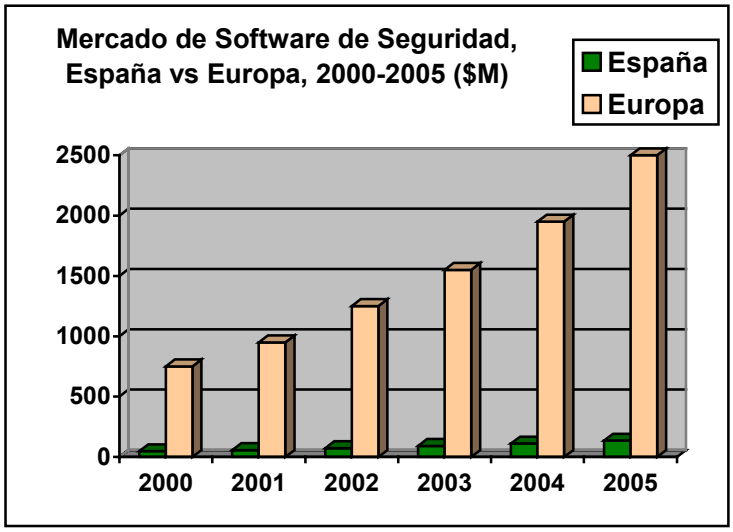
Fuent Microsoft

Estamos ante un mercado muy fragmentado donde no existe un denominador claro. Sólo si nos adentramos en los submercados podemos encontrar un claro dominio por parte de algunos proveedores. Así, mientras CA, Panda Software y Symantec comandan el mercado de antivirus y Checkpoint el mercado del firewall, Secuware y Microsoft se reparten el resto de áreas del mercado de seguridad.

Merece la pena destacar que dos de los seis fabricantes más importantes de seguridad son empresas españolas: Secuware y Panda Software, ambas con cuotas de mercado del doble que Microsoft. Y el informe de IDC recoge además que Secuware es el fabricante de mayor conocimiento técnico de todo el mercado.

El mercado de software de seguridad en España representa el 2,6 % del mercado total de software. Aunque hay que tener en cuenta que el índice de piratería en el mercado total de software en España es del 45,9%.

En comparación con el resto de Europa, la inversión en seguridad sigue siendo muy pequeña.



7. Conclusiones

La seguridad pasa a ser un elemento estratégico. La seguridad ha dejado de entenderse como un área reducida y supeditada al departamento de sistemas dentro de la empresa, para adquirir la condición de elemento estratégico. La seguridad se convierte en una cuestión que cruza transversalmente todas las áreas empresariales situándose en un nivel superior dentro del organigrama.

Transición del producto al servicio. En Europa la mayoría de los fabricantes de software están planeando migrar a un modelo de servicio. En España, esta tendencia no es tan acusada pero ya se empieza a percibir. Los fabricantes quieren cambiar las corrientes de ingresos hacia contratos de larga duración, lo que les permitirá bajar los costes de adquisición del cliente.

Securizar los dispositivos móviles: Próximo foco. La próxima gran ola de las aplicaciones de seguridad estará conducida por las aplicaciones móviles para dispositivos como los teléfonos móviles, teléfonos Web, PDA's, dispositivos de información o *wireless computers.* El cifrado, la PKI, autenticación, autorización y administración se convertirán en infraestructuras más críticas cuanto más nos dirijamos a entornos móviles.

Seguridad vs confianza. La palabra clave no será seguridad o protección sino *confianz*a. Los clientes necesitan tener confianza en que sus transacciones se llevan a cabo de una manera correcta y precisa, sin errores. Los comerciantes, bancos y partners deben tener la confianza necesaria en que sus transacciones no se realizan de manera fraudulenta y que no serán repudiadas con posterioridad.

SECUWARE

http://www.secuware.com

- **CAPÍTULO 4: SEGURIDAD FÍSICA Y DE ENTORNO**

1. Centros de datos seguros

Un *Data Center* es, tal y como su nombre indica, un "centro de datos" o "Centro de Proceso de Datos" (**CPD**). Esta definición engloba las dependencias y los sistemas asociados gracias a los cuales:

- Los datos son almacenados, tratados y distribuidos al personal o procesos autorizados para consultarlos y/o modificarlos
- Los servidores en los que se albergan estos datos se mantienen en un entorno de funcionamiento óptimo

Los primeros *Data Center*s se diseñaron siguiendo las arquitecturas clásicas de informática de red, en las que los equipos eran "apilables" en mesas, armarios o *racks*.

La necesidad de fácil gestión y de optimización del espacio han hecho que se evolucione hacia sistemas basados en equipos cuyas dimensiones permiten aprovechar al máximo el volumen disponible en los *racks* (**equipos "*enraca-bles*"**), logrando una alta densidad de equipos por unidad de espacio.

Los *Data Center* iniciales tampoco estaban diseñados para proporcionar **facilidades de red avanzadas**, ni los requerimientos mínimos de **ancho de banda y velocidad** de las arquitecturas actuales. La rápida evolución de Internet y la necesidad de estar conectados en todo momento han obligado a las empresas a requerir un **alto nivel de fiabilidad y seguridad**, de tal forma que se proteja la información corporativa y esté disponible sin interrupciones o degradación del acceso, con el objetivo de no poner en peligro sus negocios, sean del tamaño que sean. El cumplimiento de estos requisitos, cada día mas demandados, es posible dentro de un *Data Center*. Igual que un banco es el mejor sitio para guardar y gestionar el dinero, un centro de datos lo es para albergar los equipos y sistemas de información.

Ilustración. Equipos en alojamiento tradicional frente a equipos "*enracables*" de alta densidad.

Los datos almacenados, no son datos estáticos, están en constante movimiento, se interrelacionan unos con otros y dan como resultado nuevos datos. Su crecimiento es constante y ello implica no solo que deben estar protegidos mediante las **medidas de seguridad adecuadas**, sino también dotados de estupendos "motores que les permitan moverse ágilmente por las autopistas de la información".

El crecimiento exponencial del número de usuarios de los servicios *online* ha llevado a las empresas a subcontratar la gestión, mantenimiento y administración de sus equipos informáticos y de comunicaciones en los *Data Center*. Esto les permite centrarse en el desarrollo de su propio negocio y olvidarse de complejidades tecnológicas derivadas de las características anteriormente comentadas, así como prestar el servicio sin la necesidad de realizar una inversión elevada en equipamiento dedicado a este fin.

2. Necesidades y requisitos básicos

En base a la argumentación expuesta, a la hora de entender la utilidad de un *Data Center*, nos será de gran ayuda preguntarnos que es lo que demandan las empresas actualmente y ver que es lo que un *Data Center*, de calidad, puede ofrecer. Así pues, las empresas demandan:

- **Ancho de banda**. Es necesario contar con una gran capacidad de transferencia de datos, de tal forma que no sea apreciable ningún tipo de "retardo" provocado por la utilización de la red, máxime teniendo en cuenta que las líneas de comunicaciones de los posibles usuarios del servicio han mejorado considerablemente en los últimos años con la entrada en escena de servicios como el ADSL y el cable

- **Fiabilidad y alta disponibilidad**. Los sistemas deben responder a cualquier situación critica, haciendo posible la prestación del servicio sin pérdida apreciable de calidad incluso cuando es necesario atender gran cantidad de peticiones de forma puntual ("pico") o continuada. Resulta imprescindible contar con sistemas de alta disponibilidad y redundancia a través de modernas arquitecturas de red y servicios

- **Seguridad**. Cubriendo fundamentalmente tres aspectos:
  - Seguridad física: comprendiendo la seguridad de los sistemas hardware, soportes, dependencias y demás entidades «tangibles» del entorno del *Data Center*.
  - Seguridad lógica: incluyendo los aspectos de protección aportados por aplicaciones, protocolos y procesos que intervienen en el sistema, y complementado por elementos de seguridad de red (cortafuegos), detección de intrusos (IDS), y análisis a nivel de aplicación (antivirus).

- Seguridad político-corporativa: formada por los aspectos de seguridad relativos a política general de la organización, normas, procedimientos y convenciones internas aplicables. En este aspecto se debe tener en cuenta el cumplimiento de la legislación aplicable.

Dichas áreas están interrelacionadas, y la existencia coherente de medidas de seguridad en cada una ellas garantiza el nivel de protección óptimo frente a las posibles amenazas de seguridad.

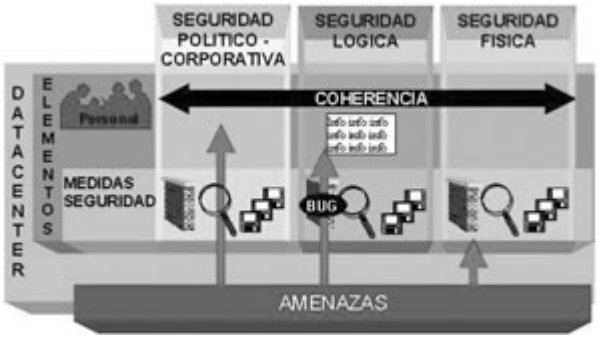


Ilustración. Aspectos de seguridad.

- **Escalabilidad, flexibilidad y rapidez** a la hora de implementar sus proyectos (*time–to-market*): Los equipos y los *web sites* del *Data Center* tienen que funcionar con la misma agilidad y rapidez que Internet para ser competitivos. La infraestructura existente tiene que permitir poner en marcha un proyecto en el mínimo tiempo posible, así como ampliar el número de elementos o la capacidad de los existentes de forma rápida y sin impacto en el servicio. Cada proyecto requerirá una solución específica cuyos requisitos variarán en el tiempo, si la infraestructura y el *Data Center* no permiten efectuar estos cambios con la celeridad necesaria nunca se logrará estar a la altura de la demanda del usuario o el servicio prestado por los posibles competidores
- **Arquitecturas sofisticadas** de comunicaciones: Para cubrir la demanda de los usuarios es necesario contar con los últimos desarrollos que la industria Internet lanza al mercado (*firewalls*, balanceadores de carga, sistemas de replicación de contenidos, etc.)
- La **gestión y administración por personal especializado:** Los sistemas implicados en la prestación del servicio requieren un alto nivel de especialización. Así mismo, la monitorización continuada 24x7 y detección precoz de errores se han convertido en requisitos imprescindibles para garantizar la calidad del servicio prestado, y lograr detectar los “cuellos de botella” antes de que representen un problema .

3. Ventajas de la externalización

Una vez comentadas las complejas necesidades y la gran cantidad de requisitos es obvio la externalización o *outsourcing,* tanto de las infraestructura del *Data Center* como de los servicios asociados a la gestión del servicio, suponen una **disminución de costes** notable, y permite que los usuarios dispongan de las tecnología mas avanzadas, beneficiándose de los ahorros derivados de la economía de escala y evitando la necesidad de realizar fuertes inversiones. tanto en el lanzamiento inicial, como en el mantenimiento a lo largo de la vida del proyecto. Esto supone una **optimización de recursos** al dejar en manos de personal especializado la responsabilidad del mantenimiento y optimización de los sistemas para centrarse en las funciones criticas para su negocio.

En el año 2000 la consultora estadounidense IDC realizó un estudio sobre los beneficios que los servicios de un *Data Center*, de calidad, podían ofrecer a las empresas en términos de retorno de la inversión y basándose en el análisis de los siguientes parámetros:

- Coste total del edificio, las operaciones y gestión de un *Data Center* comparando con los costes totales de un servicio de familia de alojamiento (*hosting*)
- Suma de ahorros estimados en un periodo de tres años
- Incremento de ingresos y reducción de costes generados tras incrementar el tiempo activo del entorno de *hosting* a lo largo de esos tres años

Las conclusiones fueron las siguientes:

- Existe una drástica disminución de los costes cuando las empresas utilizan el servicio de *outsourcing* (externalización de servicios) de un *Data Center* en lugar de emplear sus propios recursos tecnológicos
- El área donde se detectó una mayor deducción de costes dentro de la empresa fue la de personal, que puede llegara suponer hasta un 48,7 por ciento del total
- Gracias al *outsourcing*, las compañías estudiadas fueron capaces de incrementar su escalabilidad y reducir el tiempo de implementación de proyectos. En una mediana/gran empresa, realizar esas mismas tareas internamente precisaría de unos 60 técnicos cuyo periodo de contratación podría extenderse hasta los 6 meses
- Las compañías incluidas en el estudio experimentaron un incremento elevado de disponibilidad, a causa de la experiencia y escalabilidad, muy superior al que conseguían antes de utilizar los servicios del *Data Center*. Este incremento de la disponibilidad significa mayores ingresos

Por tanto, las empresas pueden reducir sus costes entre cuatro y seis veces externalizando el *hosting* de sus equipos informáticos en *Data Center* especializados. Además de este ahorro, la externalización incluye elementos de seguridad como la detección de intrusos y la

monitorización permanente 24 X 7, siendo ambas características de muy alto coste cuando tiene que realizarlos una empresa.

3. Modalidades de servicios que se proveen desde los centros seguros de datos; Alojamiento de websites (hosting/housing)

Además de la contratación de espacio físico y el acceso a red, en todo *Data Center* es conveniente disponer de varias opciones de servicios complementarios, que permitan abordar un **proyecto personalizado** con **posibilidad de crecimiento**. Los servicios que debería ofrecer un *Data Center* a la hora de subcontratar soluciones de presencia en Internet, y las características que se deben tener en cuenta son los siguientes:

- ***Hosting* compartido**. Las aplicaciones que crean los diferentes servicios son compartidos entre varios usuarios – típicamente un número de varios cientos o incluso miles de usuarios. Servicios que típicamente se prestan de esta forma son presencia web, servidores de aplicaciones, base de datos, correo electrónico, difusión de contenidos multimedia, etc

  Se pueden distinguir dos maneras de implantar técnicamente este servicio. La forma sencilla es compartir servidores únicos entre varios usuarios. Se instalan todas las aplicaciones en un único servidor y se comparte entre tantos usuarios como pueda soportar este hardware. Llegado al límite, se configura un nuevo servidor y así sucesivamente. Este tipo de hospedaje no ofrece prácticamente ningún nivel de redundancia, el fallo de un servidor se traduce en la indisponibilidad total del servicio para los usuarios que comparten este servidor.

  Una forma más avanzada del hospedaje compartido emplea granjas de servidores con balanceo de carga y uno o varios *clusters* de almacenamiento masivo. Las aplicaciones que prestan los servicios compartidos a los usuarios son instalados y configurados en varios servidores (mínimo dos por aplicación) y la carga de trabajo se distribuye entre estos servidores por medio de balanceadores hardware redundantes. En este entorno, no se asigna un hardware concreto a un usuario, sino todos los usuarios comparten varios servidores. El fallo de un único componente no perjudica la prestación del servicio. En este tipo de entornos de alta disponibilidad típicamente encontramos también los componentes de infraestructura redundados, como son los encaminadores (*routers*) y accesos a Internet, la electrónica de red (conmutadores), los cortafuegos (*firewalls*), etc

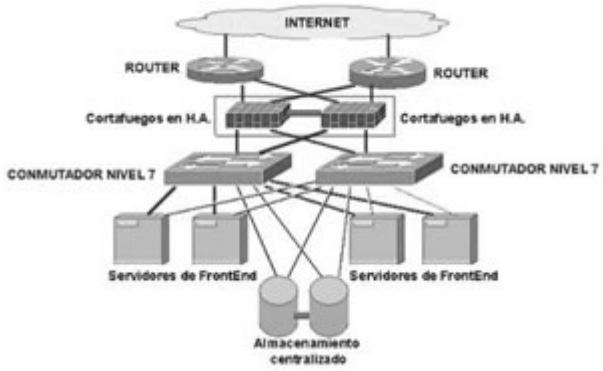


Ilustración. Esquema arquitectura balanceada.

Se trata de un servicio altamente especializado, con un soporte avanzado, monitorización continua de todos los componentes y que ofrece un control de alta nivel y también acceso a informes exhaustivos a través de un panel de control del servicio vía web. El cliente se aísla de toda la complejidad técnica subyacente al servicio que disfruta. Además, es relativamente económico, por conseguirse un compartir los recursos con un nivel muy alto

No obstante, el servicio puede ser poco flexible en el sentido, que los usuarios deberán ajustarse a los servicios que prestan las aplicaciones que el proveedor les ofrece, con lo que conviene estudiar si el proveedor proporciona opciones para los principales entornos de desarrollo (Unix y Windows) y las herramientas adicionales que se incluyen en el servicio (lenguajes soportados, estadísticas, etc.). Es importante informarse del nivel de aislamiento que se obtiene respecto a otros clientes, de tal forma que un problema en un sitio web concreto no afecte al resto. Para ello, el proveedor tendrá que tomar medidas en lo referente a aislamiento (por ejemplo, jaulas Unix, etc.) y control de recursos (CPU, memoria, disco, etc.)

- ***Hosting* dedicado**. El *hosting* dedicado recibe este nombre porque se dedica un servidor (o varios) al uso exclusivo de un cliente. Esto ofrece al cliente la principal ventaja de una libre elección del sistema operativo y las aplicaciones que quiere instalar en sus servidores, mientras que sigue confiando a su proveedor de hospedaje todos los temas relativos a la operación y el mantenimiento físico de los equipos, como son un espacio apropiado y acondicionado, sistema de clima y alimentación eléctrica redundantes, todos los trabajos de instalación, conexionado y puesta en marcha y el mantenimiento continuo del hardware.

  Típicamente, el cliente no necesita acceso físico para trabajar con su servidor, con lo que la ubicación geográfica es algo secundario. Sin embargo, hay casos cuando pueda ser aconsejable o incluso necesario trabar a pie de servidor y para ello es importante

que el *Data Center* disponga de salas de trabajo acondicionados y preparados para estas necesidades eventuales

En proveedores especializados, el servicio de hospedaje se suele extender también al soporte y mantenimiento del sistema operativo y de las aplicaciones instaladas, especialmente la actualización continua para evitar problemas de seguridad. Igualmente, deberá ofrecer un servicio de "manos remotas" para suplir la falta de la presencia física del personal del cliente y que debe poder complementarse con la posibilidad de delegar parte o la totalidad de las tareas de administración de sistemas y aplicaciones en manos del proveedor

Finalmente, hay una serie de servicios complementarios que nos deberá ofrecer el proveedor en su *Data Center* y que son imprescindibles en la mayoría de escenarios de uso. Se trata de servicios como la creación de redes locales entre los servidores del cliente, la conexión a Internet, conexiones privadas (VPN), protección con cortafuegos y detección de intrusiones, copias de seguridad a medida de las necesidades del cliente, monitorización personalizada de todos los componentes y aplicaciones, informes y estadísticas de uso, eventos, consumo, facturación, etc. Estos servicios deberán ser disponible de forma continua y respaldado por un centro de operaciones 24x7. Proveedores avanzados también ofrecerán el acceso a datos del servicio y estadísticas mediante un panel de control del servicio, vía web, semejante al que suele ofrecerse en hospedaje compartido.

- **Servidores privados**. Una solución intermedia entre el *hosting* compartido y los servidores dedicados son los llamados servidores privados, en los que se dispone de un servidor propio, con su sistema operativo y acceso total por parte del cliente, pero que se ejecuta en una máquina (*hardware*) junto con otros servidores privados de otros clientes. El aislamiento se consigue a nivel de sistema operativo, con lo que se obtienen las ventajas de la flexibilidad de los servidores dedicados y el bajo coste del alojamiento compartido.

- ***Housing (co-location)***. En este tipo de hospedaje, el proveedor, en primer lugar, se limita a ofrecer al usuario el alojamiento de los equipos en espacios especialmente acondicionados y preparados para ello, asegurando las condiciones de clima y la continua disponibilidad de la alimentación eléctrica y conexión de red. Este servicio se requiere, cuando el cliente dispone ya de los equipos que quiere alojar en el *Data Center* y también, cuando el cliente dispone ya de parte o todo el personal que se hará cargo de la operación y administración de sus sistemas. En este escenario, el cliente requiere acceso físico a sus equipos, así que todos los aspectos de seguridad física y

gestión y control de la presencia adquieren una especial importancia. Idealmente, el proveedor deberá garantizar el acceso físico a las instalaciones en cualquier momento del día o de la noche. Con ello, deberán existir mecanismos eficaces de control de acceso para garantizar la seguridad de las instalaciones, pero sin impedir el acceso libre en cualquier momento o con plazos de preaviso largos. Para que esto se cumpla, el proveedor deberá disponer de sistemas de control de acceso automáticos (por ejemplo tarjetas de proximidad) y complementado con sistemas biométricos para minimizar la posibilidad de fraude, además de sistemas de vigilancia por vídeo con grabación digital. En las salas compartidas, todos los espacios sensibles de uso común (instalaciones) y de cada cliente (armarios de 19" o jaulas) deberán contar con cerraduras y el proveedor deberá imponer un régimen estricto de gestión de llaves. Idealmente, el propio sistema automático de control de acceso al edificio y a las salas también deberá emplearse para el control de acceso a las jaulas y armarios de cada cliente

El servicio básico de *housing* o *co-location* se podrá complementar, en la medida de la necesidad del cliente y la capacidad del proveedor con los mismos servicios comunes que se han detallado ya en el punto anterior, sobre el hospedaje compartido. También para esta modalidad de hospedaje es importante que el proveedor ofrezca personal in situ las 24 horas, para suplir la falta de una presencia permanente del personal propio del cliente.

- **Servicios gestionados (*Managed services*)**. Nacen como evolución del *Housing*/*Co-location* y se sitúan en el nivel mas alto de la cadena de valor al requerir la interacción humana del personal experto del *Data Center* para su gestión. Los Servicios gestionados pueden incluir la arquitectura del servicio, configuración, implantación, migración, plan de capacidad, gestión de firewalls, gestión de los sistemas de almacenamiento informes y *tests* de los sistemas, análisis de vulnerabilidad del entorno y recuperación de daños. Mediante la utilización de estos Servicios, el cliente ya no tiene que preocuparse de disponer de un centro de datos correctamente acondicionado, ni contar con administradores de sistemas dentro de la propia empresa, ya que serán los expertos del *Data Center* los encargados de realizar estas operaciones.

  En este punto, conviene mencionar la ventaja de contratar estos servicios para la implantación de **Planes de contingencia y continuidad de negocio**, bien aprovechando la redundancia de ubicaciones de un proveedor, o contratando los servicios en un único *Data Center* como centro de respaldo al ya existente

La combinación de estos servicios proporcionan la **flexibilidad** necesaria para que el proyecto pueda crecer en función de las necesidades, e incluso contratar servicios adicionales en el menor tiempo posible ante necesidades concretas de más recursos, con lo que es fundamental determinar qué servicios nos proporciona el *Data Center*, y como están contempladas las consideraciones aplicables para cada uno de ellos.

4. Seguridad Física; Control de accesos, registros de E/S, áreas seguras

Este apartado comprende la seguridad de los sistemas de hardware, soportes, dependencias y demás entidades tangibles del entorno de prestación de servicios del *Data Center*.

Aparte de los sistemas ya comentados que garantizan la detección y gestión de alarmas y la disponibilidad del servicio, es conveniente revisar la existencia de los siguientes elementos en el edificio que alberga el *Data Center*:

Barreras y sensores de alarma

Elementos que garantizan la detección de intrusiones en el perímetro externo del edificio, o el movimiento no autorizado en las dependencias interiores.

Puesto de vigilancia y control

La existencia de un puesto de vigilancia y control en el *Data Center* es fundamental, tanto considerándolo como punto único de entrada de personal, como uno de los lugares donde se centralizan las labores de vigilancia de todo el edificio. En este puesto de vigilancia y control es deseable el cumplimiento de los siguientes requisitos:

- Personal dedicado en exclusiva a la gestión del control de acceso y vigilancia
- Punto único de entrada al edificio, y control remoto de las zonas y puertas de carga
- Registro de entradas y salidas, tanto de personal como de materiales
- Gestión de las alarmas del edificio
- Horario 24x7 los 365 días del año

Ilustración Puesto de vigilancia y control.

Control en puertas y accesos

Es importante observar las siguientes características en el control de puertas y accesos:

- Sistema de control de puertas electrónico, que permita la apertura y cierre desde el puesto de control de cualquiera de los puntos de acceso. Idealmente, las cerraduras eléctricas deben quedar abiertas en ausencia de tensión para facilitar la evacuación del edificio en caso de emergencia.
- Sistemas de identificación con tarjeta: entre los disponibles destacaremos las tarjetas de proximidad frente a las de banda magnética, por su mayor durabilidad y facilidad de uso. La misma tarjeta puede servir como credencial personalizada (con fotografía) para facilitar el control por parte del personal de seguridad

Ilustración. Lector de tarjetas de proximidad para control de acceso.

- En los puntos críticos del edificio (por ejemplo, las salas de alojamiento) es recomendable el empleo de lectores de características biométricas. Entre los dispositivos de lectura biométrica destacan los de geometría de palma de mano, ya que no tienen carácter intrusivo y proporcionan una tasa aceptable de falsos negativos/positivos. Estos dispositivos se pueden combinar con los lectores de tarjetas, de tal forma que sea necesaria tanto la presentación de la tarjeta como la lectura de la palma de la mano para conseguir el acceso a la sala restringida

Ilustración. Control de acceso tarjeta de presencia + lector biométrico.

- Control de presencia, permitiendo la realización de informes de estancias del personal autorizado en cada una de las salas
- Detección de apertura de puertas, de tal forma que desde el puesto de control se puede detectar y observar cualquier actividad sospechosa en el edificio
- Tornos de acceso para permitir la entrada/salida de forma individual y ordenada al recinto
- En el caso de tratarse de un CPD con acceso permitido a diferentes clientes, conviene estudiar las facilidades que se prestan para permitir el acceso a las salas de alojamiento, lo ideal es proporcionar acceso libre 24x7 al personal registrado, dotando a este grupo de personas de credenciales individuales e intransferibles

Circuito cerrado de televisión

Los parámetros a revisar en el sistema de Circuito cerrado de televisión son los siguientes:

- Existencia de cámaras fijas y direccionables (domos) en todos los puntos internos de paso, y en el perímetro exterior del edificio
- Sistema de grabación: es preferible emplear sistemas de Grabación digital permanente, frente a los sistemas analógicos tradicionales

- Actuación (grabación) programable por detección de actividad y ante eventos o alarmas externas (contactos, apertura de puertas, etc.)
- Tiempo de grabación: siendo deseable al menos 30 días

Ilustración. Circuito cerrado de Televisión, cámaras exteriores e interiores.

Interfonía

Es conveniente que el edificio cuente con sistemas de intercomunicación (interfonía) distribuidos en los puntos de acceso internos y externos del edificio, con comunicación directa con el puesto de seguridad y control, y los puestos de monitorización auxiliares.

Ilustración. Interfonía.

Megafonía

El sistema de megafonía en la totalidad del *Data Center* permite el envío de mensajes cuando se busca a cierta persona que se encuentra en el interior de una sala de alojamiento o en zonas comunes, y conviene que contemple:

- Envío de mensajes a zonas concretas del edificio
- Envío de mensajes a todas las zonas del edificio simultáneamente

Ilustración. Megafonía.

http://www.acens.es

• CAPÍTULO 5: SEGURIDAD EN REDES DE COMUNICACIONES

Una interrupción deliberada de las comunicaciones sólo puede significar una cosa: **la guerra**.
Star Wars, episodio I: La amenaza fantasma.

1. Introducción

Este capítulo se centrará en la seguridad en la comunicación a través de las principales redes, ya sea Internet, redes de área local o las últimamente de moda redes inalámbricas. Comprenderemos que la seguridad de las comunicaciones consiste en prevenir, detectar, evitar y solucionar violaciones a la seguridad durante la transmisión de información, como paso fundamental anterior a la seguridad de los sistemas finales, que abarca la seguridad de sistemas operativos, aplicaciones y bases de datos. Se considerará la información esencialmente en forma digital y la protección se asegurará principalmente mediante medios lógicos, más que físicos, y la correcta configuración de los activos que conforman la red.

El objetivo general es proporcionar una visión global de la problemática de seguridad que afecta a las organizaciones que manejan sistemas informáticos conectados a través de cualquier tipo de red, e implantar soluciones que permitan resguardar la confidencialidad y la integridad de la información, garantizar la autenticidad de los datos y de los mensajes y proteger a los sistemas de ataques internos o externos.

Los objetivos específicos de este capítulo son:

- Identificar las amenazas, vulnerabilidades y evaluar los riesgos asociados al manejo de la información en las redes de comunicación.
- Analizar las situaciones de una red que facilitan la penetración de intrusos, gusanos o cualquier actividad maligna así como las principales soluciones a las mismas.
- Evaluar las requisitos mínimos de seguridad que imponen a las organizaciones los nuevos entornos de trabajo, como acceso remoto, teletrabajo, redes inalámbricas, interconexión de empresas, etc.
- Implantar las medidas de seguridad para defenderse de las amenazas internas y externas a través de los controles apropiados.

