LA IMPORTANCIA DEL FACTOR HUMANO EN LA SEGURIDAD INFORMÁTICA

Alvaro Gómez Vieites
agomezvieites@gmail.com
Profesor de la Escuela de Negocios Caixanova

RESUMEN DE LA PONENCIA

La implantación de unas adecuadas medidas de Seguridad Informática exige contemplar aspectos técnicos (antivirus, cortafuegos, IDS...), organizativos (planes y procedimientos) y legales (cumplimiento de la legislación vigentes sobre protección de datos, uso de la firma electrónica, propiedad intelectual, etc.). No obstante en muchas ocasiones se presta muy poca atención a la importancia del factor humano en la seguridad informática.

Además, hay que tener en cuenta que una empresa u organización puede ser responsable subsidiara por los actos de sus empleados, que en nuestro país pueden acarrear importantes sanciones económicas, teniendo en cuenta la legislación vigente (LOPD, LSSI-CE, Código Penal...).

Por otra parte, en estos últimos años se han incrementado de forma significativa los conflictos legales sobre la debida utilización de Internet y el correo electrónico y, a falta de una clara normativa, se han dictado sentencias a favor de unos y otros, empresarios y trabajadores, avalando en unos casos despidos por abuso de Internet y rechazándolos en otros.

Por todo ello, la implantación de un Sistema de Gestión de Seguridad de la Información debería contemplar el factor humano como uno de sus elementos clave, contemplando aspectos como la adecuada formación y sensibilización de los empleados, la implicación de los responsables y directivos, la aprobación de un Reglamento Interno sobre el uso de la Informática e Internet en la organización, etc., cuestiones que se analizarán con detalle en esta ponencia.

1. LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Nadie cuestiona hoy en día la importancia adquirida por la Seguridad Informática y la Protección de Datos en el ámbito de las organizaciones. La progresiva informatización de los procesos administrativos y de negocio, el despliegue de redes privadas de datos y el desarrollo de nuevos servicios on-line a través de Internet son algunos de los factores que explican la creciente preocupación por mejorar la seguridad en los Sistemas de Información y en la conexión corporativa a Internet.

Podríamos entender dentro del contexto general de la Seguridad de la Información a cualquier medida adoptada por una organización que trate de evitar que se ejecuten operaciones no deseadas ni autorizadas sobre un sistema o red informática, cuyos efectos puedan:

- Conllevar daños sobre la información.
- Comprometer la confidencialidad.
- Disminuir el rendimiento.
- Bloquear el acceso de usuarios autorizados al sistema.

Por su parte, la norma ISO/IEC 17799 define la Seguridad de la Información en un sentido amplio como la "*preservación de su confidencialidad, su integridad y su disponibilidad*".

La información constituye un recurso que en muchos casos no se valora adecuadamente por su intangibilidad (cosa que no ocurre con los equipos informáticos, la documentación o las aplicaciones) y, además, las medidas de seguridad no influyen en la productividad del sistema, sino, más bien, al contrario, podrían disminuir su rendimiento (los filtros de los cortafuegos y antivirus, las copias de seguridad, los registros de la actividad de los usuarios y de las

aplicaciones, etc. consumen recursos en los distintos sistemas donde son implantados) e incrementar los gastos necesarios para su explotación y mantenimiento, por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.

Sin embargo, en la actualidad el negocio y el desarrollo de las actividades de muchas organizaciones dependen de los datos e información registrados en su sistema, así como del soporte adecuado de las TICs para facilitar su almacenamiento, procesamiento y distribución.

Por todo ello, es necesario trasladar a los directivos la importancia de valorar y proteger la información de sus empresas. Según un estudio realizado por la Asociación Española para la Dirección Informática (AEDI) en mayo de 2002, el 72 % de las empresas españolas quebraría en 4 días si perdiera los datos guardados en sus ordenadores. Está claro que la eliminación de todas las transacciones de un día en una empresa podría ocasionarle más pérdidas económicas que sufrir un robo o un acto de sabotaje contra alguna de sus instalaciones.