INTRUSIONES Y ATAQUES EN REDES

A medida que la tecnología evoluciona e Internet y otros medios de acceso a información o recursos se hacen más populares y accesibles, el número de intrusiones y ataques desde la Red se va acrecentado, quizás debido a que se descubren fallos de seguridad a un ritmo mayor del que se solucionan. Mucha gente no es consciente de la importancia que tiene la

seguridad hasta que su sistema se ve comprometido conforme nuevas vulnerabilidades son publicadas y los hackers siguen desarrollando sus conocimientos.

1. Sobre los ataques: clasificación

El tipo de ataque que podemos sufrir depende de diversos factores, tales como el fin que persigue el atacante (es posible que busque obtener acceso al sistema, o simplemente quiera sabotear o inutilizar un servicio) o el grado de privilegios necesarios para poder lanzar dicho ataque.

Atendiendo a este último concepto (el ámbito del ataque o grado de privilegios necesarios para lanzarlo), podemos clasificar un ataque como:

Local: se lanza desde dentro del propio sistema víctima. Es requisito indispensable gozar de acceso (normalmente no privilegiado) en el servidor ya sea, porque se dispone de una cuenta en el sistema, o bien se ha logrado el acceso mediante otro ataque -remoto- previo. El objetivo comúnmente perseguido es la elevación de privilegios.

Remoto: no se requiere acceso previo a la máquina víctima. Es el más peligroso y es usual utilizarlo como paso previo a un ataque de ámbito local, aunque a menudo el segundo paso no es necesario.
Otra clasificación posible, según sea la finalidad perseguida por el atacante, podría ser la siguiente:

Ataque de denegación de servicio o DoS[4]: no se persigue conseguir ningún tipo de acceso al servidor víctima sino simplemente se desea la interrupción del servicio que presta o, al menos, la degradación del mismo. Los ataques de este tipo son muy variados. Por nombrar alguno, recordemos el mítico ataque conocido como “Syn-Flood”, consistente en inundar un servidor con peticiones de conexión de forma que se consuman los recursos del servicio y se deje de atender peticiones de conexión legítimas.

Ataque de consecución de acceso: este ataque busca obtener unos mínimos privilegios de acceso en el servidor víctima. Se trata pues de un ataque de tipo remoto que suele ser lanzado justo antes de otro del tipo que seguidamente veremos.

Ataque de elevación de privilegios: como su nombre indica, el atacante intentará aumentar el grado de privilegios que mantiene en el sistema. El objetivo usual de este tipo de ataques es llegar a obtener privilegios de “Administrador”, en sistemas Windows, o de “root”, en entornos Unix.

[4] “DoS” son las siglas de “Denial of Service”.

Por último, se puede distinguir también entre:

Ataques dirigidos: el atacante tiene claro quién es su víctima y se centra en una o varias máquinas de su entorno. Suelen provenir de la propia plantilla de la empresa o del entorno o actividades de la misma

Ataques indiscriminados: el objetivo suele ser comprometer cuantas más máquinas mejor,usualmente como origen de sucesivos ataques, con el objeto de dificultar la identificación del atacante o bien para amplificar la potencia de un posible ataque de denegación de servicio. El caso más conocido es quizás el de los *gusanos*, que no son más que programas que exploran la red, buscando aprovecharse de una o más vulnerabilidades y que, cuando lo consiguen, infectan el ordenador víctima de forma que éste a su vez comenzará a atacar e infectar otras máquinas, logrando un efecto multiplicativo. También se pueden englobar aquí herramientas automatizadas como los “mass-rooters”, cuyo objetivo principal es comprometer máquinas para un futuro uso por parte del atacante.

2. Fases de un ataque

Un ataque se llevará a cabo en cuatro fases bien diferenciadas: i. Fase de adquisición y reunión de información; ii. Acceso inicial al sistema. iii. Escalada de privilegios. iv. Ocultación del rastro y posible instalación de puertas traseras.

La primera fase de todo ataque será la reunión de información sobre la máquina víctima por parte del atacante. El atacante deberá encontrar respuesta a preguntas como: ¿qué sistema operativo usa la máquina víctima? ¿qué puertos tiene abiertos? ¿qué servicios tiene en ejecución? ¿qué software es usado en cada servicio? ¿qué versiones? ¿se pueden enumerar usuarios en la máquina remota?. Estas son sólo algunas de las preguntas que se hará el atacante. ¿Por qué estas preguntas? A menudo las vulnerabilidades que puedan existir en el sistema víctima son dependientes del software servidor utilizado, e incluso específico de ciertas versiones de dicho software. Por tanto, identificando estos datos, se podrán identificar también las posibles vulnerabilidades o puntos débiles del sistema víctima.

Durante la segunda fase, el atacante tratará de conseguir acceso a la máquina víctima. Si el atacante lograra este acceso se dice que el sistema (víctima) ha sido comprometido. El grado de compromiso es directamente proporcional a los privilegios que el atacante haya podido conseguir en el sistema atacado. No importa que el acceso conseguido sea o no privilegiado. Para el atancante valdrá como punto de entrada al sistema, a partir del cual podrá lanzar nuevos ataques, cuyo último fin será la consecución de máximos privilegios en el sistema.

Precisamente de esto último se encarga la tercera fase del ataque: buscar alguna

vulnerabilidad local que permita aumentar nuestros privilegios hasta lograr el grado máximo para cumplir el objetivo fijado. Por ejemplo la destrucción de un disco podría requerir privilegios de usuario “disk”, no haría falta el usuario “root”. Si se obtiene el máximo privilegio el sistema habrá sido totalmente comprometido.

Por último, cuando el atacante haya conseguido su objetivo tratará de afianzar el mismo así como evitar la detección de su intrusión. Para ello, intentará borrar las huellas que su ataque haya podido dejar en el sistema. Lo anterior supondrá un conocimiento exacto de la ubicación de los ficheros de “logs”[5] del sistema, y de su estructura. Además, y si el atacante tiene pensado volver a visitar la máquina víctima no será raro que se deje una puerta abierta que le facilite el proceso, de forma que no tenga que repetir todo el ataque cada vez que desee entrar de nuevo en la máquina, o le permita la entrada en caso de que la vulnerabilidad que éste usó haya sido parcheada. Es lo que se conoce como “puerta trasera”.

3. Amenazas principales para las redes

La amenaza principal para la seguridad de una red, entendiendo por seguridad el mantenimiento de la disponibilidad, integridad y confidencialidad de la información accesible a través de ella, pasa por dos ataques muy conocidos y habituales:

Denegación de servicio (DoS): cuyo fin último es la inutilización o degradación del recurso o servicio vulnerable, no llegando al compromiso total o parcial de la máquina que lo sustenta. Puede afectar a todos los servicios próximos o que compartan recursos con la víctima del ataque. Este ataque puede afectar tanto a grandes como pequeñas compañías y suele ser dificil de evitar o el coste de la prevención es elevado.

Sniffing: captura del tráfico de la red para tratar de obtener datos privados como credenciales, correos, etc. Se verá como evitar esto en la sección de medidas de red

4. Medidas básicas para prevenir problemas comunes de seguridad

Los siguientes consejos básicos ayudarán a mantener un mínimo de seguridad sobre sistemas finales, lo que redundará en la mejora de seguridad de la propia red:

- Tener el sistema siempre actualizado según las recomendaciones del fabricante o el administrador de seguridad.
- Utilizar una interfaz de red exclusivamente dedicada a administración, y distinta de la interfaz de red que dará servicio a los usuarios.

[5] Un “log” es un historial donde el sistema almacena los eventos más importantes que han ocurrido en el sistema.

- Cerrar todos los puertos que realmente no son necesarios. En el caso de un servidor web, probablemente sólo haga falta dejar abierto el puerto 80 (y quizás, también el 443) del interfaz que da servicio. En el interfaz de administración probablemente bastará con abrir el puerto 22 (SSH).
- Asegurarse de que el tráfico más crítico (en especial, el de administración) siempre va cifrado. En particular, ninguna contraseña de acceso al servidor debería ir en claro por la red.
- Utilizar herramientas como "Tripwire", para obtener las firmas digitales de los ficheros más peligrosos, en especial, de todos los ficheros binarios. Guardar el fichero de firmas obtenido en un lugar seguro (nunca en el propio servidor).
- Definir y cumplir una política de seguridad, en especial, en cuanto a las contraseñas y a acceso se refiere : no usar contraseñas débiles, cambiar la contraseña cada cierto tiempo, etc.

5. Medidas en el ámbito de red para prevenir/paliar problemas de seguridad

Hay soluciones fáciles de implementar que pueden ayudar a paliar gran parte de los problemas enumerados con un bajo coste, además de ofrecer otras ventajas adicionales a las propias de la seguridad. Estas medidas correctamente aplicadas ayudarán a solucionar otros problemas que, si bien afectan fundamentalmente a sistemas finales más que a la red, sí que pueden llegar a afectar a la propia red. En el caso de afectar a sistemas críticos o dispositivos de red, a continuación se enumeran algunas de estas amenazas:

Virus: es un programa diseñado para actuar sin autorización o conocimiento del usuario, normalmente con una carga o rutina dañina, que además, cumple dos requisitos, como la capacidad de ejecutarse a sí mismos y la capacidad de replicarse (infectar) otros ficheros, archivos o sistemas de ficheros. Los virus necesitan de ficheros o archivos para "sobrevivir".

Gusano: son programas que tienen la capacidad de pasar de un sistema a otro sin necesidad de infectar un fichero anfitrión. Suelen vivir en la memoria del ordenador. Hoy en día los *gusanos* suelen a su vez portar una componente vírica.

Spam: envío masivo de mensajes de correo idénticos o casi idénticos no solicitados, particularmente los que contienen propaganda y especialmente cuando las direcciones de correo han sido tomadas de Internet (o cualquier otro medio) sin el consentimiento de los destinatarios.

Exploit: programa o código fuente destinado a sacar provecho de alguna vulnerabilidad existente, por ejemplo, obtención de acceso remoto a la máquina víctima, elevación de privilegios, etc.

Escaneo de puertos: si bien no es un ataque, sí es una práctica habitual antes de realizar el mismo (también es conocido como barrido de puertos). Son diferentes técnicas de exploración tratando de revelar información interesante acerca de la arquitectura y servicios de la empresa víctima, en busca de vulnerabilidades asociadas a dichos sistemas o servicios.

Estos ataques, dirigidos contra sistemas finales en lugar de la red, suelen descontrolarse y acabar en un DoS contra la red, por ejemplo un gusano en un portátil puede llegar a contaminar toda la red de la organización y el tráfico que puede causar en su afán de propagación masiva es en sí mismo un ataque. Recordemos el gusano Slammer que dejó incomunicado a Korea debido a su virulenta búsqueda de nuevas víctimas que provocaba la saturación de la red. Ocurre algo similar con el SPAM, cientos de mensajes por segundo pueden desde bloquear el servidor de correo hasta consumir todo el ancho de banda disponible no sólo para la estafeta, también para el resto de servicios que pueden estar compartiendo recursos. A su vez, un simple exploit contra un dispositivo de red o un escaneo de puertos puede llegar a tirar un sistema y provocar el temido DoS del servicio o de la red completa.

Analizaremos las principales soluciones a nivel de red que pueden paliar o minimizar estos ataques, o al menos aislarlos a segmentos determinados de la red dónde serán más fácilmente controlables:

2. Redes Privadas Virtuales (VPN)

¿Qué es?

Una red privada virtual (o, de sus siglas en inglés, una VPN) es un sistema por el cual se proporciona seguridad en las comunicaciones entre dos extremos a través de un medio inseguro. Tras una conversación inicial en la que se asegura que los dos extremos de la VPN son quienes dicen ser, se establece un *túnel* (un túnel no es más que el camino imaginario, virtual, que existe entre las redes o sistemas conectados, de forma que existe una conectividad permanente). A través de este *túnel* seguro, se pueden usar todo tipo de servicios entre los dos extremos como si estuvieran conectados en el mismo lugar.

La potencia de las VPNs reside en el hecho de que toda la comunicación inicial y el *túnel* se hacen a través de un medio inseguro, como por ejemplo Internet. A pesar de esto, si están bien configuradas, se puede confiar en que todo lo que se envíe por el *túnel* no puede ser escuchado ni falseado en su camino.

Es importante resaltar que en una VPN existen dos extremos del *túnel*. Estos extremos

pueden ser desde equipos personales a dispositivos de interconexión, como son los cortafuegos o router. La información viaja de modo seguro entre ambos extremos, por lo que antes de implantar una VPN, hay que estudiar el punto óptimo en el que establecer los extremos del *túnel*.

¿Para qué sirve?

Una VPN se utiliza en los casos en los que se quiere conectar dos puntos a través de redes desconocidas, como puede ser Internet o las redes de terceras compañías. En estos casos, realizar las conexiones directamente y sin métodos seguros tiene el riesgo de que se puedan escuchar las mismas, o incluso suplantar la identidad de quien las realiza.

Usos típicos de las VPNs serían los casos en los que existen usuarios que se conectan de forma remota a la red de la empresa, o la conexión de varias sucursales a través de Internet. Una vez establecida la VPN, el comportamiento sería similar que los dos extremos estuvieran conectados físicamente a la misma red. De esta forma, se podrían compartir ficheros, impresoras y demás recursos entre los distintos puntos con total seguridad siempre que la información viaje cifrada con protocolos de probado rendimiento como IPSec.

¿Quién la necesita?

En general, cualquier empresa o entidad en la que se requiera el acceso a servicios internos de la empresa desde Internet para empleados o sucursales.

En los casos en los que existan empleados que necesiten acceder desde lugares externos a la red interna de la empresa (para compartir ficheros, impresoras, uso del correo interno,…), una VPN sería el método correcto de acceso. En este caso, un extremo del túnel estaría ubicado en el ordenador que utilizara el empleado remoto, mientras que el otro se ubicaría en algún dispositivo de interconexión: cortafuegos, routers u otros dispositivos específicos para realizar VPNs.

Cuando la conectividad se necesita entre sucursales, los extremos del *túnel* se suelen ubicar entre elementos de interconexión en cada una de las redes, como pueden ser los cortafuegos de acceso a Internet. De este modo, todos los accesos para los usuarios internos de las redes serán totalmente transparentes y sin necesidad de realizar ningún tipo de configuración adicional.

3. Segmentación de Redes

¿Qué es?

La segmentación de redes es el concepto por el cual se separan en distintos segmentos de red grupos de equipos según una serie de criterios, principalmente de seguridad y eficiencia. Habitualmente, estos criterios dependen directamente del grado de exposición de los servicios que proporcionan los equipos y de la importancia de los datos que contienen los sistemas que forman la red.

Un ejemplo típico sería el de una empresa con un servidor web que accede a una base

de datos. Los equipos que reciben las peticiones desde el exterior, en este caso únicamente el servidor web, estarían en una red. Dado que el servidor web accede a la base de datos, se puede considerar que la base de datos es accedida indirectamente desde Internet, por lo que se ubicaría en otra red. Por último, habría otra red con los equipos internos, los cuales no pueden ser accedidos ni directa ni indirectamente desde Internet.

La segmentación de redes se puede realizar en todos los niveles, y no únicamente para equipos accesibles desde Internet o no, sino también teniendo en cuenta el grado de seguridad y accesibilidad que se marque internamente en la empresa.

¿Para qué sirve?

La segmentación de redes es una medida más de seguridad por la que se agrupan diferentes perfiles de equipos en redes independientes. Una vez agrupados, se definen qué accesos se necesitan entre cada una de estas redes y se limitan los mismos por medio de equipos específicos (cortafuegos, IDPs y otras tecnologías descritas en este mismo libro en el capítulo de cortafuegos). Si se definen correctamente estos accesos, se añade un nivel más de seguridad a las redes de la empresa.

A su vez el uso de redes conmutadas (el uso de conmutadores en lugar de concentradores) dificulta mucho uno de los principales problemas de seguridad de las redes, la captura o escucha ilegal de tráfico, pues cada sistema recibe únicamente los datos que debe recibir en lugar de recibir los de toda la red. Si esto se une con el uso de procolos cifrados (se explica en otro apartado) se incrementará de forma sustancial la seguridad.

Segmentaciones típicas de red realizan las siguientes agrupaciones:

- **DMZ:** Red en la que se ubican equipos que proporcionan servicios directamente a Internet, como pueden ser servidores web, servidores ftp,…
- **Semi-DMZ:** Red de equipos que se acceden indirectamente desde Internet. Suelen ser bases de datos que son accedidas por equipos de la DMZ.
- **Gestión:** Red utilizada por los administradores de los diferentes dispositivos para acceder a los mismos para realizar la configuración de los mismos.
- **Personal externo:** Usualmente, el personal subcontratado o que se conecta de forma temporal a la red de la empresa, idealmente lo debe de hacer a través de una red dedicada a tal fin. De este modo, se asegura que no accede a recursos privados de la empresa, como pueden ser bases de datos de facturación, personal, correo, o similar.
- **Servicios Internos:** En esta red se ubican los servidores dedicados a los empleados internos o con información restringida. Suele tratarse de servidores de correo o bases de datos de información interna.
- **Interna:** Red de empleados internos de la empresa. En esta red se conectarían los equipos de escritorio de los empleados. En general no se subdivide, pero se podría segmentar aplicando otros criterios, como son perfiles de usuarios.

¿Quién la necesita?

La segmentación de redes se suele aplicar cuando existan equipos con diferente grado de exposición o dependiendo de la confidencialidad de la información que contengan.Una correcta configuración limita de forma considerable el impacto de una intrusión en los servidores o los efectos de un gusano.

Para optimizar el uso de recursos, se puede utilizar un mismo conmutador (switch) para diferentes redes. Para ello se definen las llamadas VLAN, en las que se establece qué puertos del conmutador pertenecen a cada VLAN. El resultado desde el punto de vista funcional es similar a tener varios conmutadores, pero con un ahorro de costes que puede llegar a ser bastante importante.

El peligro en el que se incurre en este tipo de configuraciones es que si un atacante consiguiera acceder a la configuración del conmutador, tendría acceso a todas las VLAN que tenga configurado el mismo. Sin embargo, evitando configuraciones por defecto de los conmutadores, es muy improbable que se consiga tener éxito en este tipo de ataques.

4. Protocolos cifrados y comunicaciones empresa-empresa.

La comunicación a través de Internet entre sucursales o compañías distintas supone un riesgo, dado que se desconoce las redes por las que atraviesa el canal de comunicación. Acceder a equipos sin las debidas medidas de seguridad, es similar a decir en voz alta la clave de acceso a nuestros sistemas en una sala llena de gente. Puede que haya gente que sepa utilizar esa información y puede que no, pero lo ideal sería evitar correr este tipo de riesgos.

No es un problema sin solución. Existen diversos protocolos de comunicación que cifran todo lo que se transfiere a través de ellos. La identificación ante el sistema se puede realizar de forma totalmente segura. De hecho, en general están diseñados de forma que, aunque se pudiera escuchar toda la comunicación desde el principio, no sea posible obtener información ni de las claves ni de la información transferida.

Para los protocolos inseguros más comúnmente utilizados existen protocolos cifrados con las mismas capacidades. Algunas de estas asociaciones se muestran en la siguiente tabla.

Inseguro	Seguro
telnet	ssh
ftp	sftp
http	https

Es imprescindible, o al menos muy recomendable, sustituir los protocolos inseguros por los correspondientes seguros sobre todo para acceso a CLI (interfaz de línea de comandos) o web de administración o gestión del negocio a través de medios compartidos. Este tipo de accesos puede poner en peligro la información de los clientes o de la propia empresa, pudiendo suponer, además de una pérdida de imagen, las correspondientes sanciones por parte de la administración, que pueden ser muy elevadas.

Otro tipo de comunicaciones, como puede ser el envío de documentos relevantes a través del correo electrónico, debería hacerse utilizando mecanismos de cifrado eficaces, cifrar el correo es un método excelente de asegurar la privacidad de las comunicaciones de la empresa. Para un cifrado de calidad, resistente a ataques, debería usarse algoritmos de clave asimétricos, basados en clave pública-privada. Existen programas como el conocido “PGP” para este tipo de tareas y en todas las plataformas, integrándose además con los clientes de correo y facilitando mucho el uso. Debe evitarse utilizar el cifrado de herramientas como office o excel, totalmente ficticio y con múltiples herramientas disponibles en internet para romper la protección o cifrado que estos programas introducen en los documentos.

A pesar de usar protocolos cifrados, siempre hay que tener cautela en el modo de configurar los mismos, dado que una mala configuración puede llevar a que un protocolo seguro vea reducida su efectividad.

En las comunicaciones entre sucursales o entre distintas empresas que necesitan acceder a redes internas del cliente o el proveedor, será necesario seguir unas reglas mínimas que garanticen la seguridad de las redes compartidas. La idea consiste en asignar a cada red un valor o nivel de seguridad y definir una reglas de interconexión entre redes en base a esta métrica, este valor se basará en parámetros perfectamente medibles como podrían ser:

- **Valor o importancia de los datos de la red:** se asigna un valor a la red en función de los datos que albergan los sistemas que la componen, de forma que una red debería tener un nivel de importancia igual al sistema de más valor de la red, aunque lo ideal es que en redes de un valor determinado todos los sistemas tengan un nivel similar para evitar el acceso a la red de personal con menor privilegio. Esto quiere decir que en la red de bases de datos de los clientes que tendrá un nivel de seguridad alto no debería estar el servidor web público de la compañía, cuyos datos son públicos y su importancia sera media o baja.

- **Exposición:** que definiremos como la visibilidad desde la propia red de forma que cuantas más redes sean alcanzables desde una red concreta mayor nivel de exposición y por tanto deberá tener un mayor nivel de seguridad.

En función del valor de los datos de los sistemas que forman la red y de la exposición de la misma se asignará a cada red un **nivel de seguridad** y se definirá una **política de interconexión de redes** en base al nivel otorgado, de forma que redes con nivel de seguridad bajo no podrán acceder a redes con nivel de seguridad alto, o si se permite el acceso se hará con ciertas restricciones. Aquí entra en juego la importancia de la segmentación de redes explicada anteriormente en base a criterios de seguridad.

Otros factores a tener en cuenta serán el control de accesos y la gestión de usuarios, al montar las VPN explicadas anteriormente tendremos un control de accesos basados en el cliente VPN, lo que nos garantiza cierta seguridad en la autenticación del mismo y una comunicación segura (cifrada), los usuarios deberían tener distintos perfiles de privilegios en función de la red origen (por ejemplo una red externa a la organización) y la red destino (por ejemplo la red corporativa o la red de servidores), estos privilegios deberían permitir al usuario realizar las tareas que tiene encomendadas, no más. La gestión de los usuarios debería incluir tiempos de expiración para que sea necesario renovar y evitar así usuarios que hace mucho abandonaron la empresa pero que siguen teniendo acceso a la red.

5. Protección equipos de red, bastionado de sistemas y evitando configuraciones por defecto.

Un fallo común al realizar una implantación de equipos en una compañía consiste en mantener las configuraciones por defecto de los sistemas. Así, no es difícil encontrarse con dispositivos (router, conmutadores, cortafuegos, puntos de acceso de redes inalámbricas,…) o aplicaciones (incluidos sistemas operativos) que se han instalado y ofrecen servicio, pero que mantienen la configuración por defecto de instalación del mismo. Este hecho suele llevar asociado la presencia de gran cantidad de problemas de seguridad, dado que en algunos casos se mantienen servicios de administración con usuarios y claves conocidas por ser las utilizadas por defecto en los sistemas.

Un ejemplo típico de este hecho son los router y los puntos de acceso inalámbricos. En ambos casos, la instalación es sencilla y no se suelen repasar todos los parámetros de configuración para asegurar que la configuración sea segura.

La solución debe pasar por proteger todos los equipos de red, para ello en necesario bastionar los mismos acorde a procedimientos operativos de seguridad (POS) que deben estar perfectamente claros para clara plataforma. Esto minimizará el riesgo de sufrir una incidente.

Cada dispositivo deberá hacer las funciones para las que se han diseñado, por ejemplo los router deben encargarse de redirigir el tráfico, dejando la tarea de filtrado a los cortafuegos. A

veces por motivos económicos se prefiere comprar un dispositivo que cumple múltiples funciones, aunque por lo general este tipo de soluciones presentan múltiples problemas y escasa eficiencia aportando mucho más valor las soluciones dedicadas.

Las soluciones que hemos descrito dificultarán en gran medida la expansión de los problemas de seguridad a toda la organización, no los evitan en su mayor parte, pero sí que sirve para aislarlos y reducir el problema a un área concreta, es un concepto similar a los compartimentos estancos de los submarinos o petroleros, en los que en caso de incendio o escora se aisla e inunda una zona acotada buscando evitar daños mayores.

6. Seguridad en redes inalámbricas (wi-fi)

Por último, se dedicará una mención especial a este tipo de redes, tan de moda hoy en día y que, como se verá, presenta graves problemas de seguridad.

Conceptos básicos

¿Qué es una red de área local inalámbrica (WLAN)?

Una red de área local inalámbrica (WLAN) podría definirse como una extensión de las redes cableadas tradicionales, pudiendo llegar a ser un reemplazo de las mismas si la tecnología llega a alcanzar cierta madurez que aún no posee, sobre todo por la falta de acuerdo e incompatibilidades entre distintos fabricantes. La diferencia fundamental entre redes clásicas y redes inalámbricas es, que estas últimas, utilizan las ondas de radio para transmitir los datos mediante el uso de un proceso denominado modulación (la sobreposición de los datos sobre la onda portadora), a través de un medio intangible como sería el aire.

¿Qué ventajas aporta?

Sin embargo, la tecnología de las redes inalámbricas va mucho más lejos de la sola ausencia de cables, ofreciendo funcionalidades como la movilidad y facilidad de despliegue, evitando la rigidez e inmovilidad de las redes cableadas, con infraestructuras fijas que ofrecen mucha resistencia al cambio que quizás la empresa necesite, al contrario que las redes inalámbricas que poseen una facilidad de adaptación a nuevas arquitecturas flexible, económica y, sobre todo, rápida.

¿Qué desventajas?

Las principales desventajas afectan a la seguridad y rendimiento de la red. El despliegue de redes inalámbricas, como cualquier otra tecnología o infraestructura, se debe

llevar a cabo teniendo en cuenta en dicho diseño todos los aspectos concernientes a seguridad. Sin embargo, esto se está omitiendo en múltiples redes de organizaciones o, si se lleva a cabo, los ingenieros o arquitectos de redes que tratan de implementar una red segura, lo hacen en base al conocimiento que tienen de los conceptos de seguridad de redes clásicas. En el mundo inalámbrico nos enfrentamos a nuevos puntos de vista de seguridad que no se tenían antes en cuenta o no eran tan acuciantes o, en el peor de los casos, pueden llevar a cometer errores fatales, que acaben comprometiendo toda la red de la empresa u organización. El rendimiento es muy inferior a las redes cableadas tradicionales, aunque poco a poco comienzan a alcanzar ratios de rendimiento que las hacen factibles para redes de área local. Se ampliarán detalles sobre los principales problemas de esta tecnología.

Unas definiciones básicas:

Existe un estándar de comunicaciones inalámbricas conocido como **802.11**, que tiene muchas aproximaciones. A día de hoy, es el protocolo **802.11b** el que parece tener mayor aceptación, al moverse en la banda de los **2.4**Ghz (gratuita) y ser los dispositivos relativamente económicos. Las velocidades de transmisión que se consiguen son de 11 Mbps, y con desdoblamiento de velocidad hasta 22 Mbps (aún no está avalado por el IEEE).

Para introducirse en los aspectos de seguridad de dicho protocolo es necesario conocer:

- **Extended Service Set Identifier (ESSID):**
- Identifica cada una de las WLAN.
- Se emite en los *beacon frames*.
- Se emite en texto claro (sin cifrar).
- La longitud oscila entre 1 y 32 caracteres.
- Debe ser conocido por los usuarios.
- **Beacon Frames:**
- Se envían para anunciar la presencia de las redes a los terminales móviles.
- Contienen muchos datos, entre otros el ESSID.
- Se envía de forma periódica (normalmente varias veces por segundo).
- **Cifrado WEP (Wired Equivalent Privacy):**
- El estándar IEEE 802.11 define WEP como el método para protegerse contra las 'escuchas casuales'.
- Emplea un algoritmo de cifrado simétrico conocido como RC4.
- La longitud de la clave puede variar, siendo lo más normal entre 40 y 104 bits.
- Extrae las claves de la palabra de paso conocida.
- Cada paquete contiene un 'Vector de Inicialización' (IV), sin cifrar, y el bloque de datos cifrado, que contiene un CRC32 para el control de la integridad.

Puntos débiles

A continuación se pasan a analizar los principales problemas de seguridad de la tecnología WI-FI:

a. Facilidad de acceso, redes muy abiertas.

Las WLAN son fáciles de localizar, constantemente anuncian su existencia a potenciales clientes que pueden conectarse a ellas y usar los servicios que la red provee. El estándar 802.11 requiere que las redes periódicamente anuncie su existencia mediante los ***Beacon Frames***. La información necesaria para conectarse a la red es la misma que la que se necesita para lanzar un ataque contra la misma.

Hay gente, conocida como *war drivers* que usan antenas y un software especial para capturar *los Beacon Frames* y asociarlos con una determinada posición geográfica (suelen llevar un GPS de bolsillo).

De esta forma, paseando por una ciudad, se podría llegar a construir un mapa muy exacto de redes alcanzables, y estas redes acaban convirtiéndose en puntos de entrada con mayor o menor dificultad al resto de la red. Existen múltiples *sniffers* de libre acceso en Internet que emiten un sonido cuando detectan una red, convirtiendo la tarea de localización en un paseo con un portátil y unos cascos.

Algunos administradores consiguen mitigar estos problemas mediante control fuerte de accesos y soluciones de cifrado. El despliegue de los puntos de acceso (en adelante AP) debería hacerse en el lado exterior de los cortafuegos, (para evitar el by-pass), y usar VPN para proteger los datos sensibles es una solución muy sensata.

b. Despliegue incontrolado de puntos de acceso.

La característica 'Plug-n-Play' de estas redes las hace incontrolables a los administradores, siendo normal el despliegue de puntos de acceso por usuarios finales que poco o nada saben de los riesgos de seguridad que conlleva. En la mayoría de los casos, las configuraciones de los puntos de acceso se mantienen por defecto, o con cambios mínimos, lo que provoca que no se activen sus características de seguridad.

La solución contra este tipo de actuaciones no es sencilla, aunque los administradores pueden buscar con herramientas de monitorización AP (Access Points de WLAN) incontrolados, una herramienta que permite hacer esto bajo Windows es NetStumbler. Pero es una tarea que requiere mucho tiempo y que debe repetirse a menudo para evitar sorpresas, con el gasto que ello supone. Otra solución sería instalar sondas de monitorización de redes

inalámbricas al igual que suele hacerse con redes cableadas, esto resulta relativamente fácil y barato pues el despligue de las sondas no necesita ni requiere interferir con el tráfico normal de la red corporativa.

c. Uso sin autorización del servicio.

Peter Shipley, publicó un estudio en el 2001 en el que localizó en torno a 9000 AP en el centro de San Francisco, el 60% de los AP mantenían su configuración por defecto original, en su mayor parte estaban conectadas directamente al *backbone* interno de la red (no a una DMZ o en el exterior del cortafuegos). La mayor parte de estas redes, (el 85% o más), no utilizaban WEP y del 15% restante, la mitad usaba una clave de cifrado por defecto elegida por el fabricante.

El "Top" de claves por defecto:

13% tsunami
11% AirWave
10% WaveLAN Network
8% WLAN
5% linksys
2% default
2% TEKLOGIX

A esto se une el problema de redes de libre acceso, cada vez más abundantes, en universidades, cafés, bibliotecas, grupos organizados (MadridWiless, ZamoraWireless), etc. ¿Cómo distinguir una red libre de una privada?

A su vez, el solapamiento de varias redes de diversas empresas, por ejemplo, empresas que comparten edificios, puede permitir que accidentalmente un trabajador cambie de red, entrando sin permiso en una red para la que no tienen autorización, sin ser consciente de ello.

La solución contra el uso no autorizado pasa por desplegar VPN para proteger la red de los clientes wireless, además, es probable que la propia VPN ya soporte autenticación fuerte.

El uso de protocolos de autenticación como 802.1x para proteger la red del uso no autorizado, asegurándonos que los usuarios se conectan al AP para el que tiene autorización.

d. Servicio y rendimiento limitado = vulnerables a DoS

Las WLANs tienen capacidades de transmisión muy limitadas, las redes basadas en 802.11b tienen una capacidad de transferencia aproximada de 11 Mbps, (22 Mbps con desdoblamiento de velocidad) y hasta 54 Mbps con tecnología 802.11a o 802.11g (aunque es más cara, como es lógico). Esto las convierte en especialmente sensible a ataques DoS (ataques de denegación de servicio). Sin embargo, no es necesario que los ataques sean hechos de forma malintencionada, es fácil que grupos de usuarios desde la LAN interna, (un segmento de red mucho más rápido que la WLAN), sobrecarguen a la WLAN si generan mucho tráfico, al ser dos medios desiguales con mucho a favor de la ethernet. Igualmente, un atacante que tenga acceso a la red interna puede inutilizar la red WLAN simplemente lanzando un ataque por inundación de *ping* sobre los limitados recursos de estas redes. Dependiendo del escenario del ataque es posible sobrecargar varios AP utilizando direcciones *broadcast* como destinatarias de la inundación *ping*.

Las redes WI-FI son, por tanto, vulnerables a todos los ataques que afectan a redes cableadas más todos los específicos de su tecnología:

- Radio: jamming.
- Autenticación: desasociaciones.

i. Radio: jamming

El mayor problema de estas redes es el ruido, que provoca una pérdida de calidad en la comunicación, (debemos de tener en cuenta que las WLAN no están pensadas para hacer corrección de errores, sólo detección, pues para corrección se necesitan muchos más bits y que un atacante puede inyectar tráfico sin estar asociado al AP pues el protocolo 802.11 está diseñado para permitir a múltiples redes compartir el mismo espacio y canal de radio).

ii. Autenticación: desasociaciones

Consiste en que enviar tramas de desasociación a los clientes tras haber suplantado la MAC del AP de forma que provoca un DoS debido a la continua conexión y desconexión a la red, lo que imposibilita el uso normal de los recursos de la misma.

La solución al primero de estos problemas es implementar corrección de errores en lugar de sólo detección en el protocolo, hacia esto es dónde encamina el protocolo 802.11i. Aunque mientras tengan este rendimiento las redes inalámbricas siempre serán más vulnerables a ataques de inundación de tráfico o este último que las redes cableadas, sobre todo porque no se puede controlar el medio usado para la transmisión y por las limitadas prestaciones del mismo, aunque con el tiempo van mejorando en prestaciones y pronto estarán

a un nivel similar a redes cableadas.

e. Falsificación de MAC y captura de sesión.

Las redes 802.11 no autentican frames, (en realidad pasa igual con las redes tradicionales ethernet), un atacante puede falsificar (hacer *spoofing*) frames para redirigir tráfico y corromper tablas ARP. A un nivel mucho más simple el atacante podría capturar las MAC (escuchando la red, con un sniffer como ethereal, que soporta dicho protocolo), y suplantar a un usuario legítimo al tiempo que realiza un DoS contra el mismo, (recordemos que DoS siempre será posible pues nada puede evitar que un atacante acceda a la capa de radio). Más aún, un atacante podría sustituir al AP, explotando la falta de autenticación de los propios AP y emitiendo un ESSID adecuado (los AP se identificaban por su broadcast de los Beacon Frames) parecería estar en la red de forma legal, aprovechando que no hay nada en el 802.11 que requiera a un AP probar que realmente es un AP un atacante podría robar las credenciales del AP original para acceder de manera ilegal a la red y realizar un ataque 'man-in-the-middle', este ataque, básicamente consiste en hacerle creer al AP original que el atacante es el cliente y al cliente que el atacante es el AP, de esta manera todo el tráfico (tanto ida como vuelta) acaba pasando por el atacante, una herramienta para hacer este ataque es 'monkey-jack'. Igualmente podemos superar las listas de control de acceso (ACL) basadas en MAC, que incorporan algunos dispositivos, tan sólo hay que escuchar hasta obtener una MAC lícita y falsificar nuestra MAC para superar la restricción.

La falsificación de MAC puede evitarse usando tablas ARP estáticas, o creando dos VLAN en el conmutador, una para la boca en la que está conectado el AP y otra para el resto de máquinas.

f. Análisis de tráfico y escucha pasiva.

Las cabeceras de los paquetes están siempre en claro, visibles a cualquiera que tenga un analizador de redes wireless, pero el problema principal radica en la escucha, el espionaje de datos que se puede hacer, pues aunque 802.11 provee un método de cifrado (WEB), este un algoritmo con muchos puntos débiles y fácil de romper. WEP sólo protege la asociación inicial con la red y los frames de datos, dejando los paquetes de control y gestión sin cifrar o autenticar por WEP, dando gran libertad a un atacante para que altere la transmisión con paquetes falsificados.

Existen herramientas para romper el cifrado, como AirSnort o WEPCrack, debido a la naturaleza del algoritmo, la corta longitud del IV (se repite a menudo debido a su pequeño tamaño y esto permite ataques estadísticos), a que es posible generar todos los valores de IV en unas 5 horas, (tan sólo hay 16 millones de posibilidades) y muchos detalles que no entraremos aquí, (hay múltiples documentos con demostraciones sobre ataques con éxito

contra WEP), no debe considerarse segura una red cifrada con WEB. Aumentar el número de bit de la clave WEP para cifrar tan sólo duplica el tiempo necesario para encontrar la clave, en lugar de crecer exponencialmente, es un problema de diseño.

Algunos fabricantes empiezan a reaccionar y las últimas versiones de firmware de sus productos corrigen gran parte de las vulnerabilidades, usan métodos interesante como por ejemplo cambiar la clave WEP cada poco tiempo. Sin embargo la mejor solución en estos casos es usar protocolos diseñados para transmitir datos sobre canales inseguros como SSH, SSL, IPSec, que han probado su resistencia a ataques durante muchos años, WEP tiene muy poco tiempo y es probable que aparezca una nueva generación de software capaz de volver a romperlo en pocas horas.

g. Propagación del problema de seguridad hacia otras redes

Una vez que el atacante gana acceso a una WLAN, puede ser usada como cabeza de puente pare realizar ataques a otras redes, tanto de la propia organización como externas. Normalmente las WLAN no están tan monitorizadas ni securizadas como por ejemplo podría estar una DMZ. La solución pasa por desplegar estas redes fuera del perímetro de seguridad, pero con acceso especial hacia redes internas, por supuesto añadir mecanismos de seguridad extra como VPN, etc. En la mayoría de los casos es más fácil entrar en la red interna a través de la WLAN que desde Internet.

Conclusiones

Debe quedar claro que para montar una WLAN los conocimientos y medidas de seguridad deben ser superiores a los necesarios para montar una red cableada.

El talón de Aquiles del protocolo 802.11b (el que por ahora parece ganar la partida) es:

- La autenticación y control de acceso a la red (no hay mecanismos eficaces que impidan el acceso a la red de usuarios no autenticados o la suplantación de los mismos).
- El cifrado de datos (no es lo suficientemente robusta).

Tomar un mínimo de medidas de seguridad básicas:

- Habilitar el cifrado WEP.
- Cambiar las contraseñas o claves cada cierto tiempo.
- Deshabilitar la publicación del ESSID.
- Restringir el acceso vía ACL por dirección MAC, manteniendo un inventario de MAC autorizadas.

Además es necesario usar por encima del protocolo para redes inalámbricas otros protocolos seguros, de eficacia probada durante años, como son SSL, ssh, VPN, etc.

http://www.movistar.com

• CAPÍTULO 6: SEGURIDAD EN ENTORNOS WEB

"Los riesgos de las inversiones tecnológicas son hoy contingencias de nivel empresarial y, por tanto, no puedes hablar de ningún elemento de riesgo de negocio sin haber contemplado antes estos mismos peligros para las Tecnologías de la Información"

Richard Hunter, Gartner Group.
Otoño 2004

1. Introducción: el acceso a la información

Es evidente que el acceso inmediato y en tiempo real a la información se ha convertido en una necesidad vital para las empresas de la sociedad actual, que debido a la liberalización de los mercados (telecomunicaciones, energía, transportes) y a la eliminación de cuotas de importación (textil) sufren presiones del mercado y de la competencia que deben contrarrestar implementando el modelo denominado de "Empresa en Tiempo Real" para mejorar su competitividad.

Tanto para la generación directa de nuevos ingresos en este mercado global como en la automatización de sus procesos de negocio, es necesaria la inversión en (y explotación de) las Tecnologías de la Información para generar mayor valor añadido que la competencia y antes que la competencia, en el momento adecuado del mercado ("*time to market*"). En este entorno es imprescindible una interoperabilidad entre los procesos emisores y receptores de la información, que actualmente se basa en la compatibilidad y estandarización de protocolos de intercambio de datos, principalmente en sus dos vertientes:

- Acceso a la información desde los navegadores de web mediante el estándar de interacción hombre-máquina HTML (HyperText Mark-up Language, lenguaje interpretado por dichos navegadores), tanto desde ordenadores personales como desde dispositivos tecnológicos portátiles de tipo teléfonos móviles, asistentes personales (PDAs), etc. conformando lo que se denomina "computación ubicua" y modelo de acceso universal a la información.

- Intercomunicación automática entre Sistemas de Información que dan soporte a los Procesos de Negocio (integración entre aplicaciones), actualmente y con cada vez mayor frecuencia implementados mediante Aplicaciones Web que permiten interconectar estos procesos de negocio de forma automática, mediante el estándar de interacción máquina-máquina XML, un lenguaje modular universal de compartición de datos, base de la interoperabilidad y de la ejecución distribuida de aplicaciones.

2. Nuevas formas de hacer negocio: aplicaciones web

Esta posibilidad de interconectar personas, procesos y tecnología crea una sinergia que multiplica las formas tradicionales de hacer negocio y el propio modelo de negocio en sí mismo.

Por un lado se generan nuevas oportunidades de venta, llegando a un mercado masivo mundial, siguiendo la máxima de "pensar globalmente y actuar localmente". Es posible desde diversificar el mercado abriendo nuevos segmentos en Internet hasta orientar completamente el modelo de negocio de la compañía en las ventas *on-line*. Son famosos en España y utilizados como modelo de éxito los casos de venta por Internet de lotería o de productos para deportes invernales.

Por otro lado, los procesos internos se automatizan, aumentando la productividad de los recursos humanos, no solamente retornando la inversión en tecnología sino además generando mayor valor añadido percibido por el cliente, con un importante ahorro de los costes internos. Esta infraestructura permite incluso implementar modelos de negocio gracias a las nuevas arquitecturas tecnológicas y de la publicación en Internet de servicios web corporativos basados en transacciones.

Entre estos nuevos servicios que comienzan a poblar el tejido empresarial actual se encuentran las diferentes variantes del denominado e-Business:

- Banca Online y transacciones relativas a productos bancarios, que han sido las primeras empresas en ver en Internet una fuente cada vez más amplia de consumidores (Paradigma e-Commerce).
- Supermercados y tiendas on-line, como una de las divisiones de negocio que amplía los ingresos tradicionales con el nuevo mercado "Business to Consumer" (Paradigma B2C).
- Reserva de billetes de medios de transporte, agencia de viaje, hoteles y empresas relacionadas con el sector de viajes y turismo
- Sector del ocio, especialmente la reserva de entradas para espectáculos, salas de cine, etc. Comienzan a despegarse también los nuevos servicios basados en la descarga de contenidos prepago, entre ellos la música y los videojuegos online.
- Formación on-line, universidades virtuales, cursos y masters a distancia, formaciones corporativas internas etc. (Paradigma e-Learning),
- Fabricación bajo demanda "Just-in-Time", iniciado en el sector automovilístico y posteriormente adaptado al sector informático, de forma que por cada solicitud de

venta se generan automáticamente varios pedidos de fabricación gracias a la integración entre aplicaciones corporativas (EAI).

- Subastas electrónicas de modificaciones de precios en tiempo real (sectores industriales, financiero y de seguros) para poder realizar intercambios virtuales de productos.
- Servicios de atención al ciudadano (administración pública), que permiten agilizar aquellas gestiones con la administración pública que tradicionalmente consumen tiempo y esfuerzo y conllevan una carga burocrática muy alta.

Por otra parte estas nuevas aplicaciones no tienen su único medio de comunicación y publicación en las redes públicas para sus clientes (Internet), sino que además se está dotando de interfaces web a las aplicaciones corporativas de uso interno, visibles desde las redes internas y entre delegaciones (Intranet) o con las redes de sus "*partners*" y proveedores (Extranet). Entre estas aplicaciones se encuentran:

- Intranets de gestión documental, servicios de indexación y documentación basados en ingeniería del conocimiento (sectores farmacéutico, médico y de ingeniería) que producen la ejecución distribuida de funciones, realizando la correlación y unificación de contenidos en un único frontal web (servidor web que hace de punto de entrada a la aplicación).
- Portales administrativos del empleado (nóminas, vacaciones, relaciones con los sindicatos, etc.) frecuentemente utilizadas por los Departamentos de Recursos Humanos para distribuir la información entre sus empleados.
- Sistemas de planificación de recursos corporativos (ERP, Enterprise Resource Planning), de soporte a decisiones (DSS, Decision Support Systems) y de minería de datos (Data Warehouse) mediante el proceso analítico de transacciones (OLAP, OnLine Analytical Processing y OLTP, OnLine Transactional Processing) que facilitan a la dirección la toma estratégica de decisiones en base a la unificación y correlación de información dispersa de los procesos internos de distintos departamentos (Comercial y Marketing, Financiero, Recursos Humanos y Nóminas, Producción y Fabricación, Logística y Distribución, etc.), así como una rápida detección y gestión del fraude o de anomalías en los patrones estadísticos de comportamiento.
- Sistemas de gestión automática de la relación con clientes (CRM, Customer Relationship Management) y proveedores (PRM, Partner Relationship Management), de forma que puedan aprovecharse, cuidarse y realizar un seguimiento de las relaciones con clientes y proveedores, orientando la empresa al cliente y facilitando la efectividad de las campañas de marketing y posibilitando el enlace con los sistemas de facturación y tarificación (Billing).
- Centrales de compras y gestión de aprovisionamiento SCM (Supply Chain

Management), donde el sector de la construcción ha sido pionero, para poder gestionar adecuadamente la rotación de stock y la provisión masiva de materiales a lo largo de la cadena de suministro. Un paradigma del denominado Business to Business (B2B).

- Sistemas de información geográfica (GIS) que por su propia naturaleza gráfica necesitan representar sus resultados mediante interfaz web.
- Incluso los propios departamentos de Sistemas de Información utilizan frontales vía web para la administración, gestión remota y monitorización de sus sistemas, servidores, bases de datos, electrónica de red, servidores de credenciales, autenticación única SSO (Single Sign On), gestión de certificados digitales, etc.

Y así sucesivamente, cada vez va incrementándose el número de procesos de negocio o servicios de soporte a las operaciones que se van automatizando y estandarizando mediante una interoperabilidad basada en las Aplicaciones Web.

3. Los nuevos riesgos

Tras unos primeros acercamientos de las empresas en Internet hace unos años, en que se publican en la página web los datos de contacto de la empresa e información pública corporativa, este proceso ha ido evolucionando recientemente en la forma de hacer partícipe a Internet en los procesos de negocio y en hacer accesible a los empleados internos, en la intranet y a partners corporativos, en la extranet información necesaria para el funcionamiento de la compañía mediante transacciones con todo o una parte de los datos corporativos, el componente principal de la compañía.

Este acercamiento a lo que actualmente se denominan “Empresas en Tiempo Real” focaliza todos los procesos de negocio corporativos en la **confidencialidad, integridad y disponibilidad** de la información, lo cual conlleva a su vez de una redefinición del riesgo basado en la incorporación de nuevas amenazas.

Basándonos en la fórmula:

Riesgo = Probabilidad de una intrusión x Impacto económico producido

se puede comprobar que la contrapartida a todas las ventajas enunciadas implica asumir un riesgo más elevado, debido a que ambos factores se incrementan simultáneamente:

- **Mayor probabilidad de intrusión**
  Desde el mismo momento en que se amplía el acceso a todos los usuarios, a todos los partners o a todo Internet, desaparece el grupo cerrado de usuarios que puede ser en

mayor o menor medida controlable y predecible. Cualquier persona en cualquier lugar del mundo podría intentar hacer mal uso de los permisos de acceso (por error y omisión o bien deliberadamente), provocando una intrusión en el sistema.

Aunque hace años solamente existía una probabilidad de intrusión alta en empresas con atracción para los colectivos de "hacking", las nuevas técnicas basadas en la comprobación de rangos completos de direcciones (IP scanning) o la búsqueda de objetivos vulnerables mediante buscadores web hacen que cualquier empresa que disponga de una dirección IP sea vulnerable, incluso aunque no tenga publicada su existencia en los buscadores ni en los servidores de nombres de dominio que hacen accesible las webs de las empresas.

- **Mayor impacto económico en la intrusión**
  Por otro lado, una brecha de seguridad podría comprometer los datos corporativos en los que se basa el negocio, provocando unos daños económicos variables dependiendo de la gravedad de la intrusión. Incluso podría no ser posible el cálculo del impacto económico o, en casos extremos y según se derive del Plan de Continuidad de Negocio, causar un impacto tal que la empresa se vea obligada a cerrar sus operaciones, como ocurrió en el año 2002 con el operador británico de telecomunicaciones "*Cloud Nine*" tras sufrir un ataque de red continuado.

Por tanto, la aparición de nuevas aplicaciones web conlleva una problemática asociada al nuevo riesgo de intrusión mediante el abuso de las transacciones, riesgo que se vuelve más crítico cuanto mayor es el impacto económico (riesgo operacional) o de imagen (riesgo reputacional, tan de moda en entornos financieros) derivado de dicha intrusión, además de incumplimientos con la legislación vigente por no haber securizado adecuadamente la información sensible (Agencia Española de Protección de Datos, ley Orgánica de Protección de Datos, Reglamento de Medidas de Seguridad, Ley de Servicios de la Sociedad de la Información, Ley General de Telecomunicaciones, etc.).

4. Protección de aplicaciones web

La protección ante vulnerabilidades web debería abordarse desde múltiples frentes, simultáneamente.

- Uno de los más importantes consiste en la integración de la seguridad en el ciclo de vida del desarrollo de las aplicaciones, incluyendo buenas prácticas de programación segura. Esto permitiría aumentar el grado de seguridad en las aplicaciones web en

producción. Un posible medio para abordar este frente es el dotar a los departamentos de desarrollo del reciclaje en seguridad necesario para proteger adecuadamente las aplicaciones, mediante un programa de formación o incluyendo personal de seguridad en los proyectos específicos de desarrollo de aplicaciones.

- En segundo lugar, estaría la protección de la aplicación utilizando controles técnicos dentro de la categoría de Seguridad en Aplicaciones Web, como cortafuegos de aplicación o pasarelas de control de transacciones web, además de la realización de auditorías periódicas de seguridad y pruebas de intrusión sobre las aplicaciones. En el mercado español son de sobra conocidas las empresas especializadas en este tipo de servicios y es considerable el aumento de propuestas para la creación de departamentos especializados dentro de las corporaciones.
- Se conoce genéricamente como productos de Seguridad en Aplicaciones Web aquella serie de productos especializados en la protección de las aplicaciones web a medida. Estas tecnologías tienen una serie de características comunes entre sí que las distingue de otras tecnologías como cortafuegos de red o sistemas de detección/prevención de intrusiones, que son las siguientes: están destinadas exclusivamente a la protección de aplicaciones web, analizan la interacción del cliente con las aplicaciones (principalmente la transacción), utilizan la protección con transacciones de valor alto y de fuerte impacto económico en caso de intrusión y, por último, la mayoría de los productos se comercializan en forma de dispositivo hardware de propósito específico destinado a la seguridad en aplicaciones web.
- Por último, las normativas y procedimientos adecuados de gestión dentro de los Sistemas de Gestión de Seguridad de la Información, tan de moda hoy en día gracias a los modelos ISO 17799, COBIT, etc. permiten automatizar los procesos de mantenimiento y reforzar los procesos de control de cumplimiento y adecuación, además de estandarizar una serie de métricas y facilitar un posible "*benchmarking*" con otros entornos similares o compañías con las mismas problemáticas.

5. Arquitectura de seguridad en las aplicaciones web

Las aplicaciones Web están construidas mediante desarrollos propios, basados en tecnologías como .NET, J2EE, PHP, etc. o productos específicos de gestión de contenidos. Esto requiere ciclos de vida clasificados en las etapas clásicas de Ingeniería de Software, como el análisis de requisitos, el diseño del sistema, la codificación de la aplicación, las pruebas del producto y la documentación y mantenimiento del mismo.

En cada una de estas etapas es posible (aunque no frecuente) la integración de un componente de seguridad, incluso desde la fase de diseño, con el objetivo de minimizar los

costes de una modificación posterior. Es práctica frecuente que la presión por liberar nuevos servicios en determinados plazos de entrega haya reducido el período de prueba, descartándose casi siempre la verificación formal del proceso de ejecución del sistema y las revisiones y auditorías del código fuente. Esto implica una liberación del sistema para su salida a producción con un grado aceptable de seguridad, pero con vulnerabilidades intrínsecas.

La seguridad en Aplicaciones Web, entendida como la protección del acceso a las aplicaciones web para evitar el abuso específico del código que provoque una utilización incorrecta de las transacciones, es un concepto relativamente moderno, en auge actualmente debido a la proliferación de nuevas vulnerabilidades basadas en Aplicaciones Web.

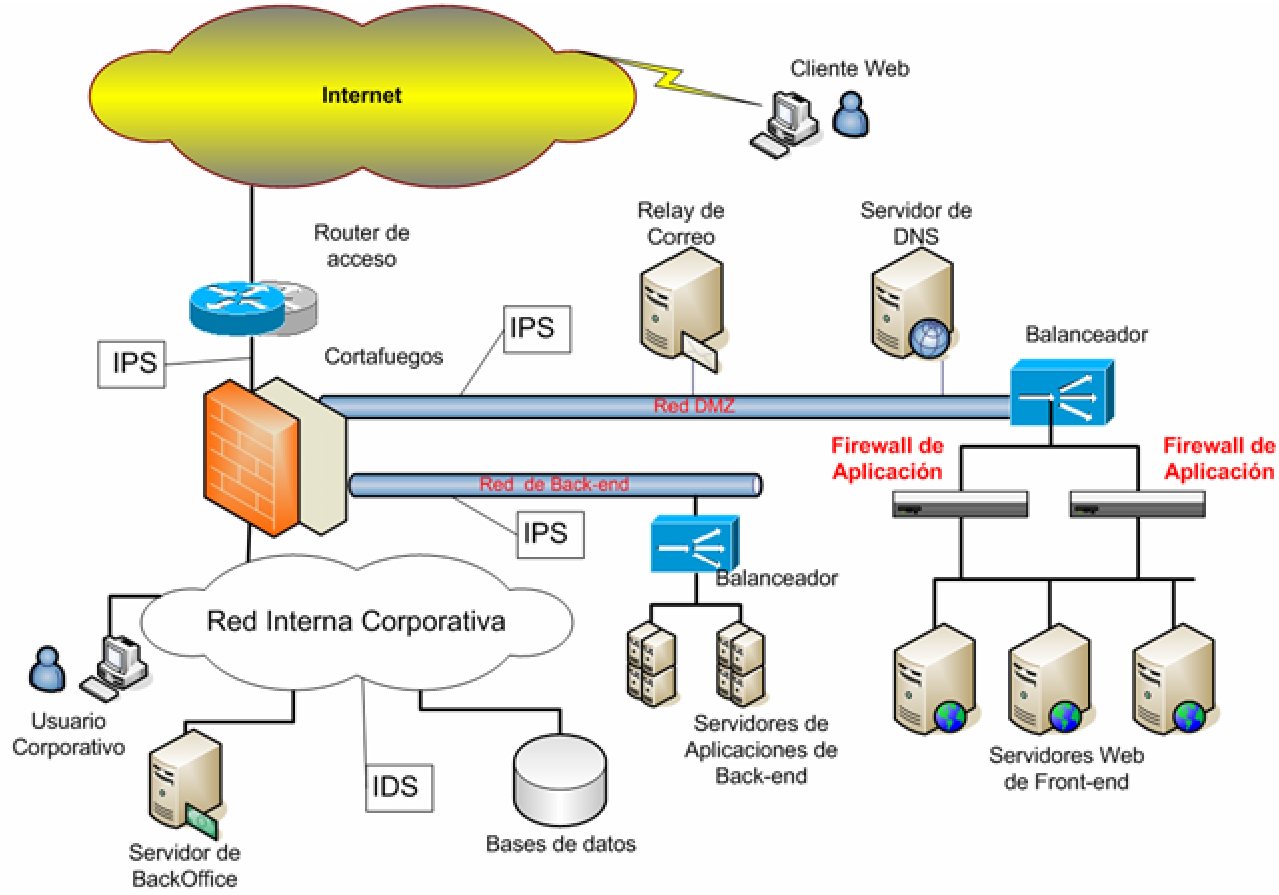
La mayor parte de las intrusiones en Aplicaciones Web consiste en la explotación de las deficiencias de seguridad inherentes al desarrollo de las aplicaciones, mediante la modificación de solicitudes válidas de acceso especialmente preparadas para que dicha Aplicación Web sea incapaz de gestionarlas correctamente. La intrusión se consigue mediante el aprovechamiento la respuesta obtenida de la aplicación. Las técnicas utilizadas para explotar las vulnerabilidades web han tenido tradicionalmente una aproximación manual, casi artesanal, dependiendo de la propia metodología de los auditores para buscar vulnerabilidades en la aplicación. Sin embargo, al igual que ha ocurrido en el pasado con las vulnerabilidades de red, la seguridad en aplicaciones web ha experimentado en los últimos años mejoras en lo relativo a estandarización, categorización y consenso en la metodología, así como una proliferación en las herramientas utilizadas y en los productos de protección de aplicaciones existentes.