Con la proliferación de las redes de ordenadores, la información de las empresas ha pasado de concentrarse en los grandes sistemas (sistemas centralizados) a distribuirse por los ordenadores y servidores ubicados en los distintos departamentos y grupos de trabajo. Por este motivo, en la actualidad, muchas organizaciones no conocen con precisión toda la información que hay en los puestos de trabajo (generalmente, ordenadores personales de la propia organización), ni los riesgos que tienen de sufrir ataques u otro tipo de desastres, ni cómo la propia organización utiliza esa información.

A la hora de analizar las posibles consecuencias de la falta de seguridad de la información, el impacto total para una organización puede resultar bastante difícil de evaluar, ya que además de los posibles daños ocasionados a la información guardada y a los equipos y dispositivos de red, deberíamos tener en cuenta otros importantes aspectos:

- Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes.
- Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos.
- Posible impacto negativo en la imagen de la empresa ante terceros.
- Robo de información confidencial: revelación de fórmulas, diseños de productos, estrategias comerciales…
- Retrasos en los procesos de producción, pérdida de pedidos, deterioro en la calidad del servicio a los clientes...
- Posibles indemnizaciones derivadas de las responsabilidades legales, sanciones administrativas.
- Etc.

Las organizaciones que no adoptan medidas de seguridad adecuadas para proteger sus redes y sistemas informáticos podrían enfrentarse a penas civiles y criminales bajo una serie de leyes existentes en distintos países.

Así, por ejemplo, el entorno legal que ha entrado en vigor en estos últimos años en nuestro país en materia de Protección de Datos de Carácter Personal (LOPD) y Prestación de Servicios de la Sociedad de la Información (LSSI) plantea nuevos retos técnicos y organizativos para los responsables de la Seguridad de la Información.

La Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD) obliga a la implantación de importantes medidas de seguridad informática a las empresas que hayan creado ficheros con datos personales. Sin embargo, la mayoría de las empresas todavía incumplen muchas de estas obligaciones, por lo que se exponen a importantes multas (las más elevadas de la Unión Europea), que podrían alcanzar los 600.000 euros para las infracciones consideradas como muy graves.

2. EL FACTOR HUMANO EN LA SEGURIDAD DE LA INFORMACIÓN

La implantación de unas adecuadas medidas de Seguridad de la Información exige contemplar aspectos técnicos (antivirus, cortafuegos, IDS...), organizativos (planes y procedimientos) y legales (cumplimiento de la legislación vigentes sobre protección de datos, uso de la firma electrónica, propiedad intelectual, etc.). No obstante, en muchas ocasiones se presta muy poca atención a la importancia del factor humano en la seguridad informática.

Según varios estudios publicados, más del 75 % de los problemas inherentes a la seguridad se producen por fallos en la configuración

de los equipos o por un mal uso por parte del personal de la propia organización.

Además, hay que tener en cuenta que una empresa u organización puede ser responsable subsidiara por los actos de sus empleados, que en nuestro país pueden acarrear importantes sanciones económicas, teniendo en cuenta la legislación vigente (LOPD, LSSI-CE, Código Penal...):

- Envíos de comunicaciones comerciales no solicitadas (*spam*), que puede acarrear una multa de hasta 150.000 euros, al incumplir la LSSI-CE.
- Cesiones no autorizadas de datos de carácter personal, con multas de hasta 600.000 euros, al incumplir con los preceptos de la LOPD.
- Delitos contra la propiedad intelectual, si se instalan y utilizan programas de intercambio de ficheros P2P (como Kazaa, e-Mule...).
- Delitos informáticos como el ataque a otros equipos desde la propia red de la empresa, realización de estafas electrónicas...
- Descarga de herramientas de hacking, acceso a pornografía o a contenidos ilegales en el país (Websites racistas o de grupos xenófobos o terroristas).
- Envío a terceros de información confidencial de la empresa.

Los principales expertos en materia de Seguridad Informática ya nos han alertado estos últimos años sobre la necesidad de contemplar el factor humano como uno de los más importantes a la hora de implantar un Sistema de Gestión de Seguridad de la Información.

Así, en palabras de Kevin Mitnick, uno de los hackers más famosos de la historia, "*usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es una llamada a un empleado desprevenido e ingresan sin más. Tienen todo en sus manos.*".