La Seguridad en Aplicaciones Web es un nuevo mercado que comienza a surgir actualmente, como evolución lógica de las tecnologías de protección en red. Tiene su origen como contrapartida a la aparición de nuevos ataques que explotan directamente la integridad de las transacciones web, realizando modificaciones en las solicitudes del interfaz web que da acceso a los servicios corporativos. Estos nuevos ataques a su vez han surgido debido a la proliferación de nuevos servicios web.

Términos técnicos de ataques como por ejemplo inyección de SQL, Cross Site Scripting, envenenamiento de cookies o falsificación de parámetros son relativamente novedosos para este nuevo conjunto de amenazas a los servicios web y que necesitan de una protección adicional a la normalmente ofrecida por los sistemas de protección en red.

Esto es debido a que los Servicios Web proporcionan un acceso directo a la aplicación y a los datos que ésta gestiona, por lo que una modificación en el interfaz web que gestiona esos datos puede provocar de forma directa un ataque a la seguridad de los datos, en sus tres sentidos:

- **Confidencialidad:** lograr un resultado de publicación web de datos internos no autorizados, modificando los datos de entrada de las variables inyectando código que permita seleccionar y mostrar los datos confidenciales.
- **Integridad:** provocar una modificación de los datos internos mediante la modificación de los parámetros deseados o mediante la inyección de sentencias que provoque la ejecución de procedimientos internos.
- **Disponibilidad:** provocar una denegación del servicio mediante la inyección de códigos o parámetros cuya interpretación o gestión de excepciones no es gestionada correctamente por la aplicación.



Frente a este tipo de tecnologías no existe un sistema único de protección, sino que es necesario abordarlo en tres frentes: control de accesos (mediante cortafuegos de red), control del tráfico (mediante sistemas de prevención de intrusiones en red) y control de las transacciones (mediante cortafuegos de aplicaciones web). Veamos un ejemplo de cómo podrían implementarse en una topología ideal estos tres niveles de protección, todos ellos necesarios para lograr una correcta securización de los servicios web en producción.

Se describen a continuación los distintos componentes de la arquitectura:

- **Usuarios del servicio**, que acceden a través de Internet a las Aplicaciones Web. Aunque los usuarios autorizados están agrupados y delimitados, los posibles atacantes de la aplicación web no forman parte de ningún grupo identificado ni predecible, pues pueden provenir desde cualquier parte del mundo con posibilidad de acceso a la aplicación.

- **Routers de acceso**, normalmente en propiedad o bajo gestión del ISP u operador de telecomunicaciones que provee del servicio de acceso a Internet y hace públicas las aplicaciones corporativas mediante publicación del direccionamiento IP. En este paso es posible encontrar una primera barrera de protección, basada en las ACLs, o listas de control de acceso, que realizan un primer filtrado basado en el direccionamiento IP de los usuarios válidos, o establecen un túnel VPN.

- **Sistemas de Gestión de Ancho de banda:** equipos que reparten el tráfico de entrada y salida (normalmente desde y hacia Internet) clasificando el tráfico según las diferentes prioridades y gestionando el ancho de banda disponible dependiendo del autoaprendizaje del tipo de servicios utilizados (independientemente del tipo de puerto TCP)

- **Cluster de cortafuegos de red**, actualmente el primer paso en el proceso de protección perimetral de cualquier sistema de información accesible en red. Controla el acceso entre diferentes redes y permite o prohíbe el establecimiento de sesión contra determinadas máquinas. Protege de intentos de acceso a máquinas no autorizadas o a servicios no autorizados dentro de una máquina accesible. Además, realiza estas comprobaciones a la máxima velocidad, pues básicamente se constituye en un sistema de enrutamiento que permite centralizar las políticas de seguridad, de enrutamiento, de traducción de direcciones, de establecimiento de túneles VPN e incluso de ciertas capacidades de filtrado de contenidos.

  Sin embargo esta protección, necesaria sin duda ninguna, no es suficiente para proteger al servicio de ataques a nivel de red que son válidos respecto a su política de seguridad (por adecuarse al rango permitido de origen – destino – servicio – autenticación) y por tanto logran atravesar la barrera del cluster cortafuegos. Surge entonces la necesidad de los sistemas de detección de intrusiones en red.

- **Zona Desmilitarizada (DMZ)** en la que se conectan los servidores de acceso público, normalmente protegida por un IDS (*Intrusion Detection System*) o un IPS (*Intrusion Prevention System*). Los sistemas de detección de intrusiones (IDS) comprueban el tráfico existente en la red, analizando el contenido mediante técnicas heurísticas y

patrones de intrusión, comparándolo con la adecuación al protocolo respecto a la detección de anomalías y a una serie de patrones identificados o al menos generalmente aceptados como potenciales intentos de ataque. De esta manera es posible comprobar, dentro de la carga (*payload*) del tráfico, si una sesión aparentemente válida contiene en realidad una secuencia de la que se tiene cierta seguridad que el servidor no va a poder gestionar correctamente.

La problemática principal de la detección de intrusiones proviene en la necesidad de gestión y reacción inmediata de las alertas. Es por ello que los fabricantes tradicionales de IDS han ido evolucionando paulatinamente sus productos hasta reconvertirlos en sistemas de prevención de intrusiones (IPS), de forma que puedan cortar/bloquear la intrusión en tiempo real, insertando un dispositivo en línea que pueda bloquear el ataque.

Este tipo de protección también es necesaria para prevenir ataques contra servicios en red, pero en el caso de Aplicaciones Web son insuficientes al no conocer la lógica de la aplicación. Es en este caso donde entran en escena la nueva tecnología que proporcionan los cortafuegos de aplicaciones web, como complemento de las anteriores.

- **Balanceadores Web**, que permiten publicar un servicio externo mediante una infraestructura interna de varios servidores redundantes replicados para garantizar la continuidad del servicio y un correcto aprovechamiento del ancho de banda, equilibrando la carga de tráfico entre los distintos servidores. Aquí se suelen encontrar también los **Servidores de Caché** y los **Aceleradores por Compresión Web.**

- **Cortafuegos de Aplicaciones Web**, que protege al sistema frente a vulnerabilidades específicas de la aplicación. Tanto el Balanceador de web como el cortafuegos de aplicación web suelen incluir **aceleración Criptográfica SSL** (incluso balanceador y cortafuegos web pueden coincidir en la misma máquina, o bien constituirse en un software basado en el propio servidor de web). Un cortafuegos de aplicación web es un sistema que analiza, filtra y protege las interacciones entre los navegadores cliente y el frontal de web que sirve como punto de entrada a las aplicaciones web existentes; infraestructura de backend soportada por los servidores de aplicaciones, servidores de backoffice y bases de datos que proveen de contenido al interfaz del navegador.

  Por ello, la función de los cortafuegos de aplicación se basa en delegar estos esfuerzos de filtrado y comprobación en un elemento externo que proteja contra ataques a nivel de aplicación. En realidad, las buenas prácticas del desarrollo seguro de aplicaciones no implican una delegación total de la seguridad en estos elementos, pero sí el poder mantener las aplicaciones seguras, mientras se dispone de tiempo, pasado el “time to

market" de lanzamiento recomendado para salida a producción, garantizando una correcta protección del servicio.

- **Frontal de Web**, constituido por una batería de servidores web redundantes con un mismo contenido común replicado (denominada granja de servidores), que sirven de punto de entrada del usuario a nivel de aplicación. Estos frontales de web son, en su mayor parte, aplicaciones a medida orientadas específicamente para dar soporte a una aplicación en concreto. Suelen programarse con tecnología .NET, J2EE, PHP o similares por un equipo de desarrollo propio o de terceros, y con un tiempo de entrega definido por el "time to market" que obliga a liberar nuevos servicios en unas fechas determinadas. Esto implica que todas las aplicaciones desarrolladas a medida llevan acarreada implícitamente la posibilidad de que sean explotadas aprovechando una vulnerabilidad para la que no haya existido tiempo suficiente de corregir o depurar. El riesgo en este sentido es la posibilidad de que explotando las vulnerabilidades inherentes al código se pueda comprometer la seguridad de los datos de provisión.

- El frontal de web accede a su vez a los **Servidores de Aplicaciones** y éstos a su vez originan las peticiones a las bases de datos, o bien a los **Servidores Corporativos** (denominados de Back-Office) que alojan las aplicaciones corporativas que a su vez consultan a las **Bases de Datos**.

De esta forma se prohíbe el acceso directo de los usuarios a los datos corporativos, salvo mediante un interfaz de web desarrollado específicamente para generar transacciones basadas en el acceso a las bases de datos. Securizando el sistema y favoreciendo la usabilidad y accesibilidad para todos los usuarios.

6. Desarrollo seguro de aplicaciones web

La constante inversión tradicional en seguridad de red, olvidando el facto de aplicación, no ha disminuido los ataques a los servicios web corporativos. Incluso, aunque en principio las nuevas soluciones específicas para la protección de web, como son los Cortafuegos de Aplicación Web, constituyen actualmente la vanguardia tecnológica para proteger este tipo de servicios, siguen siendo una medida preventiva para proteger el acceso y facilitar el lanzamiento seguro a producción, mientras se planifican las revisiones periódicas correspondientes, basadas en auditorías y revisiones de código para comprobar la adecuación del desarrollo a las buenas prácticas de programación segura. Es la existencia de una metodología de securización y de buenas prácticas de desarrollo y programación segura la que debe de complementar la implantación de salvaguardas técnicas.

El primer esfuerzo en este sentido ha venido de la mano de OWASP (Open Web Application Security Project), organización encargada de unificar esfuerzos en la clasificación de vulnerabilidades de seguridad web. Uno de sus logros ha sido el consensuar una lista de comprobaciones de seguridad para mostrar el grado de exposición de una aplicación web y una metodología estándar y consensuada para el desarrollo seguro de aplicaciones.

Además de la categorización, se ha avanzado en la definición de un lenguaje estándar de descripción de vulnerabilidades web, denominado AVDL (Lenguaje de Descripción de Vulnerabilidades de Aplicación), especificación liberada recientemente por OASIS, Organización para el Avance de Estándares de la Información Estructurados. Este estándar se basa en un esquema de definición de datos que describe las solicitudes web realizadas a nivel de transacción (denominadas pruebas), las respuestas del servidor, las vulnerabilidades encontradas y su descripción. De esta forma, se permitirá la interoperabilidad entre componentes de seguridad, como por ejemplo, el realizar comprobaciones de seguridad con herramientas automáticas de detección de vulnerabilidades web, exportar los resultados en este formato y poder importarlos en los sistemas de protección, de forma que se reconfiguren dinámicamente con los nuevos datos obtenidos. Este lenguaje descriptivo deja abierta la posibilidad de aplicaciones futuras, sobre todo en el ámbito de la correlación de eventos y en la integración de componentes de seguridad.

7. Hacking de web

Los ataques de aplicación se basan en explotar vulnerabilidades inherentes en el propio desarrollo de la aplicación y en la interpretación que ésta hace de los parámetros en las transacciones, algo para lo que la defensa perimetral y de protección de intrusión en red no es suficiente, entre otras cosas porque es diferente para cada aplicación web desarrollada a medida que existe en el mundo y no es viable determinar un patrón común más que para proteger el software servidor estándar.

Hablando más técnicamente, las intrusiones con éxito en aplicaciones web se basan principalmente en:

- Modificación de las validaciones de autenticación mediante un software intermedio (denominado proxy local) que las intercepte en la parte cliente y devuelva un valor de retorno correcto como resultado las funciones llamadas, provocando así la validación de la autenticación. Aunque una regla básica de seguridad es no delegar en la parte cliente cualquier sistema de validación o autenticación que pueda ser modificado, esto es, sin embargo, una práctica común actualmente.

- Modificación de los parámetros enviados al servidor, tanto como parte de un formulario como dentro de campos ocultos. Actualmente, el hecho de que las transacciones estén protegidas por el cifrado SSL del protocolo de web https, no evita que sea posible verse en texto claro (con un software de proxy local en el navegador cliente) el contenido de los parámetros y, por tanto, sean sujeto de modificación, algo también frecuente actualmente.

- Inyección de código en la transacción, bien en la propia solicitud web, llamada URL, que degraden la seguridad variando la confidencialidad (por ejemplo, ataques de revelación de información mediante inyección de códigos de script en campos de formularios), la integridad (por ejemplo, ataques de modificación de datos internos corporativos mediante la denominada "inyección ciega" de sentencias de acceso a bases de datos) o la disponibilidad (por ejemplo, ataques de desbordamiento de buffer mediante la inyección de los denominados Shellcodes, un tipo de ataque en el que comienza la intersección con los IPSs).

Aunque tradicionalmente han existido múltiples posibilidades para la comprobación de vulnerabilidades a nivel de red, todavía son escasas las relacionadas con la comprobación de la seguridad a nivel de aplicación web, aunque cabe destacar que están comenzando a proliferar. Esta tecnología evolucionó gracias a la aparición de los componentes software de tipo Proxy, que permiten un ataque de tipo "*man in the middle*". Este ataque se basa en suplantar la identidad del servidor para el cliente y viceversa, interceptando el tráfico y realizando modificaciones en la transmisión, de ahí su nombre.

La comprobación de vulnerabilidades específicas en aplicaciones web ha evolucionado desde el software libre hacia entornos más comerciales que han surgido últimamente. Incluso también existen aplicaciones basadas en software libre, desarrolladas específicamente con vulnerabilidades intrínsecas, con el fin de servir de plataforma de pruebas sobre la nueva problemática de vulnerabilidades web.

8. El mercado de seguridad web

Un denominador común en los fabricantes de tecnologías de Cortafuegos de Aplicaciones web es que se ha vivido un largo periodo de "evangelización" en la existencia de las nuevas amenazas y la posibilidad de protegerse contra ellas. No es hasta muy recientemente cuando han empezado a cosecharse los frutos de la siembra anterior en un mercado que está evolucionando muy rápidamente y con un enorme potencial de crecimiento. Respecto al mercado más genérico de fabricantes de productos de seguridad, el mercado actualmente está maduro respecto a productos y las compañías integradoras comienzan a diferenciarse por los

servicios de valor añadido en esa integración.

Un estudio reciente de **Yankee Group** denominado "Assessing What's Hot in Web Application Security" indica que el área de Seguridad de Aplicaciones Web es uno de los segmentos de mayor expansión hasta el año 2009. A este segmento se van a asignar una parte creciente de los presupuestos de seguridad de la información que tradicionalmente se asignaban a otros segmentos dentro de la seguridad. Los responsables (directivos) de las empresas están especialmente preocupados por "sus" aplicaciones y datos que están llevando a la red. Es por ello, que se hacen necesarios sistemas de seguridad que garanticen las transacciones impidiendo ataques.

Sin embargo, no todo son ventajas para los Cortafuegos de Aplicaciones Web; existen inconvenientes tanto técnicos como administrativos que ralentizan su implantación dentro de las infraestructuras de seguridad.

- **Necesidad de personalización**: al contrario que los sistemas tradicionales de protección en red, que pueden configurarse sin que exista incluso ningún servidor detrás a proteger; los Cortafuegos de Aplicaciones Web necesitan personalizarse respecto a la aplicación que van a proteger, lo cual implica conocer la estructura de los servidores web. Para llegar al máximo nivel de personalización incluso es necesario conocer los nombre de los parámetros y, si se quiere la máxima granularidad en la protección, incluso los rangos de valores permitidos por la aplicación. Esto conlleva no sólo tiempo y esfuerzo si se quiere llegar a securizar al máximo nivel una aplicación sino además coordinar diversos departamentos.

- **Disminución de los tiempos de respuesta**: es innegable que cualquier sistema basado en analizar tráfico, necesita de un tiempo para realizar la comprobación, lo cual provoca una cierta ralentización del rendimiento de la aplicación. En un mercado acostumbrado a los retardos de milisegundos provocados por dispositivos de red y cortafuegos de red (que únicamente analizan la cabecera del tráfico) es complicado equilibrar la balanza entre rendimiento y seguridad, teniendo en cuenta que el hecho de analizar una transacción obliga a inspeccionar los campos de una transacción a nivel de aplicación y puede llegar a incrementar un tiempo de respuesta de por sí ya dilatado por el hecho de acceder a servidores web, servidores de aplicaciones, servidores de backoffice y bases de datos.

- **Separación entre seguridad y desarrollo**: la mayoría de los departamentos de Tecnología de la Información mantienen una separación total (a veces brutal) entre los departamentos de seguridad en sistemas y comunicaciones (encargados de activar o

desactiva reglas en cortafuegos de red y sistemas de protección de intrusiones) y de los departamentos de desarrollo, encargados de sacar adelante la aplicación. No es frecuente en los equipos de desarrollo de aplicaciones una preocupación por la seguridad, bien por conocimiento, bien por las presiones de los tiempos de lanzamiento a producción. Esta preocupación suele delegarse en el departamento específico de Seguridad y Comunicaciones. A su vez, éste último departamento suele preocuparse de la seguridad a nivel de aplicación (ni mucho menos de profundizar en los parámetros y valores de las transacciones) pues suele formar parte del trabajo del departamento de desarrollo.

Todo esto permite que, a pesar de que las aplicaciones siguen siendo claramente vulnerables a nivel de aplicación (como demuestran las continuas auditorías de seguridad y frecuentes intrusiones en las aplicaciones), la responsabilidad sobre su correcta securización se difumina, salvo que exista una política de seguridad clara y desarrollada, con un Responsable de la Aplicación al frente, que sepa unificar ambos departamentos limitando el riesgo del conjunto de la aplicación.

8. Resumen

Aparte de las medidas organizativas y de alineamiento con los objetivos del negocio, las medidas técnicas adoptadas para la securización de Servicios Web, deberían ir encaminadas hacia la protección integral de todos los puntos de amenaza.

- Tradicionalmente el primer nivel ha sido la seguridad perimetral y el control de accesos, que se han resuelto mediante cortafuegos en red, etc.
- La evolución de los ataques ha necesitado de un segundo nivel que proteja de ataques en red contra los diversos tipos de servicios. Esto se está resolviendo actualmente con sistemas de detección y prevención de intrusiones, antivirus, etc.
- Nuevos tipos de ataques a nivel de aplicación están creando la necesidad de una evolución, que proteja las transacciones en servicios de web analizando la interacción entre el navegador cliente y la plataforma de servidores. En este nivel es donde se producen la mayor parte de ataques actualmente. Los productos que incorporan estas nuevas tecnologías se denominan de forma genérica Cortafuegos de Aplicaciones Web.

Sin embargo, casi más importante que elegir los productos correctos es el seleccionar a la empresa consultora o integradora adecuada que nos asesore con su experiencia y know-how en la definición e implantación de la política de seguridad y tecnologías a implantar, sin perder de vista que todos los sistemas de información deberían estar encaminados a conseguir los

objetivos de negocio.

Por tanto, las medidas de seguridad más adecuadas serán aquellas que logren disminuir el riesgo de intrusión de forma que la amortización de la implantación de dichas medidas sea económicamente menor que el riesgo resultante de no implantarlas, lo cual implica que en el fondo cualquier medida técnica debe tener una justificación de negocio y, en último término financiera.

http://www.sentryware.com

- **CAPITULO 7: SEGURIDAD EN EL COMERCIO ELECTRÓNICO**

1- ¿Qué se entiende por Comercio Electrónico o e-commerce?

En general, por comercio electrónico se entiende toda compra realizada a través de Internet, cualquiera que sea el medio de pago utilizado. La característica básica del comercio electrónico se basa, pues, en la orden de compraventa, la cual tiene que realizarse través de algún medio electrónico, con independencia del mecanismo de pago efectivo. En cualquier caso, las distintas instituciones estadísticas utilizan definiciones que pueden variar entre sí, y en especial se encuentran divergencias en lo que cada una de ellas entiende por medio electrónico

Así, U.S. Census Bureau define el comercio electrónico como aquel que *mide el valor de los bienes y servicios vendidos online a través de redes publicas como Internet, o redes privadas basadas en sistemas tales como el de Intercambio Electrónico de Datos (EDI). Las ventas de comercio electrónico son ventas de bienes y servicios para las cuales la orden de compra o la negociación del precio y condiciones de la venta tienen lugar a través de Internet, de una extranet como la red EDI, u otro sistema online. El pago podrá o no hacerse efectivo online.*

Alternativamente Statistics Canada (StatCan) da una definición según la cual *por comercio electrónico se entiende aquel comercio desarrollado a través de Internet. Esto es, transacciones llevadas a cabo sobre un canal computerizado, consistentes en la transmisión de la propiedad o uso de activos tangibles o intangibles*

De esta definición quedan, pues, excluidas las ventas realizadas a través de EDI por redes dedicadas, cajeros automáticos, así como las transacciones financieras vía Internet (si bien las comisiones bancarias derivadas de dichas operaciones estarían incluidas)

Finalmente, tanto Eurostat como la OCDE utilizan una definición de comercio electrónico basada en el criterio por el cual la orden de compra/venta que se efectúa debe ser electrónica para que la transacción sea considerada comercio electrónico.[5]

Como puede observarse, bajo estas definiciones no importa el medio de pago efectivo de la transacción, sino el sistema utilizado para efectuar la orden de compra.

Así pues, puede definirse comercio electrónico como toda transacción realizada electrónicamente a través de Internet, excluidas las realizadas en cajeros automáticos, EDI, terminales de telefonía móvil, con independencia del medio de pago utilizado, y del mecanismo de intercambio utilizado (adhesión, subasta, negociación entre las partes, etc.)

2. ¿Qué es realmente el Comercio Electrónico?

La percepción apuntada en el apartado anterior, es decir, utilizar el término de comercio electrónico para referirse exclusivamente a la compra de bienes o servicios a través de Internet, es una visión sesgada de la realidad que, cuando hablamos de seguridad en el comercio electrónico, tiene el efecto de limitar el alcance de las medidas de seguridad a sólo aquellos activos de la organización que intervienen directamente en los procedimientos de pago, dejando de lado otros aspectos igualmente importantes que forman parte del comercio electrónico.

El término comercio electrónico, en realidad engloba a cualquier solución que permita realizar las funciones comerciales mediante el empleo de redes de datos. No obstante, en este texto limitaremos a dos redes: Internet y redes de telefonía móvil, dejando a un lado las redes especiales sobre las que se realizan multitud de funciones comerciales entre empresas, tales como EDI o SNA.

Centrarse en Internet y telefonía móvil obedece a que la presencia de una de las dos o de ambas redes es condición imprescindible si una de las partes involucradas en la relación comercial es un particular o una pyme. Incluso, cada vez en mayor medida, empiezan a ser las redes soporte de transacciones entre grandes empresas, debido al importante ahorro de costes que permiten gracias a la extensión del ADSL y a la utilización de VPN para sustituir enlaces delicados.

Pero donde no debe simplificarse el alcance del término comercio electrónico es en lo que respecta a las funciones comerciales, pues son muchas las que pueden realizarse por medios electrónicos:

1. Actividades de Marketing (información comercial, presentación de productos, investigación de mercado, captación de clientes...)
2. Creación de surtido (función habitual en los denominados portales, que integran en un web ofertas de diversa índole procedentes de distintos sitios web, convirtiendo al portal en “referenciador” o, incluso, en intermediario)
3. Gestión de pedidos: concreción de la venta (obtención de información del comprador para el cobro y posterior envío –dirección física, correo electrónico-, comprobación de datos
4. Gestión de cobros (facturación telemática, cobro de la venta de bienes o servicios)
5. Distribución de bienes (software, e-books, localizadores para hoteles...) o servicios (de asesoría, de intermediación financiera, de traducciones...), sin olvidar la gestión

logística, entendiendo como tal la automatización de las ordenes de envío a través de la conexión del site en el que se ha realizado la compra con los servidores de empresas de mensajería especializadas.

6. Atención al cliente: servicio postventa, asistencia técnica, recepción de sugerencias y reclamaciones por defectos en bienes o servicios, por incidencias en la entrega, por errores de facturación...

Considerando la definición indicada para comercio electrónico, tenemos que la práctica totalidad de empresas con WEB están participando en la aventura del comercio electrónico, incluso si sólo se limitan a anunciar sus productos sin dar la opción de adquirirlos vía WEB.

3. Seguridad en el Comercio Electrónico

Ahora sí es posible apreciar la importancia de considerar aspectos de seguridad para proteger las distintas funciones comerciales integradas en el comercio electrónico, y no sólo las de cobro.

1. **Actividades de Marketing**

   La falta de seguridad en este campo puede afectar muy negativamente a un activo tan importante para la empresa como es su imagen. Pensemos en las consecuencias de un ataque de modificación de nuestra página principal.

   También son peligrosos los ataques de denegación de servicio o los problemas de indisponibilidad del web derivados de cualquier otra causa, que van a influir en el aspecto de captación de clientes, que fácilmente pueden ir a buscar a un competidor cuyo web no tenga problemas y que pueda atender a su demanda.

2. **Creación de surtido**

   En este apartado, debe vigilarse la integridad de los enlaces a páginas o aplicaciones instaladas en un tercero, pues el ataque más peligroso en este campo sería aquel en el que el visitante de un portal pinchase en un enlace y fuese dirigido a un falso web, ya que, aparte de que el portal perdería las comisiones que procediesen, el usuario podría ser fácilmente engañado entregando sus datos sensibles (número de tarjeta, claves de acceso a banca electrónica...) al web pirata.

3. **Gestión de pedidos**

   En este campo debe vigilarse la robustez de los formularios de captura de datos para evitar problemas de seguridad derivados de desbordamiento de buffers o similares.

4. Gestión de cobros

La seguridad en el momento del cobro es sumamente importante (analizaremos más adelante las soluciones específicas a esta cuestión) pues es normalmente el único punto en el que el cliente que paga siente la necesidad de percibir que puede estar tranquilo proporcionando sus datos económicos (número de tarjeta o número de cuenta).

No obstante, en España, no así en otros países, es habitual dejar en manos de un tercero la gestión de cobro con tarjeta mediante la instalación en el web de lo que se conoce como un TPV virtual.

Al igual que con los TPV físicos, la gestión del cobro se delega en una entidad bancaria que será responsable de implementar las medidas de seguridad pertinentes. El Web de comercio electrónico se limita a redirigir al cliente, de forma transparente para éste, a la entidad bancaria, a la cual habrá comunicado previamente el importe de la transacción y la referencia para el cobro. La entidad bancaria será la que solicite al cliente su número de tarjeta y la que proceda a efectuar el cargo en la misma, comunicando al Web únicamente el resultado, positivo o negativo, de la transacción.

De este modo el Web nunca conoce el número de tarjeta del cliente, y la seguridad para el mismo es, al menos a priori, máxima ya que el banco dispone de los medios para garantizar dicha seguridad.

Sin embargo pocas veces el cliente es capaz de distinguir si sus datos se los está facilitando a la tienda Web o a una entidad bancaria, por lo que no está de más que el web recalque este aspecto en la información sobre el proceso de cobro que ofrece a sus clientes.

Cabe indicar que es poco habitual que los datos de una tarjeta se roben durante una transacción, ya que los mismos viajan –o deben viajar- siempre cifrados mediante el protocolo SSL. El riesgo real está en el robo de las bases de datos con números de tarjeta que pueden estar almacenadas en un web a modo de registro de las transacciones realizadas. Por ello, estos registros deben guardarse siempre cifrados. Todo esto, claro está, en caso de que se haya optado por cobrar directamente, pues en el caso de utilizar un TPV virtual, es el banco el responsable del almacenamiento y custodia de estos datos.

Han aparecido también en escena métodos alternativos que cabe considerar a la hora de implantar un sistema de cobro por Internet tales como el pago seguro por móvil,

(mobipay y similares) en los cuales el cliente recibe en su teléfono móvil los datos de la operación que va a realizar, y si los confirma, el importe se le carga directamente en la cuenta asociada a su teléfono móvil. Estos métodos tienen para el usuario la ventaja de la percepción de seguridad asociada al teléfono móvil, que es mayor que la asocia a Internet, pero habrá que estar vigilantes de las nuevas amenazas que acechan a los móviles de última generación dotados de interpretes Java y de conexiones permanentes a Internet.

Pero la gestión de cobros va más allá del acto de cobrar, ya que debe cumplirse la reglamentación vigente en materia de facturación, y si se pretende aprovechar las ventajas de la facturación telemática deberán cumplirse un conjunto adicional de medidas de seguridad.

5. **Distribución de bienes** (software, e-books, localizadores para hoteles...) o servicios (de asesoría, de intermediación financiera, de traducciones...), sin olvidar la gestión logística, entendiendo como tal la automatización de las ordenes de envío a través de la conexión del site en el que se ha realizado la compra con los servidores de empresas de mensajería especializadas.

   En aquellos webs cuyo negocio permita el envío telemático de los bienes y servicios que adquieran los clientes resulta fundamental establecer mecanismos de seguridad muy robustos que, por un lado, impidan la visualización no autorizada de datos o descarga de ficheros ya que, el sitio estaría siendo víctima de un robo en el más fiel sentido de la palabra. Por otro lado, también es vital proteger la integridad de la información y datos que se venden, ya que no son raros los ataques de alteración de los mismos, como el de una conocida distribuidora de cursos de autoformación que un día empezó a recibir quejas de sus clientes por el contenido pornográfico del material que distribuía.

6. **Atención al cliente:** servicio postventa, asistencia técnica, recepción de sugerencias y reclamaciones por defectos en bienes o servicios, por incidencias en la entrega, por errores de facturación.

Para la seguridad en estas funciones comerciales es aplicable lo indicado para las funciones de marketing, ya que el web deberá tener un alto grado de disponibilidad y ofrecer una buena imagen de la empresa.

Además es importante vigilar la seguridad de otros sistemas informáticos de la compañía, ya que la atención post venta depende también en gran medida del buen funcionamiento de los servidores de correo electrónico.

4. ¿Es posible el Comercio Electrónico sin seguridad?

La utilización del comercio electrónico proporciona a toda empresa una presencia a nivel mundial a unos costes insignificantes. Así mismo, la incorporación de sistemas de pago electrónico puede proporcionar toda una serie de nuevas oportunidades de negocio así como un significativo ahorro de costes en la logística necesaria tanto para comprar como para vender. Sin embargo, a pesar de todas estas indiscutibles ventajas, el tan esperado auge del comercio electrónico todavía no se ha producido. Uno de los principales motivos ha sido la desconfianza de los potenciales usuarios del mismo para su uso. Es indudable por tanto, que las transacciones económicas a través de Internet poseen una serie de cuestiones de seguridad que los empresarios deberán tener en cuenta antes de acometer este tipo de proyectos, o de lo contrario puede venirse abajo toda su estrategia comercial y su reputación en el mercado derivada de cualquier incidente no deseado.

5. Algunos ejemplos significativos

Dos de los primeros sitios españoles de comercio electrónico, Uno-e y El Corte Inglés, han sido noticia por problemas derivados en la seguridad que aplican en sus sitios y que posibilitan que elementos sin escrúpulos puedan manipular u obtener ilegalmente datos privados de sus usuarios. He elegido estos ejemplos por ser públicos y por la notoriedad de las empresas implicadas, pero esto es sólo una pequeña parte de la punta del iceberg de lo que los expertos en seguridad de la información nos encontramos cada día:

a) El caso Uno-e

Un grupo de hackers, conocidos con el nombre de "Mentes inquietes" ha publicado en su página Web diversas pruebas de como pudieron acceder a cuentas de otros usuarios, simplemente "cambiando" de manera aleatoria el "ID" que se asigna a cada usuario una vez ha accedido al sitio online.

Cualquiera, explican en su página Web, podía ver las cuentas, el saldo e información personal de los clientes del banco online.

"El que estos datos sean fácilmente accesibles por cualquiera mínimamente habilidoso puede permitir a terceros malintencionados el uso de los mismos con carácter fraudulento y estafar a clientes de dicha entidad mediante ingeniería social", explican los hackers en su web.

Los hackers levantaron incluso una acta notarial sobre estas vulnerabilidades, protegiéndose así de cualquier acusación de "manipulación" que la entidad pudiera ejercer.

El Banco ha informado ya que el "agujero" ha sido solucionado y que la privacidad de sus clientes y sus cuentas están a salvo, aunque durante semanas no haya sido así.

b) El caso El Corte Inglés

En esta ocasión, ha sido un informático, Lorenzo Hernández Garcia-Hierro, quien descubrió que la tienda electrónica más visitada en nuestro país es vulnerable de ser usada para un ataque XSS (Cross Site Scripting).

Aprovechando esta vulnerabilidad (solo utilizable en el contexto del cliente), se pueden falsificar y modificar formularios de identificación para engañar al cliente y hacerle pensar que se encuentra ante el Corte Inglés cuando realmente también está conectado a una página IFRAME donde se puede incluir de forma "transparente" un sistema de login/identificación del cliente falsificado en otro sitio y que envíe los datos del cliente al atacante, robar las cookies de datos del usuario o incluir archivos ejecutables en el cliente (con navegador Internet Explorer).

La Asociación de Internautas que ha tenido conocimiento del hecho recomienda a los internautas que hasta que no se subsane dicho fallo de seguridad no accedan a dicha web desde ningún enlace externo, sino tecleando directamente en el navegador su dirección.

Dos casos, de empresas de "primera categoría" que pueden echar por tierra los esfuerzos que se están realizando para aumentar la confianza de los consumidores en las compras online y la seguridad de estas, primer factor señalado en distintos estudios de preocupación por parte de los cybercompradores.

6.- El Phising

Mención especial merece una nueva lacra (seguramente no la última) que acecha y amenaza al comercio electrónico: el phising.

El phishing consiste en la realización de ataques que tienen como fin robar datos confidenciales, normalmente los datos de autenticación como usuario y contraseña de servicios de banca electrónica. En lugar de usar complicados sistemas técnicos para atacar a la entidad bancaria, se emplean técnicas relativamente sencillas de engaño hacia el usuario del servicio que pasan normalmente por el envió de correos electrónicos o el uso de sitios web fraudulentos que simulan el aspecto y la funcionalidad de los sitios reales.

Además de los bancos, cualquier otro servicio que permita administrar de forma electrónica dinero u otros bienes puede verse afectado. Así, servicios de bolsa, tarjetas de crédito, transferencias electrónicas, tiendas o subastas on-line sufren de manera casi continua ataques de este tipo.

Los conocimientos técnicos necesarios para llevar acabo un ataque de phishing son mínimos. En el caso mas común, el atacante crea un correo electrónico html con el diseño, colores corporativos y logotipos del banco que bajo diversas excusas (como comprobaciones de seguridad o actualizaciones del servicio) solicita al usuario que ingrese sus datos, que serán enviados a sitios web hospedados en países con falta de legislación en materia de fraude electrónico, o en servidores previamente “hackeados”. Para hacer más creíble el fraude, ha habido casos en los que incluso se ha enlazado el correo fraudulento con páginas reales del servicio de banca o se han abierto paginas adicionales del propio servicio para dar una mayor credibilidad al ataque.

Dado que el objetivo del ataque son los usuarios del servicio y no el propio servicio, las medidas de seguridad adoptadas por la entidad suelen tener poca repercusión para evitar los ataques de phishing. Aún así, existen algunas excepciones como las vulnerabilidades del tipo Cross Site Scripting (XSS) que pueden emplearse para realizar los ataques de phishing a través de los propios sitios web del servicio de banca electrónica aumentando las probabilidades de engañar a la potencial victima.

Las medidas de seguridad pasan a corto plazo por la implantación de programas de divulgación al usuario para informarle sobre qué es el phishing y cómo debe proteger sus credenciales de autenticación. Igualmente, se deben incorporar a las políticas de privacidad ya existentes, apartados o referencias que indiquen al usuario claramente cuándo y cómo se le puede requerir sus datos personales y de autenticación.

A largo plazo los esfuerzos están encaminados al uso de sistemas de autenticación fuerte, como la basada en sistemas de doble factor: el uso de tokens electrónicos, certificados digitales de usuario o tarjetas inteligentes. En este sentido algunas entidades bancarias ya emplean además del usuario y contraseña clásica, tarjetas que tienen impresas claves que permiten la autenticación basada en reto y respuesta. También se están planteando sistemas que requieran el uso de canales de autenticación separados, como el teléfono móvil. En el futuro se espera que si se extiende el uso de lectores de tarjetas inteligentes pueda usarse alguno de los proyectos en fase de diseño o implantación como el DNI digital o las tarjetas de crédito EMV.

7.- Cómo aportar seguridad al Comercio Electrónico.

Existen tres factores que integran a la seguridad del comercio electrónico, los tecnológicos, los legales y los culturales.

Los tecnológicos son todos aquellos medios (protocolos, soluciones, etc.) utilizados para asegurar las transacciones económicas.

Los legales, son la obligación de cumplir con las leyes vigentes en materia de comercio electrónico (LSSI) y manejo de datos personales (LOPD). Ambos temas se tratan específicamente en otros capítulos de este manual.

Los culturales, son los derivados de los usuarios y de su percepción de la seguridad en el comercio electrónico. Aunque los factores anteriores se cumplan, los clientes y usuarios harán uso de estos servicios sólo si están convencidos de que su información, como números de tarjeta de crédito, datos personales, financieros, etc. están seguros.

En el mundo real, la seguridad se basa en la confianza por la presencia física. Los usuarios aceptan los riesgos del uso de tarjetas de crédito porque pueden ver y tocar la mercancía que están adquiriendo, ver físicamente el establecimiento y al vendedor y en base a ello realizar un juicio de la confianza que le ofrece.

Así mismo, la posesión del medio de pago (tarjeta de crédito, metálico) da una mayor sensación de control sobre el acceso y seguridad del dinero. En Internet sin esa presencia física, es mucho más difícil generar confianza en el usuario.

La ausencia de este referente físico es la que ocasiona dos de los principales riesgos a los que se expone el comercio electrónico en Internet:

Falsificación. La baja dificultad de creación de sitios web y la facilidad de copiar sitios web existentes hacen extremadamente sencillo crear un comercio electrónico falso con apariencia de un establecimiento reconocido.

Interceptación. Cuando la información viaja a través protocolos que no incluyen encriptación puede ser fácilmente interceptada con el fin de obtener los datos financieros.

8.- Principales soluciones:

Nadie esperaba que Internet, o más concretamente, la World Wide Web, creciera al ritmo exponencial de los últimos años. Sus posibilidades para el comercio fueron rápidamente vislumbradas y en un tiempo récord pasó a transformarse en teatro de transacciones comerciales, financieras y de todo tipo. Había que vender, pero vender ya. No podía esperarse a magníficos estándares que velaran por la rigurosa implantación de todos los detalles. ¿Qué método resulta más cómodo e inmediato para pagar? La tarjeta de crédito. ¿Al usuario le preocupa la seguridad? Usemos un canal seguro para transmitir el número de la tarjeta. Fue así como en poco tiempo se impuso como norma tácitamente acordada el emplear el protocolo SSL para cifrar el envío de datos personales, entre ellos el número de tarjeta.

Esta es la solución más extendida y actualmente considerada como imprescindible en el comercio electrónico. Este protocolo provee encriptación a otros protocolos de red. Su aplicación más típica suele ser encriptar el tráfico web o http seguro. Es ampliamente empleado para proteger la información confidencial y especialmente los datos financieros en sitios de comercio electrónico, banca por Internet, webmail, etc.

Este protocolo incorpora características tanto de confidencialidad (protege la información que viaja por la red) como de autenticación (permite comprobar el certificado digital que nos asegura que quien recibe la información es quien dice ser).

SSL (Secure Sockets Layer) es un protocolo de propósito general para establecer comunicaciones seguras, propuesto en 1994 por Netscape Communications Corporation junto con su primera versión del Navigator. Hoy constituye la solución de seguridad implantada en la mayoría de los servidores web que ofrecen servicios de comercio electrónico. Para pagar, el usuario debe rellenar un formulario con sus datos personales (tanto para el caso del envío de los bienes comprados, como para comprobar la veracidad de la información de pago), y los datos correspondientes a su tarjeta de crédito (número, fecha de caducidad, titular). Esta arquitectura no exige que el servidor disponga de capacidades especiales para el comercio. Basta con que se utilice como mínimo un canal seguro para transmitir la información de pago y el comerciante ya se ocupará manualmente de gestionar con su banco las compras. El canal seguro lo proporciona SSL. Sin embargo, este enfoque, aunque práctico y fácil de implantar, no ofrece una solución comercialmente integrada ni totalmente segura (al menos en España, debido a que los navegadores utilizan 40 bits de longitud de clave, protección muy fácil de romper). SSL deja de lado demasiados aspectos para considerarse la solución definitiva:

- Sólo protege transacciones entre dos puntos (el servidor web comercial y el navegador del comprador). Sin embargo, una operación de pago con tarjeta de crédito involucra como mínimo tres partes: el consumidor, el comerciante y el emisor de tarjetas.

- No protege al comprador del riesgo de que un comerciante deshonesto utilice ilícitamente su tarjeta.
- Los comerciantes corren el riesgo de que el número de tarjeta de un cliente sea fraudulento o que ésta no haya sido aprobada.

Son demasiados problemas e incertidumbres como para dejar las cosas como están. Se hacía necesaria la existencia de un protocolo específico para el pago, que superase todos los inconvenientes y limitaciones anteriores, motivo por el que se creó SET.

El estándar SET (Secure Electronic Transaction) fue desarrollado en 1995 por Visa y MasterCard, con la colaboración de gigantes de la industria del software, como Microsoft, IBM y Netscape. La gran ventaja de este protocolo es que ofrece autenticación de todas las partes implicadas (el cliente, el comerciante y los bancos, emisor y adquiriente); confidencialidad e integridad, gracias a técnicas criptográficas robustas, que impiden que el comerciante acceda a la información de pago (eliminando así su potencial de fraude) y que el banco acceda a la información de los pedidos (previniendo que confeccione perfiles de compra); y sobre todo gestión del pago, ya que SET gestiona tareas asociadas a la actividad comercial de gran importancia, como registro del titular y del comerciante, autorizaciones y liquidaciones de pagos, anulaciones, etc.

Entonces, si todo son alabanzas, ventajas y puntos fuertes, ¿por qué SET no ha terminado por implantarse? ¿Por qué no goza de la popularidad de SSL, si se supone mejor adaptado? En primer lugar, su despliegue está siendo muy lento. Exige software especial, tanto para el comprador (aplicación de monedero electrónico) como para el comerciante (aplicación POST o terminal de punto de venta), que se está desarrollando con lentitud. En segundo lugar, aunque varios productos cumplan con el estándar SET, esto no significa necesariamente que sean compatibles. Este es un problema que exige mayores esfuerzos de coordinación y más pruebas a escala mundial para asegurar la interoperabilidad. Sus puntos fuertes son también su talón de Aquiles: la autenticación de todas las partes exige rígidas jerarquías de certificación, ya que tanto los clientes como comerciantes deben adquirir certificados distintos para cada tipo de tarjeta de crédito, trámites que resultan tremendamente complicados, para la mayoría de los usuarios.

En definitiva,. SSL no es tan perfecto, no ofrece la seguridad ni las garantías de SET, pero funciona. Y lo que es más, el usuario de a pie no tiene que hacer nada.

9.- Medios de Pago Seguros

El principal medio de pago en el comercio electrónico en la actualidad es la tarjeta de crédito. Esto es así a pesar de ser uno de los medios menos idóneos, ya que para realizar una transacción basta únicamente con conocer el número de tarjeta de crédito, fecha de caducidad y nombre del titular.

Para intentar solventar estos problemas de seguridad que se traducen en grandes índices de fraude, se están intentando aplicar diversas soluciones. Algunas de ellas son especificas para el comercio online, como puede ser el sistema CCV2. Otras en cambio son de ámbito más general para solventar los presentes fallos de seguridad en todo el sistema de tarjetas de pago como son el Estándar EMV para tarjetas de crédito y el CEPS para monedero electrónico.

Dado que un proyecto de comercio electrónico puede abarcar distintos grados de aplicación de los sistemas de pago seguros, Sistemas de TPV virtual para las PYMES, implantación de tarjetas inteligentes que incorporen sistemas de pago, uso generalizado de tarjeta inteligente, etc. se deberá de realizar un estudio especifico de los sistemas a implementar dependiendo de los servicios que se quieran prestar.

A continuación veremos cuales son los principales medios de pago que han surgido para reemplazar o asegurar los sistemas clásicos de pago por tarjeta de crédito.

Los sistemas de protección de tarjetas de crédito online se añaden a las tarjetas medios adicionales de autentificación, por ejemplo un código PIN específico para las transacciones por Internet u otros medios para que el titular de la tarjeta pueda autorizar el cargo, como hace el programa “Verified by VISA” que añade un PIN exclusivo para la compra a través de Internet.

Una aproximación diferente es el sistema CCV2. Este sistema requiere que adicionalmente a la tarjeta de crédito se facilite el código CCV2 de tres dígitos que viene impreso en el reverso de la tarjeta, de forma que solo el propietario de la tarjeta puede facilitar ese código, ya que este código solo se encuentra impreso en la tarjeta, y en las bases de datos del emisor de la tarjeta, y en teoría no debería de almacenarse en ningún otro lugar, de forma que no puede ser sustraído por delincuentes por medio de lectores de tarjeta de banda magnética o por acceder a la base de datos un comerciante.

Otras cuestiones a tener en cuenta a la hora de cobro con tarjeta es la futura implantación del estándar EMV y el estándar CEPS de monedero.

Las especificaciones EMV permitirán la progresiva sustitución de la banda magnética por el chip en transacciones financieras de débito y crédito. Las especificaciones CEPS permitirán la adaptación de los actuales esquemas domésticos de monedero electrónico al estándar internacional Ambas especificaciones (EMV y CEPS), se centran básicamente en la vertiente tecnológica, son abiertas, y requieren un desarrollo específico de las mismas por cada marca internacional (Visa, Europay).

Paralelamente cada marca establece en su entorno las Reglas Operativas entre Entidades adquirentes y emisoras dependiendo del producto que se trate.

La importancia de estudiar la aplicación del estándar EMV en el ámbito de las ciudades digitales viene dada por que a partir de enero de 2005 en caso de fraude, habrá un cambio de responsabilidad del emisor y adquirente hacia aquellos que no estén bajo EMV, es decir la responsabilidad pasara a quien no halla sido capaz de implantar el estándar EMV.

El cumplimiento del EMV también deberá considerarse si se planea desplegar algún tipo de terminales, tpv , kioskos, etc que presten servicios de cara al usuario que permitan el pago por tarjeta, ya que existen también requerimientos de cumplimiento obligatorio, por ejemplo para aquellos sistemas que acepten Visa Electrón deben disponer de lector chip EMV y de Pin-Pad seguro.

El estándar CEPS por su parte puede convivir en una tarjeta inteligente multiaplicación con el EMV o existir de forma independiente, su aplicación es siempre recomendable para la realización de micro pagos (Tonos móviles, contenidos de pago en publicaciones electrónicas, etc.) en lugar de soluciones de monedero electrónico cerrado, que son mucho más cuestionables desde el punto de vista de la seguridad.

10.- Últimas Actuaciones:

Finread: En septiembre de 2004 el consorcio Finread -constituido por Banksys (sistema de tarjetas de Bélgica), Europay International, Ingenico, Interpay (sistema de tarjetas holandés), SIZ (informática de las cajas de ahorro alemanas), Visa y Groupement de Cartes Banciares (sistema de tarjetas francés)?, con el respaldo de la Comisión Europea, ya se ha puesto de acuerdo sobre las especificaciones que pueden securizar las transacciones electrónicas a través de tarjetas. Este Financial Transactional IC Crad Reader, cuyas especificaciones acaban de ser reconocidas por el Comité Europeo de Normalización (CEN), es un lector de tarjetas con chip que abre la vía a la securización de un amplio abanico de aplicaciones: operaciones financieras, pagos destinados al comercio electrónico, salud, autentificación o cualquier otro dominio de aplicación que necesite un nivel de seguridad

importante. Los promotores de estas especificaciones técnicas del lector de tarjetas afirman que “este acontecimiento es importante en la historia de Internet, puesto que estas especificaciones se impondrán rápidamente como el estándar de facto**.**

En España está prevista para finales del año 2005 la introducción del DNI digital que puede ser un factor que ayude a aumentar la seguridad en las transacciones electrónicas y por tanto aumente la confianza de los usuarios del comercio electrónico.

11. Recomendaciones

Antes de lanzarnos al uso de esta herramienta comercial, es siempre recomendable la realización de un estudio que tenga por objetivo la Prevención del Fraude en el Comercio Electrónico. Se trata de un análisis de vulnerabilidades ante el fraude en sistemas de comercio electrónico, especialmente en venta de productos y servicios en Internet, incluidas las realizadas a través de telefonía móvil, así como en sistemas de pago y monederos electrónicos basados en tarjetas inteligentes, tarjetas contactless, etc.

Adicionalmente pueden implantarse sistemas que permitan reconocer patrones de actividades fraudulentas (la responsabilidad del coste de operaciones fraudulentas con tarjetas de crédito en Internet suele recaer sobre el comerciante).

Por lo que se refiere al protocolo SSL, su uso se debe complementar siempre con un nivel adecuado de seguridad en todos aquellos sistemas TI que manejen información financiera. SSL sólo protege el vínculo que se establece entre comprador y comercio electrónico en el momento de la compra, pero posteriormente han de ser otras medidas las que aseguren que la información financiera esta protegida durante su proceso, transmisión y almacenamiento.

- **CAPITULO 8: SEGURIDAD EN EL CORREO ELECTRONICO**

1. Introducción: Breve historia y primeros problemas

Hoy en día consideramos el correo electrónico un elemento prácticamente imprescindible de nuestra comunicación, ya sea personal o profesional e independiente del sector en el que desarrollamos nuestra actividad y tenemos la sensación de que siempre ha sido así.

Sin embargo, no hace tanto tiempo, en la década de los 80 el correo electrónico era conocido y utilizado únicamente por unos pocos miles de privilegiados que tenían acceso a redes universitarias internacionales que experimentaban con nuevas tecnologías.

A principios de la década de los 90 vimos como el correo electrónico pasó a ser una herramienta de comunicación que las grandes empresas multinacionales ponían a disposición de sus ejecutivos y directores a costes muy elevados; a mediados de esta década vimos como aparecían los primeros proveedores que vendían los primeros servicios de correo electrónico y que hacían posible que las grandes empresas pudieran extender este servicio a casi todos sus empleados y las PYMES mas innovadoras empezaran a adoptar este nuevo sistema de comunicación.

A finales de la década de los 90 con la explosión que supuso Internet, las empresas *.com* y la generalización de las cuentas gratuitas de correo electrónico hicieron que este nuevo método de comunicación de hiciera prácticamente universal y pasara a ser una herramienta de comunicación imprescindible para las empresas y que ya en el año 2.000 superó en numero de comunicaciones diarias al correo tradicional y redujo el uso del Fax a una forma de envío de información casi obsoleta.

Hasta aquí todo parece un cuento de hadas donde el avance de la tecnología en el breve plazo de una década nos ha dado con el correo electrónico una herramienta de comunicación casi instantánea, con un coste muy bajo o incluso gratuito que nos permite comunicarnos con cualquier persona o empresa en cualquier sitio del planeta, pero.....

Problemas que teníamos antes se empiezan a manifestar en esta nueva forma de comunicarnos que es el correo electrónico, los virus que nos llegaban en disquetes empiezan a llegar por correo electrónico, los faxes no solicitados con diversas ofertas se empiezan a reemplazar por correos electrónicos no solicitados inicio de un de los problemas mas graves en la actualidad, el SPAM.

Pero también aparecen problemas que no teníamos antes, llegada de correos electrónicos con contenidos ofensivos, facilidad con la que información entre y sale de nuestra organización, incremento exponencial en el número de correos que afectan nuestra productividad, hackers que capturan nuestro servidor de correo para enviar correos SPAM.

2- Problemas de Seguridad en el Correo Electrónico.

2.1.- Virus y Códigos Malignos

El principal problema de seguridad que ha tenido y sigue teniendo la tecnología del correo electrónico son los virus y otros códigos malignos, que han ido evolucionando en paralelo con el desarrollo y popularización del correo electrónico.

Vamos ha hacer una clasificación simple de este problema siguiendo un criterio de evolución empezando con lo que denominaremos virus clásicos que existían pasando por la explosión de los virus de macro que se apoyaron en el gran incremento de envío por correo electrónico de archivos con datos en formatos Word, Excel para terminar con lo que denominaremos virus de vulnerabilidades que apoyándose ,

2.1.1.- Virus Clásicos y su evolución

El problema de los virus es anterior a la popularización del uso del correo electrónico y que se agudizó con un nuevo medio de transmisión vírica que multiplico el numero de infecciones.

El virus clásico previo al correo electrónico se transmitía de un ordenador a otro realizando una copia de si mismo en los disquetes que en aquel entonces se usaban como el medio para enviar información en formato digital, y utilizaba fundamentalmente dos métodos para reproducirse , el primero que el usuario ejecutara el virus desde el disquete y el segundo copiándose en el sector de arranque del ordenador y por tanto ejecutándose cada vez que se encendía el ordenador y a partir de ese momento todo disquete que era introducido en el ordenador quedaba infectado. Dos métodos seguros pero bastante contenidos.

La mutación evolutiva que realizó el virus que utilizaba el disquete como medio para transmitirse de un ordenador a otro fue el desarrollo de la habilidad la de realizar una copia de si mismo, guardarla en el ordenador infectado y utilizando los programas de correo electrónico enviar un copia de si mismo mediante un correo electrónico a las direcciones de correo existentes en la lista de contactos.

Una segunda mutación fue la de incluir dentro de la actividad del virus un motor de correo electrónico que envía los correos electrónico con la copia del virus sin necesidad de utilizar el sistema de correo del ordenador, simplemente su conexión a Internet y utilizando todas las direcciones de correo que pueda encontrar en el ordenador infectado.

Todo esto, con ser un salto cualitativo en el problema de las infecciones por virus informáticos tenia una limitación fundamental y era que requería que el usuario ejecutara el virus, aunque para llevarle al engaño los virus han venido utilizando diversas tretas que se han venido a llamar ingeniería social .

Podemos decir que con la mutación de los virus clásicos para ser capaces de distribuirse utilizando el propio correo electrónico el numero de infecciones por virus informáticos se multiplico como mínimo por un factor de diez.

2.1.1.- Virus de Macro

La aparición del los virus de macro trajo consigo un nuevo incremento en los problemas de virus en el correo electrónico.

El virus de macro se aprovecha de las facilidades que se incluyeron especialmente en los procesadores de texto como Word u hojas de calculo como Excel, cuyos lenguajes de programación macro permiten acceder a diversos recursos del ordenador que se está utilizando.

Los virus de macro ya nacieron con el concepto de transmitirse únicamente a través del correo electrónico , es decir realizaban copias de si mismo o infectaban plantillas con lo cual todo documento u hoja de cálculo creado a partir de la infección tenia el virus incluido y utilizaban o bien el sistema de correo electrónico presente en el ordenador infectado o bien uno propio.

Cuando aparecieron los primeros virus de Macro, los usuarios que habían aprendido a no ejecutar programas que les llegaban por correo electrónico se encontraron con un nuevo sistema que les engañaba e infectaba sus ordenadores.

Se juntaron dos circunstancias, primero que el uso del correo electrónico se incrementaba exponencialmente día a día y segundo la transmisión de ficheros Word y Excel eran el medio mas habitual de transmisión de información en formato digital, esto produjo que ocurrieran dos de las epidemias de virus con mayor impacto económico en el triste ranking de los virus que han producido el mayor daño económico.

Este tipo de virus requiere también la ayuda de los usuarios para su propagación, ya que por el simple hecho de abrir un documento de Word o Excel se activa el virus y se puede iniciar una epidemia.