El propio experto en criptografía y seguridad Bruce Scheneir llegaba a afirmar en uno de sus últimos libros, *Secrets and Lies* (Verdades y Mentiras) que "*...si piensas que la tecnología puede resolver tus problemas de seguridad, entonces no entiendes el problema y no entiendes la tecnología*".

Por otra parte, en estos últimos años se han incrementado de forma significativa los conflictos legales sobre la debida utilización de Internet y el correo electrónico y, a falta de una clara normativa, se han dictado sentencias a favor de unos y otros, empresarios y trabajadores, avalando en unos casos despidos por abuso de Internet y rechazándolos en otros.

Por todo ello, la implantación de un Sistema de Gestión de Seguridad de la Información debería considerar el factor humano como uno de sus elementos clave, contemplando aspectos como la adecuada formación y sensibilización de los empleados, la implicación de los responsables y directivos, la aprobación de un Reglamento Interno sobre el uso de la Informática e Internet en la organización, etc.

3. FUNCIONES Y RESPONSABILIDADES DE LOS EMPLEADOS Y DIRECTIVOS

Las funciones y obligaciones de cada una de las distintas personas que tienen acceso a los datos y a los servicios del Sistema de Información de una organización deberían estar claramente definidas.

Asimismo, la organización debería adoptar las medidas necesarias para que estas personas conozcan las normas de seguridad que afecten al desarrollo de sus funciones y obligaciones respecto a la utilización de los servicios y herramientas informáticas y su acatamiento a las mismas, así como las consecuencias en que pudiera incurrir cada usuario en caso de incumplimiento.

Debemos tener en cuenta que estas medidas afectan a los distintos colectivos que pueden tener acceso a los servicios del Sistema de Información de la organización:

- Administradores de la red informática.
- Desarrolladores de aplicaciones.
- Técnicos responsables del mantenimiento de los equipos y de la red informática.
- Usuarios finales del sistema.
- Directivos.
- Personal externo: empresas de servicios que tienen acceso a los recursos informáticos de la organización.

- Etc.

Por todo ello, sería recomendable que la organización elaborase un Reglamento Interno sobre Seguridad Informática, Utilización de Internet y Protección de Datos de Carácter Personal, que tendría su base jurídica en el entorno normativo existente en España y la Unión Europea: la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD); 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; la Ley de Servicios de la Sociedad de la Información (LSSI); el nuevo Código Penal, que contempla nuevos tipos de delitos informáticos y contra la propiedad intelectual; la Ley General de Telecomunicaciones (LGT); etc.

Este Reglamento Interno debería ser consensuado con los representantes de los empleados y el Departamento de Recursos Humanos de la organización, estar autorizado por la Dirección y divulgado entre los empleados con acceso a los recursos informáticos.

Cada usuario del sistema debería conocer y aceptar estas normas, haciéndose responsable de los daños y perjuicios que pudiera causar debido a su falta de cumplimiento diligente. Asimismo, se deberían dar a conocer cuáles serían las medidas disciplinarias adoptadas por la organización en caso de incumplimiento.

Por supuesto, todas estas normas deberían ser transmitidas con total transparencia a las personas que se incorporan a la organización y que puedan tener acceso a sus recursos informáticos.

Asimismo, los empleados con acceso a datos sensibles deberían firmar en sus contratos cláusulas de confidencialidad y de cumplimiento de determinadas normas básicas de seguridad informática y en materia de protección de datos de carácter personal.

El personal afectado por esta normativa se podría clasificar en dos grandes categorías:

1. Administradores del sistema, analistas, programadores y técnicos informáticos, que se encargan de administrar o mantener el entorno del sistema informático y de las aplicaciones de gestión, así como del desarrollo de nuevas herramientas y aplicaciones. Este personal puede utilizar herramientas de administración que permitan el acceso a los datos protegidos, servicios y aplicaciones, saltándose las barreras de acceso de las aplicaciones o del sistema operativo.
2. Usuarios básicos del sistema informático y de las aplicaciones de gestión que pueden tener acceso a los ficheros con datos y a los servicios ofrecidos por la red informática de la organización.