Durante unos años , además de los virus clásicos esta fue la mayor amenaza a la seguridad en el correo electrónico, pero aun nos quedaba por ver otros cambios , evoluciones y mutaciones en las amenazas de los virus informáticos

2.1.1.- Virus de Vulnerabilidad

La última hola de virus que estamos padeciendo es la de aquellos que aprovechan las vulnerabilidades de sistemas operativos, gestores de correos e incluso aplicaciones de uso general como pueden ser las bases de datos y que desde 2001 con los virus Code Red y Nimda cambió los paradigmas que existían respecto a la protección antivirus.

Los primeros virus que aprovechaban vulnerabilidades aparecieron en el entorno de los gestores de correo electrónico y más específicamente en los productos de Microsoft Outlook y Outlook Express por ser los productos más utilizados en el entorno empresarial y el entorno de pequeñas Pymes, profesionales autónomos y usuarios domésticos respectivamente.

La técnica que utilizaban los primeros virus de vulnerabilidad era la denominada " Buffer Overflow" que en esencia no es mas que enviar mayor información que la que puede procesar un programa y por tanto generar un error que permite tomar control del programa o simplemente conseguir ejecutar unas instrucciones que se aprovecharán para iniciar el virus.

Pero, en que se traduce esta innovación que se produjo en los virus que llegaban a nuestros gestores de correo electrónico?

Esta innovación produce un cambio esencial, ya no es necesaria la intervención del usuario final para que el virus realice su infección y se propague a otros sistemas, simplemente por el hecho de no tener nuestro gestor de correos debidamente actualizado y con los parches de seguridad incluidos, la llegada de uno de estos virus por correo electrónico puede infectarnos y usar nuestro ordenador como un elemento de propagación del virus.

En la actualidad los virus de vulnerabilidad han evolucionado aún mas y se han liberado de la necesidad de utilizar el correo electrónico como el medio para transmitirse y propagarse, han aparecido los virus de red, denominados también Gusanos de Red, que utilizan vulnerabilidades en otros programas diferentes del correo electrónico y se transmiten utilizando las infraestructuras de red y la interconexión de equipos a través de Internet.

Pero el tema de los Gusanos de Red trasciende de la seguridad en el correo electrónico y podría ser objeto de un capitulo aparte en la seguridad de los sistemas informáticos..

2.2.- SPAM

Este problema, que proviene de otro mas antiguo , el faxing, que nos llenaba el fax de ofertas no solicitadas y nos hacia gastar un buen numero de las antiguas pesetas en papel de fax, inicialmente fue tomado casi a broma y con las cadenas de correos electrónicos para las más diversas peticiones u solicitudes vimos como se empezaba a incrementar el número de correos electrónicos que debíamos atender, sin por ello incrementar nuestro trabajo efectivo.

Casi con la misma rapidez que se incrementaba el número de buzones de correo, tanto de uso empresarial como de uso domestico, se incrementaba el número de CORREOS BASURA, otro nombre del SPAM, legando a ser uno de los mayores problemas del correo electrónico hasta el punto que los catastrofistas llegaran a augurar que el correo electrónico se hará inutilizable para finales del 2004.

Cierto es que le problema del SPAM es grave, en algunas empresas la proporción de correo basura frente al correo útil es casi de un 50% y esto está cercano a las predicciones catastrofistas.

El SPAM vive de el número de direcciones de correo electrónico diferentes a las que pueda enviar su mensaje, ya que detrás del CORREO Basura se esconde una floreciente industria de venta por Internet y que se basa en criterios estadísticos para realizar su negocio.

Para conseguir direcciones de correo, los SPAMERS utilizaban técnicas de búsqueda en WEBs, envió de millones de correos a direcciones aleatorias pero razonables con la esperanza de obtener respuesta y así confirmar que esa dirección era valida. Pronto los usuarios del correo electrónico aprendimos que nunca se debe responder , ni siquiera por enfado a un correo basura, pues entonces entraremos en la lista de correos validos y nuestro nivel de SPAM crecerá exponencialmente.

Si solamente un 0,001% de aquellos que reciben SPAM al final del proceso realizan una compra o cualquier otra cosa a la que les incite el correo basura, entonces para conseguir efectividad, se tiene que enviar al menos 100 millones de SPAM para conseguir 1.000 compradores.

Esto hizo que apareciera un nuevo método de conseguir direcciones de correo para incrementar el número de correos basura que enviar y tener una mejor rentabilidad a este proceso de dudosa legalidad; aparecieron virus de correo electrónico que además de

reenviarse a todas las direcciones de correo que encontraban en el ordenador infectado, enviaban todas esas direcciones a sitios específicos en Internet donde quedaban a disposición de los SPAMERS.

En la actualidad se encuentran el Internet bases de datos con centenares de millones de direcciones de correo electrónico que cubren todos los países del mundo, aunque esto legislado y prohibido en España por la LOPD, indudablemente seguimos expuestos al SPAM que proviene de allende nuestras fronteras, que por cierto en Internet son más bien inexistentes.

2.3.- Otras Amenazas en el correo electrónico

Han aparecido otras variedades de amenazas en el uso del correo electrónico , como son los contenidos racistas, sexuales , sectarios que no solamente nos desagraden por sus expresiones o imágenes, sino que además son ilegales y si fuera posible determinar su fuente podrían estar sujetos a sanciones.

Otras amenazas que viene por el correo electrónico aunque afectan más bien a la navegación por Internet son el “Spyware” , código maligno que espía nuestras actividades con el ordenador y envía nuestros datos de números de tarjeta de crédito, passwords y otras informaciones sensibles a sitios donde pueden ser utilizados fraudulentamente o el “Adware” código maligno que se dedica a abrir paginas de publicidad mientras navegamos legando a entorpecer la navegación de tal manera que puede llegar a bloquear nuestro ordenador.

Pero tal vez de las nuevas amenazas la más reciente y la más dañina es el denominad “Phishing”, que es la utilización del correo electrónico para conseguir nuestras nombres de usuario y claves para acceder a servicios como la banca electrónica y directamente realizar actividades delictivas de robo en cuentas bancarias.

Como vemos las nuevas amenazas que van apareciendo en el correo electrónico han pasado de ser un problema de operación segura de nuestros sistemas informáticos a amenazas cuyos hechos delictivos pueden tener efectos devastadores para nuestras empresas o cuentas corrientes personales.

3- Modelos de uso del Correo Electrónico

Hay muchos métodos y sistemas para clasificar la forma de utilización del correo electrónico, me voy a permitir usar el criterio de tipo de gestión para simplificar luego las medidas que se deben tomar para reducir los riesgos e incrementar la seguridad en el uso del correo electrónico.

En los inicios de la tecnología del correo electrónico la única manera de disponer de un buzón de correo era a través de unas empresas proveedoras de este servicio, ya no existe ninguna de ellas, que se dedicaban únicamente a prestar servicios de correo electrónico, disponían de un sistema centralizado al que se conectaban sus usuarios, empresariales y domésticos por igual, para acceder a sus buzones de correo y poder así leer los mensajes que habían recibido y contestar dichos mensajes.

La generalización de Internet trajo consigo la aparición de los ISP, Internet Service Provider o en Español Proveedores de Servicios de Internet , que rápidamente coparon el mercado de los proveedores de correo electrónico, forzándoles a convertirse en ISP o desaparecer del mercado.

La aparición del Proveedor de Servicios de Internet abrió las posibilidades de uso del correo electrónico a varios otros sistemas como por ejemplo el permitir que el servidor de correos estuviera en el centro de proceso de datos de la empresa, este modelo fue rápidamente adoptado por las empresas mas grandes y que disponían de infraestructura y medios para alojar y gestionar sus servidores de correo.

Otro modelo que apareció fue el tener servidores de correo electrónico propios , pero por razones de ancho de banda, los equipos estaban físicamente en las instalaciones del ISP.

Además para las empresas mas pequeñas se ofrecía la posibilidad de usar servidores de correo electrónico compartidos , de tal manera que un mismo equipo físico era capaz de gestionar el correo de varia empresas a la vez, dando la sensación de que cada una de ellas disponía de su propio servidor de correo electrónico.

Y finalmente, por supuesto que estaban disponibles los buzones de correo genéricos y que por un módico precio podían utilizarse incluso por usuarios domésticos que empezaban a interesarse por el fenómeno de Internet.

3.1.- Correo Electrónico Gestionado Internamente

Una vez que el correo electrónico se convirtió en la principal herramienta de comunicación de las empresas, uno de los modelos de gestión del correo electrónico fue el de instalar servidores de correo electrónico en los centros de proceso de datos de las empresas.

Este modelo de gestión inicialmente se generalizó entre las grandes empresas que terminaron dando un buzón de correo a todos y cada uno de sus empleados y por tanto necesitando de grandes servidores de correo y al disponer de mayores recursos pudieron

dedicarlos a mantener y gestionar estos sistemas. Los servidores de correo pasaron así a formar parte de las redes y sistemas informáticos de las grandes empresas.

Los gestores de Correo Electrónico más utilizados son y han sido desde un principio Microsoft Exchange y Louts Notes, que coparon entre ambos más de un 80 por ciento del mercado y aunque también aparecieron sistemas basados en Linux, su utilización , aunque en crecimiento actualmente aún no son mayoritarios.

Pero este modelo de gestión no solamente fue adoptado por las grandes empresas, también fue y sigue siendo utilizado por muchas pequeñas y medianas empresas, puesto que Microsoft añadió a sus sistemas operativos de red para PYMES versiones simplificadas del Microsoft Exchange que hicieron que muchas empresas decidieran tener el correo electrónico dentro de sus propias oficinas.

El modelo de correo electrónico gestionado internamente tiene como ventaja fundamental la cercanía de la gestión que lo hace más flexible, sin embargo desde el punto de vista de la seguridad esta gestión se hace mas complicada y consume muchos más recursos.

Sin embargo, en este modelo además de los recursos necesarios para mantener en buen estado de funcionamiento el correo electrónico, las organizaciones que adoptaron este sistema se encontraron con que además tiene que dedicar tiempo y dinero para reducir los riesgos de sufrir amenazas que llegan a través del corroe electrónico y que pueden afectar a todo sus sistemas informáticos.

3.2.- Correo Electrónico Externalizado

Otro modelo que apareció desde un principio fue el de tener el servicio de correo electrónico externalizado, de hecho fue el primer modelo que fue capaz de prestar un servicio útil y que ayudó y fue fundamental para el rapidísimo desarrollo de esta tecnología.

Realmente, aunque todos empezamos con el modelo de correo electrónico externalizado, esto ha cambiado de tal manera y ha evolucionado a soluciones mucho más flexibles y con unos niveles de servicio francamente inmejorables.

Para simplificar, vamos a clasificar el correo electrónico externalizado en tres, hosting privado, hosting compartido y plataformas abiertas.

3.2.1.- Hosting Privado

El hosting privado del correo electrónico es un servicio mediante el cual los servidores de correo están físicamente en las instalaciones del proveedor de servicios y que están separados dentro de la red de otros equipos tanto del proveedor de servicios como del resto de los clientes.

La gestión de estos equipos puede ser realizada por el propio cliente de forma remota o por el proveedor de servicios, incluso en la actualidad se produce una gestión compartida realizada por el propio cliente en horas de oficina y por el proveedor de servicios en el resto del tiempo hasta lograr un servicio 24X7.

3.2.2.- Hosting Compartido

El hosting compartido surgió de aprovechar las ventajas que conseguían con el hosting privado para empresas más pequeñas que tenían necesidades menores pero que requerían un alto nivel de servicio.

La mejora continuada de los productos de Software de Gestión de correo electrónico a lo largo de esto años ha permitido que un mismo sistema sea capaz de mantener y gestionar de manera eficaz el correo electrónico de varios clientes a la vez y de tal manera que todos ellos tengan la percepción de ser los únicos usuarios del sistema.

Con este sistema se consigue mejorar el rendimiento y por ende reducir el coste de los servicios haciendo posible que empresas más pequeñas puedan utilizar un servicio similar al que reciben clientas más grandes y con un alto nivel de servicios que puede llegar al 24X7 y muy importante con unos costes razonables

3.2.1.- Plataformas Abiertas

En los últimos tiempos hemos visto como el hosting compartido ha evolucionado hacia lo que podemos denominar plataformas abiertas de correo electrónico, capaces de albergar millones de buzones y de dar servicio a un gran número de empresas con la percepción que estar utilizando un sistema dedicado a cada una de las empresas usuarios.

Con estos sistemas se ha conseguido finalmente que el correo electrónico haya pasado a ser el medio de comunicación más importante de la PYMES, al poder contratar servicios a precios razonables y con un nivel de calidad excelente.

Como una extensión de estas plataformas abiertas aparecen los servicios de correo electrónico gratuito, del cual se benefician especialmente los usuarios individuales pero también las empresas más pequeñas que consiguen tener acceso al gran medio de comunicación mundial prácticamente sin coste.

Así pues con esto hemos llegado a una situación en la que prácticamente allí donde hay un mínimo de infraestructura de telecomunicaciones se puede tener acceso al correo electrónico y por ende a la posibilidad de comunicarse globalmente.

4- Medidas de prevención de amenazas en el Correo Electrónico

Este capitulo trata de la seguridad en el correo electrónico y hasta ahora solamente hemos planteado las amenazas que existen y que han surgido desde los primeros días del correo electrónico así como de los modelos de funcionamiento y gestión.

Llega el momento de ver que medidas tenemos que tomar para la prevención de amenazas en el correo electrónico y para ello vamos a dividir este capitulo en dos grandes grupos, prevención de amenazas utilizando la tecnología y prevención de amenazas por la educación de los usuarios que denominaremos medidas de higiene tecnológica.

Ciertamente todo avance en el uso de las nuevas tecnologías trae consigo nuevos problemas que hace que los usuarios tengan que aprender nuevas formas de reaccionar a problemas que no conocían en el pasado.

Lamentablemente en el desarrollo del correo electrónico han primado criterios de facilidad de uso sobre criterios de seguridad y por tanto la propia tecnología tiene vulnerabilidades y fallos que hacen que la colaboración de los usuarios para la reducción de riegos sea absolutamente necesaria.

Por supuesto también se ha desarrollado nuevas tecnologías de seguridad informática que han permitido mantener el riesgo a niveles razonablemente bajos como para que el Correo Electrónico pudiera llegar a ser la herramienta de comunicación más extendida en el mundo.

4.1.- Medidas de Prevención usando la tecnología

Según ha ido avanzando la tecnología del Correo Electrónico han ido apareciendo tecnologías de protección que aseguran un buen funcionamiento de nuestros sistemas , inicialmente todas las medidas de seguridad se basaban en aplicaciones de seguridad en el puesto de trabajo, puesto que era en el PC donde se recibía el correo electrónico y por tanto era donde teníamos que establecer la medidas y aplicaciones de seguridad.

Al evolucionar el correo electrónico, como vimos en la parte inicial de este capítulo, con la llegada de los programas de Gestión de Correo Electrónico, fundamentalmente Microsoft Exchange y Lotus Notes, aparecieron aplicaciones de seguridad que se integraban con el Gestor de Correos para dar un nuevo nivel de protección al correo electrónico de los usuarios.

Finalmente al crecer las redes y su interconexión a través de Internet aparecieron nuevas aplicaciones de seguridad que eran capaces de proteger el correo electrónico aun antes de llegar a los gestores de correo electrónico y esto es lo que se denomina en la actualidad seguridad perimetral.

Así pues, vamos a ver los tres niveles de protección que debemos aplicar a nuestros sistemas de Correo Electrónico independientemente del sistema de gestión, interna o externalizada, que hayamos elegido.

4.1.1.- Prevención en el Puesto de Trabajo

La primera medida de seguridad que tuvo el usuario en el puesto de trabajo para proteger sus correos electrónicos fue el tradicional antivirus que era útil con ficheros infectados que cuando intentaban ser copiados al disco duro eran detectados y eliminados.

De hecho esta medida de seguridad es previa incluso a la llegada del correo electrónico, pero que fue muy útil para detectar los primeros virus o códigos malignos clásicos que llegaban en archivos adjuntos y aunque solo infectaban el equipo que los recibía y no eran aun capaces de replicarse y distribuirse usando el correo electrónico si que eran fastidiosos y dañinos.

La primera medida de seguridad especifica para el correo electrónico en los puestos de trabajo fue la extensión del antivirus para los clientes de correo Microsoft Outlook y Microsoft Outlook Express, que ya era capaz de detectar los virus y otros códigos malignos en los correos electrónicos y enviarlos a carpetas de cuarentena o eliminarlos directamente.

La llegada de esta medida de seguridad coincidió con la proliferación de los denominados virus de Macro y fue una solución de gran utilidad que con el tiempo llegó a controlar este problema especifico de los virus de Macro.

Otro problema que gradualmente se fue haciendo más agudo fue el del SPAM y para hacerle frente se añadió al Antivirus de puesto de trabajo módulos capaces de detectar correo no solicitado y redirigirlo a carpetas donde una vez puestos en cuarentena podían ser eliminados con seguridad.

Esta estrategia , aunque útil, tiene el inconveniente de que el SPAM o correo basura llega al usuario final y puede por tanto entorpecer su trabajo de tal manera que en algún caso se ha llegado a decir que el SPAM representaría el final del uso practico del correo electrónico.

Además, aparecieron los virus que se aprovechaban de las vulnerabilidades en los clientes de correo Microsoft Outlook y Microsoft Outlook Express, que obligaron a un cambio de estrategia en los antivirus para puesto.

La búsqueda, escaneo en términos más técnicos, de los virus en los puestos de trabajo se hacia una vez que el virus había sido copiado a disco duro para allí ser ejecutado por el usuario. Con esta nueva generación de virus se tenia que buscar el virus en memoria, antes aun de ser copiado a disco para su visualización o utilización por el usuario.

Este método de trabajo era necesario puesto que si el virus llegaba a nuestro programa cliente de correo electrónico, se aprovechaba de la vulnerabilidad y sin intervención del usuario podía iniciar una infección masiva o epidemia de virus informático.

Otra medida de seguridad se hacia necesaria, era la revisión sistemática de todos los puestos de trabajo y el parcheo de todas las vulnerabilidades conocidas.

Las medidas de protección en el puesto de trabajo, muy útiles, no son suficientes y pronto fueron complementadas con otras medidas en el siguiente escalón de nuestros sistemas de correo electrónico que no es otro que el de los programas gestores de correo electrónico.

4.1.2.- Prevención en el Gestor de Correo Electrónico

Aunque en el puesto de trabajo se desarrollaron muchas medidas de seguridad que permitieron seguir usando el correo electrónico de una manera cada vez más masiva, algunos de estos problemas serán resueltos de mejor manera con herramientas de seguridad que se integran con los gestores de correo electrónico.

La solución al problema de los virus y otros códigos maligno se puede tratar en este nivel antes de que llegue al usuario final, liberando de esta manera recursos de los puestos de trabajo y usuarios finales.

Parece muy sensato utilizar una estrategia centralizada en la detección y eliminación de virus, puesto que el propio sistema de correo electrónico se centraliza con el uso de grandes servidores de correo electrónico.

Además de la búsqueda de virus en los correos electrónicos que se gestionan desde servidores centralizados de coreo electrónico , utilizando la misma tecnología se puede realizar lo que se denomina como control y gestión de contenidos.

El control de contenidos permite eliminar o enviar a carpetas de cuarentena correos electrónicos inadecuados que puedan llegar como pueden ser correos con contenidos sexuales, xenófobos, etc.

Pero además de esta funcionalidad de evitar la llegada de correos electrónicos con contenidos ofensivos, el control de contenidos nos permite que datos sensibles de nuestra organización puedan salir sin la debida autorización a través de nuestro corroe electrónico.

Un ejemplo pueden ser los documentos comerciales, que llegando a destinatarios inadecuados puedan causar cuantiosas perdidas a la empresa.

Con respecto al problema del SPAM, parece también evidente que cuanto antes sea detectado y eliminado, mejor, por lo que si integramos en nuestro gestor centralizado de correo electrónico un módulo de Anti Spam reduciremos los problemas que causa en nuestros usuarios y en sus puestos de trabajo.

Además de estas herramientas, antivirus, antispam y control de contenidos, que podemos integrar en nuestros gestores de correo electrónico, debemos añadir un modulo que impida que nuestro sistema pueda ser capturado por algún hacker o spamer y que sirva para reenviar correos desde nuestro sistema y utilizando nuestras infraestructuras de comunicación.

Este modulo de Anti Relay, que es el nombre técnico de la medida de seguridad, es en la actualidad un requerimiento básico en la implementación de cualquier nuevo sistema de correo electrónico.

Las medidas de seguridad integradas en el gestor de correo electrónico complementan y amplían la seguridad que se implementa en el puesto de trabajo y por tanto ambas deben estar presente en nuestro sistema.

4.1.3.- Prevención en el Perímetro de la red

Los sistemas servidores de correo electrónico se han integrado cada vez mas en redes complejas que incluyen servidores de los mas diversos servicios, como pueden ser los servidores de paginas Web, los servidores de Bases de Datos, los servidores de aplicaciones, etc.

Toda esta red de servidores en unión con la red de puestos de trabajos ha formado redes informáticas que incluso en las Pymes han adquirido una gran complejidad. Estas redes tienen además conexión con redes de otras empresas mediante conexiones de Internet dedicadas.

Con el advenimiento de las tecnologías xDSL y Cable, este modelo de conexión dedicada ha llegado a las Pymes, con lo que las medidas de prevención en el perímetro, que antes solamente ocupaban a las grandes empresas o a los proveedores de servicios se hacen necesarias también en redes mucho más pequeñas.

Las principales medidas de seguridad en el perímetro de una red y que protegen especialmente al correo electrónico son el Cortafuegos, el detector de intrusiones y el antivirus que ha evolucionado a una herramienta de seguridad que también protege del Spam y los contenidos no deseados.

El Cortafuegos, Firewall en inglés, es un elemento cuyo principal objetivo es filtrar las conexiones permitidas haciendo que nuestra red se conecte únicamente con aquellas otras redes que sean de nuestro interés. Evidentemente el cortafuegos tiene además otras funciones, pero en el caso del correo electrónico esta es su mejor aportación.

El detector de intrusiones, IDS, como bien dice su nombre es un elemento de la seguridad perimetral que sirve para detectar las posibles intrusiones que se intentan realizar tanto por Hackers como por virus que intentan penetrar en nuestra red. En los últimos tiempos estas aplicaciones han evolucionado hacia los que ahora se denomina IPS o sistemas de Prevención de intrusiones, que no solamente detectan sino que además son capaces de tomar medidas que protegen efectivamente la red de un ataque malicioso.

Hemos visto que el antivirus puede y debe estar presente en otros dos niveles , el puesto de trabajo y el servidor gestor de correo electrónico, pero esto no es suficiente por varios motivos.

El primer motivo es que muchas empresas, pero fundamentalmente muchos proveedores de servicios que han instalado grandes servidores de correo electrónico han usado aplicaciones para las cuales no existe un antivirus especifico con lo cual el nivel de protección se reduce al puesto de trabajo.

El motivo principal es que tanto para el problema de los virus informáticos, el SPAM o los contenidos inadecuados, si dejamos que lleguen al servidor de correo electrónico o incluso al puesto de trabajo le añadimos un trabajo que se puede hacer mejor previamente.

Un sistema de seguridad integrado en el perímetro de la red para el sistema de correo electrónico que realice en una sola acción la detección y limpieza de Virus, Spam y contenidos inadecuados conseguirá que nuestros usuarios solo reciban información útil, descargando además al servidor de correos de una función secundaria y añadida.

La pregunta es, entonces ya no es necesario tener antivirus en el servidor de correos y el puesto de trabajo? La respuesta inicial sería si, sin embargo con los virus existentes en la actualidad la respuesta es No, son absolutamente necesarias las protecciones en el puesto de trabajo y en los servidores de correo.

Los virus de red pueden entrar a través de una vulnerabilidad en el sistema operativo o incluso de alguna aplicación y una vez infectado el sistema pueden utilizar el correo electrónico como un medio adicional para distribuirse por otras redes. En este caso los tres niveles de protección, puesto de trabajo, gestor de correo electrónico y perímetro de la red son necesarios.

4.2.- Medidas de Higiene Tecnológica

Un elemento importantísimo en la seguridad del correo electrónico es lo que vengo a denominar Higiene Tecnológica.

De los problemas que aquejan al correo electrónico una gran parte son los virus y el SPAM que durante mucho tiempo utilizado a los propios usuarios finales como el elemento desencadenante de las epidemias de virus o incremento del SPAM.

Mediante la denominada ingeniería social muchos virus han conseguido que fuera el propio usuario quien infectara su puesto de trabajo al ejecutar o visualizar ficheros adjuntos que le llegaban desde direcciones desconocidas, un ejemplo fue el virus Kournikova que llegaba a los usuarios simulando una fotografía de la tensita y que muchos usuarios picados por la curiosidad abrían el archivo y por tanto infectaban sus ordenadores y ayudaban a extender la epidemia.

La higiene tecnológica esta relacionada con la educación de los usuarios y aunque se han realizado varias campañas publicas aun nos encontramos que los virus nuevos continúan utilizando la ingeniería social con un cierto éxito.

Con respecto al Spam, uno de los errores mas habituales de los usuarios en responder al correo del Spam indicándole que no desean recibir mas información de ese sitio, es precisamente esto lo que hace que nuestra dirección de correo electrónico pase a formar parte de las direcciones comprobadas y a partir de entonces recibiremos aun mas SPAM puesto que nuestros datos ya comprobados pasaran a engordar las grandes bases de datos de direcciones de correo electrónico.

Un fenómeno mas reciente es el PHISING o la utilización de correos electrónicos que mediante ingeniería social, como no, nos invitan a enviar nuestros datos de usuario y password de por ejemplo banca electrónica o dirigir nuestro navegador a sitios muy similares al de nuestro banco donde nos capturan dichos datos de usuario y password.

Las entidades Bancarias recuerdan constantemente a sus usuarios que en ningún caso debemos dar estos datos por correo electrónico ni siquiera por teléfono.

Así pues, esta higiene tecnológica debe estar presente cada vez que utilizamos el correo electrónico puesto que vemos que no solamente incrementar los problemas de virus o SPAM sino que incluso podemos llegar ser victimas de delitos contra nuestra propiedad.

5- Conclusiones

El correo electrónico es el medio de comunicación global en nuestros días, tanto de uso empresarial como privado, y que a lo largo de su evolución ha sufrido diversos problemas de seguridad y que probablemente sufra nuevas amenazas en un futuro.

Sin embargo, en paralelo han ido apareciendo productos y servicios de seguridad que hacen que el correo electrónico no solo siga siendo el medio de comunicación más masivo sino que en el futuro sea aun más útil.

Sin embargo, aunque los productos de seguridad para el correo electrónico como el antivirus, antispam, control de contenidos, cortafuegos, detectores de intrusiones, etc ayudan a reducir el riesgo de sufrir ataques o perdidas en nuestro correos electrónico necesitan de un elemento primordial para mejorar la seguridad y es una mayor higiene tecnológica.

Cuanto mas alertas estemos todos para evitar, incluso accidentalmente, epidemias de virus, que nuestra dirección de correos u otros datos confidenciales caigan en manos de organizaciones delictivas conseguiremos que el correo electrónico siga siendo un medio de comunicación global, ágil y por que no seguro.

En definitiva, utilicemos todos los medios a nuestro alcance, tanto tecnológicos como humanos para proteger nuestro correo electrónico, que algunos ya dicen que es imprescindible en nuestras vidas.

http://es.trendmicro-europe.com

- **CAPITULO 9: GESTION DE CONTINUIDAD DE NEGOCIO**

Se estima que dos de cada cinco empresas que sufran un desastre estarán fuera del mercado en un plazo de cinco años. Las empresas están en disposición de cambiar esta probabilidad pero sólo si han tomado los pasos necesarios antes y después del desastre.

Gartner - Septiembre 2001

1. Introducción

A lo largo de los últimos años la importancia del concepto de continuidad de negocio se ha puesto de relevancia con acontecimientos como el efecto 2000, el cambio al euro o algunos desastres como la falta de energía eléctrica en California durante el año 2001 o los terribles incendios que asolaron el área de Sydney durante los años 2000 y 2001. Pero fueron los terribles atentados terroristas del 11 de Septiembre contra el World Trade Center de Nueva York los que supusieron un auténtico punto de inflexión en la idea de que **la gestión de la continuidad de negocio ha dejado de ser una moda para convertirse en una necesidad estratégica** que todas las empresas de cualquier tamaño deben tener en cuenta en mayor o menor medida.