Dentro del primer grupo, los administradores de la red informática y de los sistemas operativos dispondrán de los máximos privilegios y, por tanto, tendrán acceso a todas las aplicaciones y herramientas del sistema informático, así como a los ficheros o bases de datos necesarios para resolver los problemas que surjan. Para reducir el riesgo de que una actuación errónea pueda afectar a la seguridad del sistema, sólo deberían utilizar una cuenta de administrador con los máximos privilegios cuando sea necesario para ejercer sus funciones como tales, empleando una cuenta de un usuario básico del sistema en las restantes ocasiones en que se encuentren trabajando dentro de la red informática de la organización.

Por otra parte, las actuaciones de los analistas, programadores y técnicos de operación y mantenimiento se tendrían que limitar a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deberían, en principio, tener acceso directo a los datos de los ficheros, siempre y cuando su actuación no precise de dicho acceso.

La normativa aprobada por la organización se encargaría, por lo tanto, de regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad o del entorno de red, de forma que se prohibiese expresamente el acceso no autorizado a los ficheros con datos sensibles o a determinados servicios o aplicaciones, sin pasar por los procedimientos de control de acceso con los que puedan contar las aplicaciones. Por ello, ninguna herramienta o programa de utilidad que permita el acceso directo a los ficheros y bases de datos, como los editores universales, analizadores de ficheros, *sniffers*, editores de consultas (‘*queries*’) en gestores de bases de datos, etc., deberían ser accesibles a ningún usuario o administrador no autorizado.

Por otra parte, todos los usuarios del sistema informático tendrían que aplicar ciertas normas prácticas de seguridad relativas al mane-

jo de los equipos y aplicaciones a las que pueden tener acceso. Seguidamente se presentan, a modo de ejemplo, algunas de las cuestiones a tener en cuenta en esta normativa para los usuarios finales del sistema:

- Cada equipo informático asignado a un puesto de trabajo estará bajo la responsabilidad de uno de los usuarios autorizados en el sistema informático de la organización. Este usuario deberá garantizar que la información que muestra no pueda ser vista por personas no autorizadas. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.
- Antes de abandonar el equipo del puesto de trabajo, ya sea temporalmente o bien al finalizar su turno de trabajo, deberá cancelar todas las sesiones activas y conexiones con los servidores de la red corporativa.
- Utilizar un salvapantallas protegido con contraseña para bloquear su equipo ante una ausencia del puesto de trabajo, aunque sea breve, de tal modo que impida la visualización de los datos protegidos.
- Impedir que otros usuarios puedan utilizar su identidad (nombre de usuario y contraseña) para acceder al sistema. Para ello, deberán responsabilizarse de guardar a buen recaudo su contraseña de acceso al sistema.
- No introducir CD-ROM, disquetes u otros soportes en los equipos sin la comprobación previa de que no contienen riesgos de ninguna clase (estén dañados, contengan virus, etc).
- No se cambiará la configuración del equipo ni se intentarán solucionar problemas de funcionamiento. En caso de mal funcionamiento, el usuario deberá comunicárselo a la persona encargada.
- Sólo se utilizarán las herramientas corporativas, quedando prohibida la instalación de software en los PC de la empresa que no haya sido expresamente autorizado por el responsable de la seguridad del sistema.
- No se podrán realizar copias de bases de datos o documentos clasificados como confidenciales o que contengan datos personales en soportes externos sin la previa autorización expresa del responsable de seguridad del sistema.
- Los disquetes y documentos con información sensible o confidencial se deberán guardar en armarios o cajones bajo llave, evitando que por descuido puedan dejarse encima de las mesas de trabajo u otros lugares sin la adecuada protección.
- En el caso de las impresoras los usuarios deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de carácter personal, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
- Deberá informarse de cualquier incidencia que pudiera afectar a la seguridad de la red informática o el sistema de información
- Los equipos y medios informáticos de la organización no pueden ser sacados fuera de ésta sin la correspondiente autorización
- Se limitará el acceso a Internet solamente a fines profesionales[1], compatible con las funciones propias del puesto de trabajo, prohibiéndose actividades de Internet ajenas a dicho fin. Se prohíbe expresamente la visita de páginas de contenido ajeno a la actividad de la organización, la descarga e intercambio de ficheros digitales (música, vídeos, libros) que puedan vulnerar la propiedad intelectual, la participación en chats o en foros de contenido general, o la utilización del correo electrónico para fines particulares.