En todos los casos mencionados anteriormente la anticipación y la planificación explicitadas en los planes de continuidad de negocio han sido los elementos claves que han asegurado la supervivencia de algunas empresas que han vistos sus negocios amenazados por los riesgos de dichos acontecimientos. Al contrario otras empresas que no contaban con ninguna planificación de continuidad de negocio han visto extinguida su actividad.

La calificación de desastre es totalmente subjetiva y depende de cada empresa y de cada sector pero de cualquier modo todo directivo responsable debería conocer en detalle que incidentes se pueden calificar de desastre dentro de su organización y plantearse regularmente preguntas como:

- ¿Qué sucedería en el caso de que un incendio destruyera la sede central de la compañía?
- ¿Qué pasaría en el caso de un ataque masivo de un virus informático que formateara los equipos de la red local?
- ¿Cómo afrontaría la empresa la marcha o desaparición accidental de miembros claves de la organización?

- ¿Cómo manejaríamos el robo o exposición accidental de datos confidenciales de nuestros clientes, empleados o proveedores?

El objetivo de este capítulo es poder responder a este tipo de preguntas examinando **qué es la gestión de la continuidad** de negocio, viendo las razones objetivas de por qué es importante y esbozando brevemente como se plantea un proyecto de implementación de este tipo de gestión dentro de la organización.

2. Evolución histórica

Siete de los diez desastres más costosos económicamente sucedidos en los EEUU han sucedido desde 1989 hasta hoy.

IBHS - 2001

El concepto de **gestión de continuidad** de negocio se puede definir como el proceso que se ocupa de detallar el conjunto de actuaciones estratégicas, políticas y planes operativos, destinados a restablecer la plena operatividad de la empresa como consecuencia de una crisis, en un horizonte temporal breve, medio y largo.

Esta idea surge durante los años finales de la década de los setenta como una reacción natural a la introducción de la tecnología informática en el núcleo de los procesos de negocio de las empresas. Por primera vez en la historia empresarial se constató que fallos en un único sistema podían ocasionar graves daños en la actividad operativa de toda una empresa llegando en caso extremos a una paralización total de la actividad. Por ello no es extraño que los primeros elementos en nacer dentro de la gestión de continuidad de negocio fueran la reparación de fallos y los **planes de recuperación de desastres**, ambos encargados de proporcionar a la empresa de la adecuada planificación para responder a eventos que pusieran en peligro las aplicaciones o sistemas críticos para la continuidad de la actividad empresarial.

En una etapa posterior y a principio de la década de los noventa se pasó de esta postura reactiva a una estrategia proactiva en la que la anticipación y la planificación ya ocupaban un espacio fundamental. Aprovechando los avances que se estaban produciendo en el cálculo de probabilidades, se introdujo el nuevo concepto de la prevención y análisis de riesgos como una disciplina primordial para que las empresas se prepararan ante un entorno cada vez más complejo e inestable.

Evolucionando desde el planteamiento anterior aparecieron los **planes de contingencia** como la preparación de las acciones integrales de respuesta a los distintos riesgos identificados como de gran impacto para la empresa y que un primer momento seguían muy ligado a conceptos informáticos como fallos de hardware, de software, etc.

Paulatinamente este concepto se ha ido expandiendo dentro del ámbito de la empresa para cubrir todos aquellos percances que pueden afectar a la supervivencia del negocio como la marcha de una persona clave, de un cliente importante, de un proveedor estratégico, etc. y se ha empezado a tratar como un proceso continuo y en constante evolución dando paso a lo que se conoce como **gestión de continuidad de negocio**. Este cambio supone la introducción y el desarrollo de controles y pruebas que aseguren la continuidad del negocio y el funcionamiento de los distintos planes en cualquier situación temporal o geográfica.

Actualmente la existencia de un plan de continuidad de negocio se considera como algo que toda empresa debe tener en cuenta aunque las estadísticas nos muestran que la implementación real de estos planes está todavía lejos de estar ampliamente extendida en el tejido empresarial. Según datos de la consultora *Gartner* habrá que esperar al menos hasta el año 2007 para que el 35% de las grandes empresas dispongan de una infraestructura completa de continuidad de negocio.

Si bien los departamentos de TI están en su mayoría reconocen la necesidad de la elaboración de estos planes a menudo se choca con la falta de fondos tanto en el desarrollo de la consultoría y los planes de continuidad como en las acciones e inversiones necesarias para que estos planes se lleven a cabo.

3. La situación actual en España

Un 77% de las empresas españolas tiene problemas esporádicos con la seguridad informática, mientras que un 6% los sufre habitualmente.

Grupo Penteo - 2004

La situación en España es reflejo de la situación internacional. Existe una preocupación clara por la seguridad de los sistemas de información y es una tendencia que empieza a formar parte de la cultura empresarial y a dejar de ser una preocupación exclusiva de los departamentos de sistemas.

La patronal *AETIC* y el *Grupo Teneo* publican anualmente el estudio “La seguridad informática en la empresa española” que mediante un muestreo de 238 empresas de distintos

sectores y niveles de facturación proporciona una excelente visión de conjunto de la situación actual del mundo empresarial con respecto a los temas relacionados con la seguridad.

Algunos datos relevantes de ese estudio nos muestran el incremento que durante el año 2004 ha sufrido la elaboración de los planes de continuidad en la empresa española. En el estudio del año 2003 solamente una de cada diez empresas tenía desarrollado un plan y un 42% tenían previsto acometerlo próximamente. En el año 2004 los datos nos dicen que esta previsión estaba totalmente fundada ya que el 58% de las empresas encuestadas han materializado un plan de continuidad mientras que un 37% tiene prevista su elaboración a corto plazo.

De este estudio también se desprende la idea de que la gestión de la continuidad de negocio todavía es vista como una disciplina totalmente vinculada a los sistemas informáticos. Todavía queda por recorrer el camino que haga de la continuidad de negocio una preocupación que resida en todos los miembros de la organización empresarial desde los equipos directivos hasta todos los trabajadores de cualquier área.

4. Definición de la gestión de continuidad de negocio

La confianza y reputación pueden desaparecer de la noche a la mañana.

Alan Greenspan – Reserva Federal de EE.UU.

Según el *Business Continuity Institute* podemos definir la gestión de la continuidad de negocio como **la acción de prever aquellos incidentes que afectan a funciones o procesos críticos para la organización y que asegura que la respuesta a todos ellos se ejecuta de una manera organizada y consecuente.**

Podemos extraer los tres elementos claves de esta definición:

- Se trata de anticipar una crisis o incidente
- Afecta gravemente al conjunto de la organización
- Requiere de un plan de respuesta

Como podemos observar los conceptos fundamentales que habrá que tener en cuenta en la gestión de la continuidad de negocio surgen de estos elementos claves.

El primero de ellos es la anticipación. La base sobre la que se asienta una adecuada gestión de la continuidad de negocio es una evaluación y gestión de riesgos realista que sea transversal e implique a toda la organización.

Una vez definidos los posibles riesgos hay que evaluarlos y priorizarlos ya que sólo van a ser objeto de esta gestión aquellos que tengan graves consecuencias en el negocio o la actividad operativa de la empresa. Se requiere de un profundo conocimiento de la organización de la empresa para evaluar adecuadamente cuales son las consecuencias que cada uno de los riesgos conlleva.

Con toda la información recopilada anteriormente y como último paso hay que elaborar la estrategia apropiada para recuperar el nivel normal de actividad de la forma más rápida y eficiente que sea posible.

De cualquier forma es necesario entender que no existe un método universalmente válido para la implantación de la gestión de continuidad de negocio en una empresa ya que ésta depende de múltiples factores que son únicos de cada organización como pueden ser la cultura de la empresa, el estilo de gestión, el sector o el propio organigrama funcional. De hecho un plan que puede ser perfectamente válido para una institución financiera puede resultar absolutamente inservible para una empresa industrial.

Uno de los errores más comunes que se han cometido en la aplicación de la gestión de continuidad de negocio es el pensar que el objetivo final de todo el proceso es la confección de un documento que sea lo más extenso posible. Esta idea, alimentada habitualmente por los consultores y asesores externos, suele buscar como objetivo cumplir objetivos que se encuentran bastante alejados de la filosofía real de la gestión de continuidad de negocio, como el cumplimiento de algún requerimiento de la compañía de seguros o de los auditores de calidad. El resultado final en estos casos es un plan obsoleto y erróneo en su concepción cuya aplicación puede llegar a ser peor que la falta total de cualquier tipo de plan.

El contexto perfecto para la adecuada implementación de la gestión de continuidad de negocio la encontramos cuando la idea ha sido inspirada y promovida desde la alta dirección y que ésta participe en algún grado en el mantenimiento y actualización de toda la información generada. Es absolutamente necesario que la gestión de continuidad de negocio se vea como un proceso continuo que es necesario mantener vivo y que forma parte de la cultura y de las buenas prácticas de gestión de la organización a todos los niveles.

5. El por qué de la gestión de continuidad de negocio

El 83% de las empresas españolas ha sufrido problemas de seguridad informática.

Grupo Penteo - 2004

Existen gran cantidad de causas que pueden provocar en cualquier momento que una empresa quede total o parcialmente inoperativa. El siguiente grafico reflejas las principales causas:

Debido a la naturaleza de la gestión de continuidad de negocio y a la amplitud de temas de los que se ocupa nos encontramos que sus implicaciones son muy variadas y multidisciplinares. Nos vamos a centrar en algunos de los aspectos que más relevancia tienen y que consideramos que son los más comunes entre empresas de distintos sectores productivos y niveles de facturación.

Aspectos legales

Dentro de la normativa actual podemos encontrar varias referencias a la seguridad de los datos e infraestructuras de sistemas de la información que de hecho obligan legalmente a las empresas a tener en cuenta y a realizar ciertas inversiones que cubren parte del objeto del que trata la continuidad de negocio.

En concreto en el artículo 9.1. de la Ley Orgánica de Protección de Datos Personales podemos leer:

> *"Se adoptarán las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural."*

De la lectura de este artículo podemos extraer obligaciones que la empresa debe acometer a varios niveles tanto técnicos como organizativos y que comparte el mismo proceso y el mismo objetivo final que la gestión de la continuidad de negocio, responder a riesgos de forma ordenada mediante una adecuada respuesta organizativa y técnica.

Aspectos económicos

Cada empresa es una organización única con sus peculiaridades particulares lo que hace que no se pueda hablar de implicaciones económicas universales y que afecten a todas las organizaciones por igual.

De cualquier modo parece evidente que la mayor repercusión en la cuenta de resultados de una parada de la actividad de la empresa provendrá de la bajada de los ingresos por ventas que no se hayan podido obtener.

Los equipos directivos son los responsables de conocer mediante análisis de riesgos y de impacto de negocio como afecta a su organización cada incidente, cuándo estos deben llegar a la categoría de desastre y cómo debe responder su empresa ante ellos.

Se han realizado estudios, principalmente en los EE.UU., que nos permiten entrever cómo afecta un desastre a distintos tipos de empresas mediante el cálculo de la media del coste por hora en situaciones de crisis:

Industria	Área de negocio	Coste medio por hora
Financiera	Operaciones de cambio	6,5 millones de dólares
Financiera	Autorizaciones de tarjeta de crédito	2,6 millones de dólares
Comunicaciones	Ventas por pago por visión	1,1 millones de dólares
Comercio	Venta por televisión	$113.000
Comercio	Venta por catálogo	$90.000
Transporte	Reserva de billetes de aerolíneas	$89.500

Fuente: Business Continuity:When disaster strikes, 2000, Fibre Channel Association,Texas

En otro estudio publicado por el *Disaster Recovery Journal* se muestra que el coste medio por hora en situación de crisis de la industria de los EE.UU. fue de $330.000 en los primeros años de esta década, haciendo que el coste global ascendiera a los 4 billones de dólares, provenientes principalmente de la bajada de ingresos que supusieron los distintos incidentes.

Otro aspecto económico que surgió tras los atentados del 11 de Septiembre es la subida de las primas de las aseguradoras, que fue uno de los sectores más afectados.

Cada vez es más habitual que las empresas aseguradoras, y muy especialmente en aquellos casos en que aseguran negocios cuyo núcleo reside en sistemas informáticos, pregunten como parte del cuestionario de solicitud si la empresa posee un plan de continuidad de negocio, de contingencia o de recuperación de desastres. La respuesta a esta pregunta afectará al cálculo de la prima.

Aspectos empresariales

Como consecuencia del incremento de la competencia existe una tendencia en el mercado actual que provoca la total orientación al cliente por parte de la empresa con el objetivo final de fidelizar a los clientes y conseguir una ventaja competitiva en el mercado.

Dentro de esta estrategia las tecnologías de la información tienen un papel preponderante que permite que las empresas ofrezcan a sus clientes niveles de información de todo tipo y servicios de forma transparente y cubriendo franjas horarias que se salen de la atención habitual del horario de oficina.

En este contexto el fallo de los sistemas que controlan este tipo de servicios provoca toda una serie de problemas que son difícilmente cuantificables económicamente pero que sin embargo tienen un enorme impacto empresarial ya que afecta a la relación de la empresa con sus clientes.

Pensemos en fallos de seguridad en la extranet de una empresa con sus clientes que hagan que los niveles de riesgo puedan ser consultados por un competidor, o un error en la banca online que provoque que no se pueda realizar una transferencia en el plazo previsto, o una parada en el sistema de planificación de recursos (ERP) que haga que nos sea imposible aceptar un pedido de uno de nuestros clientes…

Todos estos problemas van más allá de la cuenta de resultados ya que al final afectan a la imagen, la reputación y el saber hacer de la empresa en el mercado lo que a la larga y de no solucionarse puede afectar gravemente a su posición competitiva en el mercado.

Por otro lado, también existen oportunidades derivadas de la implantación de infraestructuras de continuidad de negocio como la posibilidad de diferenciarse de la competencia ofreciendo acuerdos de nivel de servicio (SLA) o acuerdos contractuales que no puedan ser igualados por nadie más.

6. La puesta en marcha de la gestión de continuidad de negocio

Para la preparación de la batalla siempre he encontrado que los planes han sido inútiles pero la planificación ha sido indispensable.

Dwight D. Eisenhower

Pese a que la preocupación existente por la necesidad de sistemas que aseguren la continuidad de negocio ha evolucionado dando lugar a una disciplina con sus propios departamentos dentro de las consultoras, su propia metodología, sus sistemas de software personalizados y abundante literatura hay que pensar en que en esencia, es un proceso muy simple y de sentido común.

Quizá la parte más importante, y habitualmente no tomada en consideración, es comprender que la gestión de la continuidad de negocio no es la producción de un plan o de una serie de documentos, sino de **un proceso interno que cambie la cultura de la organización y haga comprender a todos los miembros, que los riesgos y desastres existen, que tienen consecuencias graves para la continuidad de la empresa y que se pueden prevenir tomando las acciones adecuadas.**

Dentro de este entorno, el plan sólo es el último escalón en el que se recoge el conocimiento de todo el proceso, pero de hecho es muy probable que el equipo que ha participado en la elaboración y el mantenimiento del plan prácticamente no lo necesite más que como guía de apoyo en el momento de su aplicación.

La mejor aproximación al proceso de la gestión de continuidad de negocio es acometerla en distintas fases:

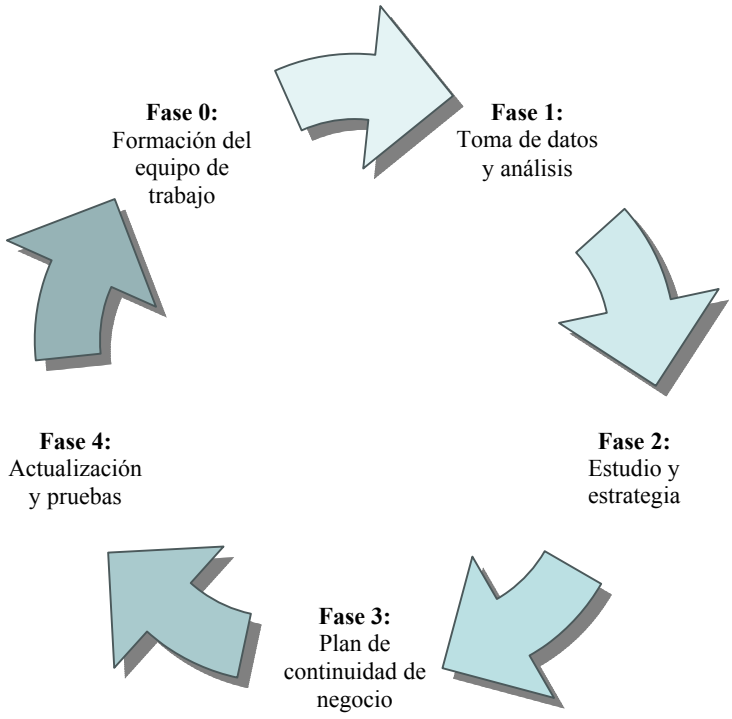


Figura 1: Fases del proceso de gestión de continuidad de negocio

Fase 0: Formación del equipo de trabajo

La puesta en marcha de un sistema de este tipo requiere de la implicación de varias áreas de la empresa así como de un decidido impulso por parte de la dirección y el establecimiento de un objetivo compartido por toda la organización cuya finalidad sea realmente crear una infraestructura de continuidad de negocio y no cumplir meramente con alguno requisitos sean legales, corporativos o económicos.

Si no logramos crear este impulso interno dentro de la organización y si no existe un objetivo real, claro y compartido estaremos perdiendo recursos y dinero ya que el fracaso de la iniciativa es lo más probable.

Una vez que la empresa ha tomado la decisión de poner en marcha la gestión de continuidad de negocio se debe comenzar por el nombramiento de una persona responsable de su desarrollo y mantenimiento. Este perfil debe tener la autorizad suficiente dentro de la organización y tener una visión clara y global del conjunto del negocio.

Es muy recomendable que el siguiente paso sea la creación de un grupo de trabajo para llevar a cabo el seguimiento y actualización de los pasos que se vayan dando. La composición de este grupo varía de empresa a empresa pero de él deberían formar parte personas de todos

los departamentos que se consideren necesarios para el mantenimiento de la actividad de la empresa.

Al menos mensualmente el responsable de la continuidad de negocio debe convocar una reunión con el grupo de trabajo. Estas reuniones ejecutivas no deberían tener una duración de más de una hora y lograr los siguientes objetivos:

- Mantener informada a toda la organización de los pasos que se están dando en otros departamentos
- Hacer un seguimiento de la implantación de la gestión de continuidad de negocio
- Asegurar que todos los procesos de negocio críticos para la empresa se están teniendo en cuenta

Fase 1: Toma de datos y análisis

Una de las partes fundamentales más importantes y de la que puede depender el éxito o fracaso de un plan de continuidad de negocio es el desarrollo de los estudios previos. El objetivo de estos estudios es el análisis de los riesgos a los que la empresa se enfrenta conjuntamente con el estudio de las probabilidades de que estos se materialicen y el análisis del impacto en el negocio de cada uno de esos riesgos.

Normalmente estos estudios se realizan a través de cuestionarios y entrevistas con los directivos y mandos intermedios de cada uno de los departamentos de la organización. Como un mero ejemplo citamos algunos de los datos relevantes que deberían salir de las entrevistas:

- Tipo de problema
- Impacto del problema a varios niveles: legal, económico, de imagen…
- Establecimiento de métodos de funcionamiento alternativos desde el punto de vista de tiempo y recursos
- Restablecimiento total del sistema que ha fallado desde el punto de vista de tiempo y recursos
- Existencia de personas claves para el funcionamiento del sistema

Con ello se logra tener una idea clara del conjunto de problemas posibles para luego pasar al trabajo más importante que es dotar de la prioridad adecuada a todos estos problemas para que el análisis de impacto de negocio no se convierta en un listado de las preocupaciones de cada departamento sino que tenga una consistencia y una visión global que afecte a la empresa como un todo y que permita la toma de decisiones en los pasos posteriores.

Fase 2: Estudio y estrategia

Durante esta fase se toma la información en bruto obtenida anteriormente y se depura y estudia con el objeto de comenzar a establecer las estrategias adecuadas para el tratamiento de cada problema y riesgo así como la necesaria dotación presupuestaria para llevar a cabo las distintas acciones requeridas para la recuperación y el restablecimiento de cada sistema que se vaya a estudiar.

Una pregunta recurrente en esta fase es si es necesaria la intervención de consultores externos. La respuesta en nuestra opinión es que no son necesarios pero sí convenientes.

Por un lado sería del todo imprudente poner en manos externas el desarrollo de la estrategia necesaria para implantar un plan de continuidad de negocio para cuyo desarrollo es necesario un profundo conocimiento de la empresa a todos los niveles.

Por otro lado la intervención de personas externas aporta otra perspectiva al proceso enriqueciéndolo con la experiencia de implantaciones en otras empresas con problemáticas similares y con el aprovechamiento del conocimiento generado en la industria y la aplicación de las mejores prácticas.

En general cada empresa debe obtener el balance adecuado entre las dos opciones para lograr aprovechar lo mejor de cada una de ellas y desarrollar la labor de la mejor forma posible.

Fase 3: Plan de continuidad de negocio

Este es el documento en el que se va a recoger el conocimiento generado en las fases anteriores. Nunca hay que perder de vista que el objetivo final de este documento es su aplicación en medio de una crisis grave y no el obtener un impresionantemente largo documento perfectamente elaborado pero poco práctico.

Algunas de las características de un buen plan son:

- Simple: de fácil comprensión
- Práctico: escrito con conocimientos del funcionamiento de los procesos de la empresa
- Flexible: que tenga en cuenta los posibles fallos y errores que puedan poner en peligro la puesta en marcha del plan así como la posibilidad de enfrentarse a desastres que no estén reflejados de forma explícita
- De fácil actualización: es un documento vivo y que debe cambiar a lo largo del tiempo

Fase 4: Actualización y pruebas

Como hemos comentado varias veces a lo largo de estas páginas, el objetivo último de un plan de continuidad de negocio es su aplicación práctica. Por ello no debemos quedarnos en la obtención de un documento que con mejor o peor apariencia y más o menos páginas deje contentos a la dirección de la compañía, a la empresa aseguradora o a los consultores externos.

Es obligación inexcusable del responsable de continuidad de negocio el establecimiento de un plan de pruebas periódico que asegure que todos los datos, procesos, personas y recursos materiales que se detallan en el plan están disponibles y en perfecto estado de aplicación en todo momento.

De este plan de pruebas irán surgiendo cambios y variaciones que irán enriqueciendo el plan original para que se acerque cada vez más a los objetivos que debe cumplir.

No cabe duda de que la empresa es un ente vivo y en continua evolución por lo que el plan de continuidad debe estar a la par de los cambios que sufra la empresa en su evolución natural. La fuente de información adecuada para lograr esto son las reuniones periódicas del grupo de trabajo de continuidad de negocio en el que los responsables de los distintos departamentos deben informar sobre los cambios operativos, técnicos u organizativos que se van produciendo y que puedan tener su impacto en el plan de continuidad.

En definitiva lo que es importante que la organización tenga en cuenta es que no estamos ante un documento estático que hay que tener al día sino ante un proceso de mejora continua, que involucra a toda la organización y cuyo resultado final se plasma en un documento.

7. Conclusiones

- Los planes de continuidad pueden convertirse en el elemento clave para la supervivencia de una empresa ante un desastre.
- No existe una calificación ni una clasificación genérica de desastre por ello los planes de continuidad son únicos para cada empresa.
- No estamos hablando de producir un plan sino de desarrollar un proceso interno que cambie la cultura de la organización.
- Es necesario conocer la empresa en profundidad para ser capaces de priorizar.

- El éxito de la gestión de la continuidad recae en la implicación de la organización tanto en su desarrollo como en su mantenimiento.

http://www.going.es

- **CAPITULO 10: CONFORMIDAD LEGAL**

1- Introducción: La Ley aplicada a las nuevas tecnologías

Hoy en día, y el presente manual es una prueba de ello, nos ha tocado vivir una auténtica revolución, como en su día fue la "revolución industrial". Las tecnologías de telecomunicación se han sumado a la informática dando lugar a la telemática y a las redes de ordenadores, cuyo máximo exponente es la red Internet.

Las empresas, como es patente, no están al margen de esta revolución. Cada vez son más las que se introducen en el nuevo entorno de Internet, ofreciendo información sobre sus productos o servicios o, incluso, comerciando directamente a través de la Red. Es lo que conocemos popularmente como Comercio Electrónico.

El Derecho, como instrumento organizador de las relaciones sociales y económicas, debe dar respuesta a esta nueva realidad, regulándola "ex novo" o aplicándole el marco legal tradicional, a través de su interpretación. Debido a ello, asistimos al importante desarrollo de una nueva rama o especialidad jurídica: el Derecho Informático.

Parte de esta tarea ya se ha realizado: la Ley Orgánica 15/1999 de Protección de Datos de carácter Personal (LOPD), la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI) o la más reciente Ley 59/2003 de Firma Electrónica son ejemplos de ello.

Sin embargo, hay que destacar que, muy al contrario de lo que se suele poner de manifiesto en los foros de noticias, Internet no escapa a la aplicación de la Ley. Puesto que, aunque no se aprueben nuevas normas especificas, el Derecho tradicional también se aplica a la Red. Al fin y al cabo, detrás de este "mundo virtual" se hallan personas reales, con su nombre, sus apellidos y su dirección física. Todos los días vemos ejemplos en los medios de comunicación que lo demuestran: detención de hackers, demandas contra contenidos de páginas web, recuperación de nombres de dominio que vulneraban marcas, compras y ventas válidas realizadas "on-line", defensa de la libre competencia (caso Microsoft) y la protección de los derechos sobre las creaciones originales (caso Napster), entre otros.

En conclusión, cabe decir que, quedando aún mucho por hacer, el Derecho Informático ya está lo suficientemente desarrollado como para solucionar la mayoría de los conflictos y regular la mayoría de las relaciones sociales y económicas que se producen en Internet y, en general, en la nueva Sociedad de la Información.

En el presente capítulo trataremos de poner de relieve los ámbitos más destacados de esta nueva rama del Derecho así como su visión práctica para las empresas que deciden aventurarse en el nuevo entorno de negocios que supone Internet y las nuevas Tecnologías.

2- Protección de Datos en la Empresa:

2.1.- Obligaciones generales derivadas de la LOPD.

La enorme capacidad de tratamiento y transmisión de la información que ofrecen las nuevas tecnologías hacen acuciante la necesidad de proteger los derechos fundamentales del individuo ante el posible uso abusivo de las mismas, en concreto: el derecho al honor, a la intimidad personal y familiar y a la propia imagen, tal y como se reconoce en el artículo 18, apartado 4, de nuestra Constitución de 1978.

Debido a ello, ha surgido diversa normativa internacional, europea y española que se ha denominado genéricamente como de “Protección de Datos” y que ha culminado en nuestro país con la adopción de la llamada LOPD.

LOPD son las siglas abreviadas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Esta Ley, fundamentalmente, tiene el objetivo de proteger a las personas físicas con respecto al tratamiento que se pueda realizar de sus datos individuales llevado a cabo por distintas entidades, ya sean públicas o privadas.

Dicha regulación pretende, fundamentalmente, establecer un control sobre quién tiene dichos datos, para qué los usa y a quién y cómo los cede. Para ello, impone una serie de obligaciones a los responsables de dichos ficheros de datos: como son las de recabar el consentimiento de los titulares de los datos para poder tratarlos, comunicar a un Registro especial la existencia de dichas bases de datos y su finalidad, así como mantener unas medidas de seguridad mínimas sobre las mismas, en función del tipo de datos recogidos. Por otro lado, la LOPD reconoce al individuo una serie de derechos sobre sus datos como son los de información, acceso, rectificación e, incluso, de cancelación de los mismos en determinados supuestos.

Como entidad de control, se designa a la Agencia Española de Protección de Datos, como órgano administrativo autónomo encargado de hacer cumplir la LOPD y sus reglamentos, pudiendo inspeccionar e imponer fuertes sanciones a aquellos sujetos que la infrinjan. Dichas sanciones van desde los 600 a 60.000 euros, por una infracción leve, pasando por los 60.000 a 300.000, por una grave, hasta los 300.000 a 600.000 euros, por una muy grave. Teniendo en cuenta que los mínimos de cada tramo se aplican siempre, incluso a una PYME o incluso a un

autónomo, cabe considerar dichas sanciones enormemente gravosas y que convierten esta materia en una de las que generan mayor preocupación al empresario en la actualidad.

2.2.- Las Medidas de Seguridad exigibles en el R.D.994/1999: Niveles de Seguridad y su aplicación.

Entre las normas que desarrollan la Ley de Protección de Datos, destaca especialmente el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de las Medidas de Seguridad que deben cumplir los ficheros con datos de carácter personal.