[1] Se trata de una medida propuesta a modo de ejemplo, si bien la organización podría considerar conveniente permitir el acceso limitado a Internet para ciertos usos privados no relacionados con la actividad profesional del usuario.

4. EL CONTROL Y SUPERVISIÓN DE LOS EMPLEADOS

Según un estudio realizado por la organización estadounidense Fundación por la Privacidad, más de un tercio de los trabajadores americanos que disponen en su lugar de trabajo de acceso a Internet están siendo controlados por sus jefes.

De hecho, en algunos países el abuso o mal uso de Internet se ha convertido en una de las principales causas de despido. Según un estudio de la revista "Personnel Today" publicado en julio de 2002, cerca del 70 % de las empresas británicas de más de 2.500 empleados habían despedido a alguna persona por perder el tiempo navegando por la Red o accediendo a páginas de contenido pornográfico.

Por otra parte, en agosto de 2004 el diario británico "The Sun" informaba que cientos de funcionarios británicos habían sido sancionados por haber consultado páginas pornográficas, incluyendo imágenes de carácter pedófilo, en sus ordenadores. Como ejemplo, el diario citaba a los empleados del Servicio de Jubilaciones y Trabajo, que consultaron más de dos millones de páginas de pornografía en tan sólo ocho meses (desde diciembre de 2003). Un control de los ordenadores permitió identificar a los culpables. Uno de ellos fue condenado por la justicia, mientras que dieciséis perdieron su empleo, otros tres renunciaron y 221 fueron sancionados por mala conducta

En Galicia, el Gobierno de la Xunta anunciaba en noviembre de 2004 que eliminaría el acceso a Websites "sensibles" y las descargas P2P desde sus ordenadores. La Consellería de Presidencia de la Xunta de Galicia tiene previsto adoptar medidas para promover el "uso racional" de Internet desde las oficinas de la Administración Autonómica, con el fin de maximizar la eficacia de este servicio y garantizar una mejor atención al ciudadano. De hecho, en un informe publicado en noviembre de 2004 y en el que se analizaba el uso de Internet desde las 2.700 oficinas de la Administración gallega (incluyendo hospitales, ambulatorios y organismos autónomos) que disponen de conexión a la red, con más de 90.000 usuarios, se señalaba que hasta el 39,8 % de tráfico registrado en el pasado mes de junio de 2004 entre todas las Consellerías de la Xunta fue considerado como "no productivo".

En definitiva, el uso indebido de Internet en el trabajo generó unas pérdidas de 16.520 millones de euros en 2003, según datos de la empresa de seguridad informática Internet Security Systems (ISS). Este estudio señala que entre el 30 y el 40 por ciento del uso de Internet en la empresa no está relacionado con la actividad laboral, y que dos de cada tres accesos a páginas pornográficas se realizan durante el horario de trabajo. Asimismo, según ISS, cada empleado envía una media de 5 correos electrónicos de carácter privado al día, y el 30 por ciento de los trabajadores ha enviado alguna vez, intencionadamente o por error, información corporativa confidencial a buzones externos. Como conclusión de su estudio, la empresa ISS considera que la utilización de herramientas de seguridad puede ayudar a las empresas a elevar la productividad de sus empleados, descongestionar su capacidad de almacenamiento y su ancho de banda, limitar la entrada de virus y la sustracción de información confidencial, y minimizar los riesgos de responsabilidad legal.

Por lo tanto, la implantación de la conexión a Internet en los puestos de trabajo está planteando nuevos problemas que afectan a las comunicaciones de los empleados, entre los que cabría destacar:

- La posibilidad de que el empresario pueda abrir el correo electrónico de un empleado.
- El acceso al ordenador de un trabajador y a sus archivos.
- La potestad para controlar el uso que los empleados hacen de Internet.
- La capacidad de los representantes sindicales para utilizar el correo electrónico para sus comunicaciones con los empleados.

Abusar del acceso a Internet y del correo electrónico desde el lugar del trabajo para fines distintos de los estrictamente profesionales puede tener consecuencias graves para los trabajadores. Esta es la tendencia de las últimas sentencias dadas a conocer en España, que consideraron procedente el despido de trabajadores que abusaron del uso de Internet en sus empresas (por ejemplo, por la consulta reiterada a sitios de ocio en Internet durante la jornada de trabajo y con el ordenador de la empresa).

Las empresas pueden implantar distintas herramientas que faciliten el control de accesos y la monitorización del uso de los servicios de Internet. Entre las principales funcionalidades contempladas por estas herramientas podríamos destacar las siguientes:

- Bloqueo de direcciones Web a las que se desee impedir el acceso: para ello se puede recurrir a una lista de páginas prohibidas y/o a una lista de páginas o direcciones permitidas. Asimismo, se podría contemplar la posibilidad de realizar una actualización periódica de estas listas a través de una empresa especializada que ofrezca este servicio a sus clientes.
- Asignación de permisos de acceso a los servicios de Internet en función de los diferentes perfiles de usuarios y del momento (día y hora) en que se produce la conexión. De esta forma, se podrían establecer franjas horarias e intervalos de acceso en función de los horarios de trabajo y de la disponibilidad de intervalos de tiempo libre durante la jornada laboral (descansos para el café o tiempo destinado a la comida, momentos en los que la organización podría facilitar el acceso a ciertos servicios o contenidos restringidos en otros momentos para que no interfieran con la actividad empresarial).
- Restricción de los servicios que se pueden utilizar en cada momento y por cada usuario (correo, chat, descarga e intercambio de ficheros...).
- Utilización de distintas tecnologías de Filtrado de Contenidos:
    - Localización y filtrado de páginas que incluyen determinadas palabras clave relacionadas con pornografía o contenidos considerados como ilícitos o problemáticos para la organización[2].
    - Análisis semántico, mediante herramientas de Inteligencia Artificial como Optenet (www.optenet.com) o Rulespace (www.rulespace.com).
- Otras funcionalidades: algunas de estas herramientas impiden el envío de datos sensibles (direcciones, tarjetas de crédito, ficheros con datos sensibles de la organización); permiten limitar el tiempo máximo de conexión de cada usuario o el ancho de banda consumido; etc...

Por otra parte, gracias a estas herramientas la empresa puede disponer de un completo registro de la actividad de los usuarios que utilizan los servicios de Internet: páginas Web visitadas; tipo y tamaño de los ficheros descargados; comandos FTP; cabeceras de los mensajes de correo electrónicos; tiempo dedicado a la utilización de estos servicios; ancho de banda consumido; etc.

Conviene destacar en este caso que la empresa debe preservar la privacidad de los usuarios, por lo que NO es recomendable registrar el contenido de los mensajes de correo o la información accedida dentro de cada página Web por cada usuario, limitándose a registrar el hecho de que se produce la utilización de dicho servicio.

También hay que tener en cuenta que las conexiones que utilizan protocolos seguros (basados en algoritmos criptográficos) como SSH, SSL o IPSec pueden eludir las funciones de registro de estas herramientas, por lo que la organización podría considerar la restricción en el uso de este tipo de conexiones por parte de determinados usuarios. Así, por ejemplo, un usuario podría establecer una conexión SSH (Secure Shell) con un servidor externo y descargar materiales o contenidos no autorizados por la organización, sin que esta actividad pudiera ser detectada por las herramientas de monitorización y control.

En el caso concreto del servicio de correo electrónico, algunas empresas han decidido facilitar dos cuentas de correo a sus empleados, una de uso estrictamente profesional, que podría ser intervenida por la empresa, y otra de uso personal. Conviene distinguir, además, entre el uso de la(s) cuenta(s) de correo de la empresa y la conexión desde la empresa a una cuenta de correo personal que el trabajador tenga abierta en un servidor de Internet, ya que en este último caso la empresa no podría acceder bajo ninguna circunstancia a los contenidos de los mensajes de correo del usuario.

No obstante, si se deciden implantar este tipo de herramientas de control y monitorización del acceso, la empresa debería advertir que el uso de Internet debe tener fines laborales, y dejar clara cuál es la política de utilización de este medio. Sin una advertencia previa por parte

[2] No obstante, se plantea un problema con estas tecnologías: según varios estudios realizados, muchos filtros "anti-porno" restringen el acceso a Websites con información sobre la salud.

de la empresa, podría crearse una expectativa de privacidad entre los empleados. Es decir, los trabajadores podrían argumentar "que nadie les avisó de que no podían usar Internet para fines personales".