Esta norma se basa en el artículo 9 de la LOPD, que impone la obligación al responsable del fichero y al encargado del tratamiento de adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

El incumplimiento de esta obligación, es decir, mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad, supone una falta grave sancionable con una multa de entre 60.000 y 300.000 euros (10 y 50 millones de las antiguas pesetas), en base a los artículos 44.3 y 45.2 de la LOPD.

El Reglamento de Medidas de Seguridad estipula tres niveles de seguridad aplicables: el básico, el medio y el alto. Para saber cuál de ellos debemos aplicar, hay que fijarse en el tipo de datos personales tratados en cada fichero: a mayor sensibilidad de los mismos, mayor es el nivel de seguridad aplicable. De este modo, en base a lo dispuesto en el artículo 4 del Reglamento, se deduce lo siguiente:

1- Nivel básico:

- Aplicable a todos los sistemas con datos personales en general.

2- Nivel Medio:

- Datos de comisión de infracciones administrativas o penales,
- Datos de Hacienda Pública,
- Datos de servicios financieros,
- Datos sobre solvencia patrimonial y crédito y

- Conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

2- Nivel Alto: para datos referidos a la

- Ideología,
- Religión,
- Creencias,
- Origen racial,
- Salud o vida sexual y
- Datos recabados para fines policiales.

En lo que respecta a las medidas de seguridad, las mismas se aplican de forma cumulativa: así el nivel alto deberá cumplir también las reguladas para el nivel medio y el nivel bajo de seguridad.

Destacamos especialmente la redacción de un Documento de Seguridad, donde se estipule la normativa interna y las obligaciones del personal en materia de protección de datos, así como la necesidad, a partir del nivel medio, de realizar una Auditoría de Seguridad cada dos años. Esta auditoría, que deberá dictaminar en un Informe final sobre la corrección de las medidas adoptadas, debe tener un doble carácter técnico y jurídico que interprete correctamente el cumplimiento de la normativa en los sistemas y procesos de la entidad.

2.3.- Modelo de Plan de Adaptación de la empresa al Reglamento y a la LOPD

En base a la experiencia acumulada por nuestro bufete en servicios de consultoría prestados a empresas en materia de LOPD, hemos elaborado un Plan de Adaptación al Reglamento y a la LOPD (PAR LOPD), que pretende, de un modo global, evaluar, asesorar jurídicamente e implementar medidas sobre cualquier empresa para su correcta adaptación tanto al Reglamento de Medidas de Seguridad como a la propia Ley en cuanto al procedimiento, documentación y requisitos exigidos.

Dicho PAR LOPD se estructura en cuatro fases fundamentales:

1ª FASE: ANÁLISIS DE LA SITUACIÓN JURÍDICA DE LOS FICHEROS

En esta primera etapa, se pretende comprobar el nivel de cumplimiento de la normativa sobre Protección de Datos Personales, tanto de la LOPD como del Reglamento sobre Medidas de Seguridad, en la empresa.

En la misma, se deberán realizan las siguientes actuaciones:

1- Se impartirá una charla previa de presentación de la LOPD y de los servicios a los responsables de la empresa, sin perjuicio de la formación ulterior. En base a nuestra experiencia, esta charla facilita mucho el resto de los trabajos, sobre todo en lo referido al punto siguiente.

2- Se formulará presencialmente un Cuestionario de Seguridad, claro y exhaustivo, a la empresa con el fin de evaluar su situación actual. Durante dicha cumplimentación, los auditores asistirán y responderán a todas las dudas y consultas sobre el mismo, aunque su contenido deberá ser de preguntas sencillas y de fácil comprensión.

3- En base al resultado de dicho Cuestionario y a las Bases de Datos detectadas en la empresa, se analizará su contenido y se estipulará la necesidad o no de su registro en la Agencia Española de Protección de Datos. En su caso, se inscribirán los ficheros necesarios en el Registro General de Protección de Datos del mencionado organismo.

4- En función de la tipología de los datos personales registrados, se determinará el nivel de seguridad aplicable según el Reglamento. (Aplicación del Nivel Básico, Medio o Alto de Seguridad)

5- En base al nivel estipulado y al análisis de las medidas de seguridad existentes, se señalarán las que cumplen con la normativa y las que será necesario implementar para este fin.

6- Se estipulará el grado de cumplimiento de la normativa de seguridad y realizarán, en su caso, las recomendaciones pertinentes a la empresa auditada con el fin de lograr una correcta a adaptación al Reglamento y a la LOPD.

2ª FASE: ELABORACIÓN Y SUPERVISIÓN DE LA DOCUMENTACIÓN

En esta segunda Fase, se procede a elaborar los documentos que preceptúa el Reglamento sobre medidas de seguridad para los ficheros automatizados que contengan datos de carácter personal, según el nivel de protección exigido. Deberá comprender las siguientes acciones:

1- Redacción del Documento de Seguridad de la Empresa exigido por el Reglamento. La correcta realización de este Documento es extremadamente importante ya que es el que estipulará la normativa de seguridad que deberá regir en la empresa auditada. La confección y el grado de complejidad de este texto variarán en función del nivel de seguridad exigido para los ficheros de datos personales.

2- Creación de un Registro de Incidencias para la empresa auditada, así como asesoramiento al responsable de los ficheros protegidos sobre su llevanza.

3- Supervisión o creación, en su caso, de una Relación Actualizada de los Usuarios Autorizados al acceso a los ficheros protegidos, así como la evaluación sobre la suficiencia o exceso en su grado de autorización en el acceso.

4- Supervisión de la correcta creación, en su caso, de un Registro de Soportes que contengan datos personales, así como la corrección en su uso.

5- Elaboración, en su caso, de los Escritos de Autorización, exigidos por el Reglamento, que deberá emitir el responsable de los ficheros protegidos para determinados procesos en su manipulación.

6- Creación y supervisión, en su caso, de un Registro de Accesos preceptivo, así como del Informe que el responsable de seguridad deberá emitir mensualmente sobre su revisión, en base al Reglamento.

3ª FASE: EVALUACIÓN DE LA APLICACIÓN DE LA NORMATIVA

El objetivo de la tercera Fase es evaluar la Ejecución de las medidas de adaptación a la normativa de seguridad. Comprenderá las siguientes actuaciones:

1- Supervisión y asesoramiento jurídico en cuanto a las medidas de seguridad implementadas por la empresa auditada.

2- Evaluación de las aplicaciones elaboradas por los técnicos, así como de las modificaciones técnicas y organizativas efectuadas, en cuanto a su suficiencia para cumplir con la normativa de seguridad exigida.

3- Realización de un Informe Final de Auditoría, en cumplimiento del artículo 17 del Reglamento, en el cual se contemplarán las conclusiones de los análisis efectuados, el grado de cumplimiento final de la normativa y una serie de recomendaciones en cuanto a las actuaciones periódicas a realizar para cumplir con la legalidad vigente en materia de protección de datos y prevenir posibles incidencias.

4ª FASE: FORMACIÓN Y ASESORAMIENTO LEGAL ULTERIOR

En una cuarta Fase, estimamos muy necesario el formar al personal de la empresa y contar con un asesoramiento jurídico continuado sobre cualquier cuestión que se suscite en relación con la implementación y funcionamiento de las medidas de seguridad evaluadas, así como cualquier consulta sobre la regulación vigente en materia de protección de datos. En concreto:

1- Formación del Responsable del Fichero, así como de los responsables de seguridad y demás personal dependiente del empresario que trate datos personales de cara a evitar posibles incumplimientos de la LOPD y del Reglamento.

2- Asesoramiento jurídico continuado del responsable de los ficheros, así como de los responsables de seguridad, en cuanto al desempeño de sus funciones.

3- Información actualizada del empresario sobre los posibles cambios que se produzcan en la normativa sobre protección de datos de carácter personal y en las exigencias sobre las medidas de seguridad aplicables producidos durante el plazo de un año.

4- Modificación o nueva redacción del documento de seguridad así como inscripción de nuevos ficheros ante la Agencia de Protección de Datos (creación, modificación o cancelación), en el caso de cambios en la estructura de los mismos o de la propia organización empresarial.

5- Asesoramiento y representación legal de la empresa auditada frente a posibles medidas o procedimientos administrativos sancionadores que se produjeren en relación al cumplimiento de la legalidad vigente en materia de protección de datos personales.

3- La Ley de Servicios de Sociedad de la Información y de comercio electrónico (LSSI)

Tras un largo período de evolución y consulta prelegislativa, en el cual se sucedieron hasta cinco borradores del anteproyecto de Ley, llevada a cabo por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología, finalmente se presentó el Proyecto de Ley a las Cortes el día 8 de febrero de 2002 y, tras nuevas e importantes modificaciones en el trámite parlamentario, se promulgó como Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico publicándose en el BOE de 12 de julio de 2002. En adelante, nos referiremos a esta norma por sus siglas “LSSI”.

A lo largo de los siguientes epígrafes, iremos abordando algunos aspectos de esta ley que viene a colmar importantes lagunas en nuestro ordenamiento jurídico y que tendrá una trascendencia fundamental sobre el desarrollo de la Sociedad de la Información en los próximos años.

3.1.- Ámbitos regulados por la LSSI: ¿Qué regula la Ley?

La Directiva 2000/31/CE sobre el Comercio Electrónico impone una serie de ámbitos que los estados miembros de la Unión Europea deben regular a través de las normas de transposición de la misma. La LSSI, como ley de transposición al ordenamiento jurídico español de la citada directiva, aborda en su articulado principalmente dichos ámbitos aunque, sorprendentemente, aborda otros que no estaban previstos ni incluidos en los borradores de anteproyecto preliminares.

En cuanto a los ámbitos señalados por la directiva, la LSSI regula los siguientes:

a) Régimen de establecimiento e información de los prestadores de servicios de la Sociedad de la Información, que se aborda en el Capítulo I del Título II y en los artículos 9 y 10 de la LSSI.

b) Régimen de las Comunicaciones Comerciales por vía Electrónica, que se regula en el Título III de la LSSI con una solución sorprendente como luego veremos.

c) Régimen de la Contratación por vía Electrónica, abordado en el Título IV de la LSSI así como en la Disposición Adicional Cuarta que realiza una importante modificación de los artículos 1.262 y 54 del Código Civil y del Código de Comercio, respectivamente.

d) Régimen de Responsabilidad de los prestadores de servicios intermediarios, el cual se desarrolla exclusivamente en la Sección 2ª del Capítulo II del Título II de la LSSI, añadiéndose, como veremos, nuevas categorías de prestadores intermediarios .

e) Dentro ya del apartado de la aplicación de la normativa, encontramos los Códigos de Conducta para los Servicios de la Sociedad de la Información y el Comercio Electrónico, fomentados igualmente por la Directiva y regulados en el Capítulo III del Título II de la LSSI.

f) Solución Extrajudicial de Conflictos surgidos en este ámbito, abordada en el Capítulo II del Título V y la Disposición Adicional Tercera de la LSSI.

g) Solución Judicial de Conflictos, viene incluida en el Capítulo I del Título V de la LSSI a través de la regulación de la acción de cesación para las conductas contrarias a la Ley que lesionen intereses colectivos o difusos que, a su vez, transpone parcialmente la Directiva 98/27/CE, de 19 de mayo de 1998, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores.

h) Información, Cooperación y Control de las Administraciones Públicas, viene recogido en el Título VI de la LSSI con importantes novedades respecto a la Directiva y

i) Régimen Sancionador, desarrollado amplia y severamente en el Título VII de la LSSI.

Por otro lado, en cuanto a los ámbitos no incluidos en la Directiva, pero los cuales el legislador ha decidido incluir en la LSSI con importantes consecuencias, destacan los siguientes:

j) Obligaciones de colaboración y de retención de datos del tráfico electrónico de los prestadores de servicios intermediarios, contempladas en los artículos 11 y 12 de la LSSI, respectivamente.

k) Principios inspiradores del sistema de asignación de nombres de dominio bajo el código de país correspondiente a España ".es" y regulación de la tasa para dicha asignación, regulados respectivamente en la Disposición Adicional Sexta y en la Disposición Final Segunda de la LSSI y

l) Configuración del acceso a Internet como un verdadero servicio universal, modificando al efecto el artículo 37 y la Disposición Transitoria Duodécima de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones a través de las Disposiciones Adicionales Primera y Tercera de la propia LSSI.

3.2.- Deber de información del empresario en su página Web

Es el fin del anonimato en Internet. Esto podríamos interpretarlo negativamente si nos refiriéramos a los usuarios de la Red pero, afortunadamente, aludimos exclusivamente a los prestadores de servicios en este medio. Es decir, se pretende acabar con las páginas Web comerciales no identificadas, cuyo propietario no aparece en ningún sitio y los datos de contacto son, en el mejor de los casos, una mera dirección de e-mail o un mero formulario sin más información sobre su destinatario.

Una vez más, la LSSI contribuye en este caso a dotar de una mayor seguridad jurídica a la Red al obligar a los empresarios a identificarse plenamente en su sitio Web.

Y ¿cuál es la información concreta que deben facilitar? En concreto, el artículo 10 de la LSSI dispone que, como mínimo, se deberá incluir (de una manera permanente, fácil, directa y gratuita) la siguiente:

a) El nombre o denominación social, dirección física, e-mail y otros datos de contacto.

b) Datos de inscripción en el Registro Mercantil u otro competente.

c) Datos de la autorización administrativa para la actividad, caso de ser necesaria.

d) En el caso de profesiones reguladas:

1º - Los datos del Colegio profesional al y número de colegiado.

2º - Datos de expedición u homologación del título académico.

3º - Las normas profesionales aplicables.

e) El número de identificación fiscal.

f) Los precios de los productos o servicios, incluyendo datos sobre impuestos y gastos de transporte aplicables (en su caso).

g) Los códigos de conducta a los que se esté adherido (en su caso).

Esta información es trascendental para el usuario ya que podrá identificar plenamente a la entidad que está detrás de la "fachada virtual" que representa la Web y saber dónde está ubicada, para así poder valorar el riesgo que asume al comprar sus productos o contratar sus servicios y, en su caso, saber contra quién dirigirse en caso de problemas.

3.3.- Responsabilidad de Prestadores Intermediarios: operadores, ISPs, buscadores, links, etc.

Por otro lado, una de las cuestiones más debatidas en los últimos tiempos es el problema de los contenidos ilícitos o nocivos de Internet. El hecho de que podamos encontrar páginas Web que describan con todo detalle cómo fabricar bombas caseras o que hagan apología de ideas xenófobas, es algo que inquieta enormemente a la opinión pública y a los distintos gobiernos.

A nivel internacional, este problema se ha abordado de muy distintas maneras por lo estados: desde la más restrictiva de prohibir totalmente el acceso a la Red (como el caso de Libia o Corea del Norte) o de censurar los contenidos (como el caso de China) hasta la más flexible de permitir una libertad total de expresión en Internet, como es el caso de los Estados Unidos.

Si bien es cierto que en éste último país hubo un intento de "censurar" la Red a nivel federal, a través de la aprobación de la llamada Decency Act (o Ley de Decencia) de 1996, mediante la cual se intentaban eliminar los contenidos ilícitos o inmorales de Internet, finalmente esta norma fue declarada inconstitucional y anulada por el Tribunal Supremo por entender que atentaba contra la libertad de expresión de los ciudadanos.

En la Unión Europea, esta cuestión ha sido regulada por la Directiva 2000/31/CE, de 8 de junio, sobre el Comercio Electrónico que en España ha sido transpuesta por la LSSI. Esta normativa intenta adoptar una postura intermedia, es decir, se rechaza cualquier tipo de censura previa de los contenidos de Internet pero se le atribuye al estado la posibilidad de controlar e incluso limitar dichos contenidos a posteriori si los mismos atentan contra principios tales como el Orden Público, la defensa nacional, la salud pública, la dignidad humana o la protección de la infancia.

En estos casos, el artículo 13 y siguientes de la LSSI atribuye la responsabilidad, ya sea civil o penal, de dichos contenidos ilícitos o nocivos a los sujetos que hayan desarrollado, introducido o referenciado activamente dichos datos en la Red, excluyendo a los prestadores de servicios intermediarios que únicamente les hayan dado cauce para su propagación sin conocer su naturaleza. Así, ni los operadores de redes, ni los proveedores de acceso a Internet, ni tampoco los alojadores de páginas Web van a ser responsables por aquellos contenidos que canalizan o almacenan si no han sido originados o modificados por ellos, aunque sí, obviamente, sus clientes que sí lo han hecho. Sin embargo, se les puede hacer responsables de dichos contenidos si no los retiran o impiden el acceso a los mismos cuando tengan conocimiento efectivo de su condición ilícita o de una resolución que ordene su retirada.

Como novedad de última hora, la Ley española ha incluido también a los sujetos que tengan enlaces o links a páginas con dichos contenidos o a los buscadores que los tengan indexados, los cuales pueden ser igualmente responsables sino eliminan dichos accesos en las condiciones anteriores. Esto puede dar lugar a muchos problemas en la práctica. En particular con aquellos buscadores o páginas con miles de enlaces que pueden ser incluso introducidos por terceros o por programas automáticos de rastreo, lo cual dificulta el control de los mismos por el prestador.

3.4.- Publicidad en Internet: el SPAM

No hay duda de que el llamado SPAM, o correo electrónico de publicidad no solicitada, es uno de los mayores problemas de la Red en los últimos tiempos.

Para atajar este problema desde un punto de vista legal, la LSSI prohíbe expresamente esta práctica en su artículo 21. Dicho artículo, dispone que no se podrán enviar comunicaciones comerciales por correo electrónico o medio equivalente a destinatarios que no lo hayan solicitado o autorizado expresa y previamente.

El incumplimiento de esta prohibición, se contempla como una infracción leve o grave, si hay habitualidad (más de tres envíos en un año), con sanciones de hasta 30.000 ó 150.000 euros, respectivamente.

Por otro lado, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) impone asimismo la obligación de solicitar el consentimiento de los destinatarios para poder incluir su dirección de e-mail en el fichero de publicidad de la empresa. Esta norma, por su parte, cataloga como infracción grave su incumplimiento con una sanción de hasta 300.000 euros.

Sin embargo, estas leyes se aplican solamente a empresarios radicados en España o, de modo similar, a los establecidos en la Unión Europea. ¿Y qué ocurre con el resto? Pues, por ejemplo, los medios norteamericanos, que no olvidemos son la mayoría en la Red, podrán seguir enviando SPAM y tratando datos personales sin ninguna limitación más de la que decidan auto imponerse vía códigos de conducta o políticas internas dado que no existe legislación restrictiva sobre la materia en los EE.UU. En definitiva, esta solución legal solo impedirá o paliará el SPAM “local” pero no el que nos viene de fuera, para ello habrá que esperar al desarrollo de un normativa internacional que lo regule.

¿Y cómo debe cumplir esta legislación el empresario español para evitar ser sancionado? Pues, nuestro consejo es que se dirija uno por uno a todos los destinatarios de correos electrónicos publicitarios que figuren en su base de datos y les solicite su consentimiento expreso para poder seguir enviándole comunicaciones comerciales por este medio y no se incluya a ningún otro nuevo sin haber cumplido este requisito. Esto sólo es aplicable si dichos destinatarios no lo habían solicitado o autorizado expresamente en el pasado.

Es importante destacar que sólo se cumple la normativa si obtenemos una “respuesta expresa” de los destinatarios autorizando el envío, esto es por ejemplo: que nos envíen un correo electrónico de vuelta manifestando su conformidad. Tanto los destinatarios que se

nieguen como los que no contesten, deben ser eliminados sin dilación de la base de datos de publicidad y no se les podrá dirigir ningún correo electrónico de este tipo en el futuro. Esto, sin duda, disminuirá significativamente el número de destinatarios de nuestra publicidad pero, por contra, aumentará su calidad y nos evitará posibles sanciones en el futuro.

3.5.- Contratación Electrónica: proceso de contratación en Web

En los anteriores epígrafes tuvimos oportunidad de analizar distintos aspectos más o menos polémicos de la LSSI. Sin embargo, podemos decir sin lugar a dudas que unos de los aspectos más positivos de la Ley se refiere a lo dispuesto en materia de contratos electrónicos.

En efecto, la LSSI reconoce la plena validez jurídica de los contratos celebrados por vía electrónica y no sólo se queda ahí ya que, además, en el apartado 3 de su artículo 23 equipara los mismos al "contrato escrito" por lo que, siempre que la ley exija que un contrato conste por escrito (p. ej. determinados contratos de trabajo) será suficiente con que se celebre por medios telemáticos.

Este reconocimiento tiene una gran trascendencia ya que, desde la aprobación de esta Ley, podemos realizar todo tipo de operaciones a través de Internet y con pleno reconocimiento jurídico: desde comprar un coche o alquilar un apartamento hasta pedir un préstamo o contratar a un empleado. De hecho, la LSSI sólo señala dos excepciones donde los contratos electrónicos no son admisibles:

1) Los contratos referidos al Derecho de Familia y Sucesiones, es decir, no podremos hacer testamento ni capitulaciones matrimoniales a través de Internet y

2) Todas aquellas operaciones que exijan la intervención de un notario o corredor de comercio y el otorgamiento de una escritura o documento público.

En cuanto a este último caso, y poniendo un ejemplo claro: podremos incluso comprar una casa a través de Internet, con plena validez jurídica, ahora si queremos inscribir dicha adquisición en el Registro de la Propiedad entonces deberemos acudir además al notario para dar fe pública del contrato electrónico celebrado.

4.- La problemática de las transacciones con tarjetas en el comercio electrónico

Generalmente, se suele dictaminar que uno de los principales factores que frenan el desarrollo del comercio electrónico es el miedo de los consumidores a facilitar los datos de su

tarjeta de crédito o de débito a través de Internet. Por ello, existe la creencia de que el consumidor está más desprotegido en la Red que el propio ciber-empresario.

Sin embargo, la realidad es justamente la contraria:

El artículo 46 de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista dispone que "cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, su titular podrá exigir la inmediata anulación del cargo". Esto significa que el consumidor siempre podrá solicitar que se le devuelvan pagos no reconocidos cargados a su tarjeta y simplemente con una mera comunicación al banco. La protección aquí es total.

Por el contrario, en lo que se refiere al empresario, cuando realiza una venta con tarjeta en el "mundo físico" (léase no electrónico) le da a firmar al cliente un justificante de la transacción. Sin embargo, en el "mundo virtual" (léase en Internet) no existe este trámite ya que simplemente el cliente introduce los datos de la tarjeta y se realiza automáticamente la transacción.

De este modo, si un cliente rechaza un pago realizado con tarjeta el empresario "no virtual" siempre puede presentar el justificante firmado como prueba de que el mismo sí realizó la compra, dejando sin efecto la devolución del pago pero, en el comercio electrónico, el ciber-empresario no podrá presentar dicha prueba y deberá asistir cuasi-impotente a la devolución de dicho pago.

Por tanto, el ciber-empresario es el que está verdaderamente desprotegido en las compras electrónicas con tarjeta y no así el consumidor.

Ante esta situación, ¿cómo puede protegerse el ciber-empresario? Pues, además de intentar hacer acopio de otros medios probatorios que demuestren la compra efectiva por parte del cliente (por ejemplo: firma de albaranes de entrega, etc.) lo deseable sería la utilización de la firma electrónica en este tipo de transacciones la cual permitiría su prueba de modo equivalente al papel. Sin embargo, desgraciadamente aún estamos lejos de la popularización de este sistema en el comercio electrónico.

5.- Reconocimiento legal de la Firma Electrónica

Estamos demasiado acostumbrados a la tinta y al papel. Parece que sólo existe un contrato si se recoge en una serie de hojas firmadas y, a ser posible, matasselladas (y, por qué no, en papel timbrado).

Nada más lejos de la realidad jurídica. Todos los días celebramos decenas de contratos sin casi darnos cuenta: cuando compramos el periódico, tomamos un café, cogemos el autobús o vamos al cine. En todas estas situaciones estamos celebrando contratos “no escritos” que, sin embargo, son válidos desde un punto de vista legal. De hecho, si el periódico está mal impreso o el café está frío, podemos reclamar su restitución o la devolución del dinero al kiosco o al camarero incluso por vía judicial.

A pesar de ello, en muchas situaciones es conveniente, o incluso necesario, que haya un documento escrito, bien por la cuantía o importancia del asunto o bien por exigencia legal. Ahora bien, incluso aquí “escrito” no es sinónimo de “en papel”.

Prueba de ello es el Real Decreto-Ley 14/1999, de 17 de septiembre, por el que se regula la Firma Electrónica, recientemente sustituida por la Ley 59/2003 de Firma Electrónica. Con esta normativa, España se convirtió en uno de los primeros países en reconocer legalmente la validez de un documento firmado digitalmente. Además, el mismo es incluso más seguro y fiable como prueba ya que la firma electrónica no sólo indica “quién firma” sino también “lo que firma" ya que se vincula al propio texto del documento (lo cual en papel es imposible).

De acuerdo entonces: la firma electrónica existe jurídicamente desde 1999 en nuestro país y es útil. Ahora bien, ¿se utiliza en la práctica? Desgraciadamente no lo que sería deseable.

Sin embargo, hay una honrosa excepción: la declaración de impuestos a través de Internet es un exitoso ejemplo de la implantación y utilidad de la firma electrónica. Lamentablemente, no ha cundido demasiado en el ámbito privado y, por ello, el Gobierno ha efectuado una importante reforma, con la nueva Ley 59/2003 de Firma Electrónica, que contempla la creación del DNI digital, el cual supondrá la generalización de la tenencia (no se sabe si del uso) de la firma electrónica en nuestro país.

Si esta iniciativa tiene éxito, contribuirá a dotar de una mayor seguridad jurídica al Comercio Electrónico y a que finalmente “cambiemos el chip” y confiemos al menos tanto en la realidad digital como en la física (sino más).

6.- El uso del correo electrónico en el ámbito laboral

Una de las cuestiones que más problemas han suscitado en el ámbito del Derecho de las nuevas tecnologías es el del uso del correo electrónico en el puesto de trabajo. La cuestión es la siguiente: ¿Quién es el dueño del e-mail profesional: el empresario o el trabajador? O, dicho

de otro modo, ¿Tiene el empresario derecho a leer los mensajes de sus empleados por el mero hecho de facilitarle la cuenta de correo electrónico?

El artículo 18 de la Constitución reconoce el derecho a la intimidad de las personas que protege tanto sus comunicaciones como su correspondencia de injerencias ajenas sin el consentimiento de su titular o sin una orden judicial. Asimismo, el artículo 197 del Código Penal tipifica como delito el hecho de acceder al contenido de mensajes de correo electrónico ajenos, castigado con hasta 4 años de prisión.

Cierta confusión sembró la Sentencia del Tribunal Superior de Justicia de Cataluña nº 9382/2000, de 14 de Noviembre de 2000, destapó la caja de los truenos al declarar la procedencia del despido de un trabajador del Deutsche Bank con base en el contenido de sus correos electrónicos intervenidos por el empresario. Sin embargo, el trabajador despedido, convenientemente asesorado, se querelló posteriormente contra sus antiguos jefes acusándolos del citado delito, estando el asunto pendiente de sentencia.

Por tanto, ¿qué se puede hacer para garantizar el control del empresario sobre sus medios de producción sin vulnerar los derechos fundamentales del trabajador?

Conviene advertir que no es suficiente con que simplemente se advierta del correo electrónico de la empresa es para uso exclusivamente profesional o que se anuncien las monitorizaciones como la política de seguridad. Para poder acceder al contenido de los mensajes, se hace necesario solicitar el consentimiento previo y expreso del trabajador: bien añadiendo una cláusula específica en el contrato de trabajo o bien recabando la firma del trabajador en documento aparte.

Sin este consentimiento, el empresario deberá abstenerse de controlar el correo más allá de la mera comprobación de virus o, en su caso, de los destinatarios o emisores del mismo.

- **EMPRESAS AUTORAS DE ESTE MANUAL**

Acens Technologies

http://www.acens.es

Going Investment

http://www.going.es

ESA Security

http://www.esa-security.com

http://www.movistar.com

Pintos & Salgado Abogados

http://www.pintos-salgado.com

Secuware

http://www.secuware.com

Sentryware

http://www.sentryware.com

TB Security

http://www.tb-security.com

Trend Micro España

http://es.trendmicro-europe.com

Esta publicación ha sido patrocinada por la Comunidad de Madrid

Asociación Nacional de Empresas de Internet, ANEI
http://www.a-nei.org

Dirección de proyecto:
Joaquín Mouriz
Director de Comunicación y RRPP

Madrid, a 21 de abril de 2006