Distintos expertos en materia laboral han destacado en los últimos años sobre el conflicto de derechos que se produce en estos casos. Frente al derecho del empresario a controlar el uso de los medios técnicos puestos a disposición de sus empleados, se encuentra el de éstos a su intimidad. El artículo 18 del Estatuto de los Trabajadores permite al empresario registrar los efectos personales del trabajador cuando considere que se están perjudicando su patrimonio o intereses. Los medios tecnológicos son titularidad de la empresa y ésta es la encargada de establecer los límites de su utilización.. No obstante, el control de estos medios debe conjugarse con el derecho a la intimidad y al secreto de las comunicaciones de los trabajadores.

Los principales argumentos a favor de la empresa que pueden justificar las medidas adoptadas para control y vigilar el uso de los servicios de Internet son los que se citan a continuación:

- Los medios tecnológicos son titularidad de la empresa, por lo que ésta es la encargada de establecer los límites de su utilización (facultad de organización de trabajo).
- El artículo 20.3. del Estatuto de los Trabajadores es el que reconoce y delimita las facultades de control y vigilancia, cuando establece que el empresario puede adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos en su caso.

Por otra parte, en la legislación también encontramos importantes argumentos (bastante más numerosos, por cierto) en defensa de los trabajadores:

- El artículo 4.2. del Estatuto de los Trabajadores establece "el derecho del trabajador al respeto de su intimidad y a la consideración debida a su dignidad".
- En el artículo 18 del Estatuto de los Trabajadores se afirma que "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. 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".
- La propia Constitución Española, en su artículo 18.3: "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".
- El artículo 197 del Código Penal equipara el correo electrónico a una carta (ha sido uno de los primeros de la Unión Europea en reflejarlo): "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." (artículo 197.1).
- El documento de la UE sobre vigilancia de las comunicaciones electrónicas en el lugar de trabajo, aprobado en mayo de 2002, afirma que el derecho a la intimidad del empleado es indiscutible, aunque se puede ver atenuado por motivos de seguridad de la empresa.

Por lo tanto, y como conclusión sobre esta delicada cuestión, podemos afirmar que corresponde en exclusiva a la empresa la autorización para navegar por Internet con fines privados. Además, la empresa puede bloquear el acceso a algunos Websites y a determinados servicios de Internet, así como comprobar el tiempo utilizado en la navegación y cuáles han sido los lugares visitados.

Pero para que la vigilancia sea legítima, ésta ha de ser necesaria, dirigida a un fin concreto, realizada de forma abierta y clara, según los principios de adecuación, pertinencia y proporcionalidad, y con las mínimas repercusiones sobre el derecho a la intimidad de los trabajadores.

5. FORMACIÓN DE LOS USUARIOS

En este último apartado de la ponencia se vuelve a incidir en la importancia de llevar a cabo acciones de formación y de sensibilización de forma periódica para mejorar y actualizar los conocimientos informáticos y en materia de seguridad de los empleados con acceso a los servicios y aplicaciones del Sistema de Información de la organización.

Asimismo, como complemento de dicha formación, y en cumplimiento de la legislación vigente en España (Ley Orgánica de Protección de Datos), la organización debería informar puntualmente a sus empleados con acceso al Sistema de Información de cuáles son sus obligaciones en materia de seguridad y protección de datos de carácter personal.

Por otra parte, también se debe contemplar una adecuada preparación de aquellas personas que se incorporen a la organización, sobre todo cuando pudieran tener acceso a datos sensibles y a determinados ficheros con datos de carácter personal.

Seguidamente se presenta una relación de temas a incluir en la formación básica sobre Seguridad Informática para los empleados de la organización:

- Utilización segura de las aplicaciones corporativas
- Utilización segura de los servicios autorizados de Internet: navegación por páginas Web evitando engaños y posibles contenidos dañinos; utilización de la firma electrónica y la criptografía en el correo electrónico para garantizar la autenticidad, integridad y confidencialidad de los mensajes sensibles; cómo llevar a cabo transacciones en servidores seguros; etc.
- Cómo evitar la entrada de virus y otros códigos dañinos: reconocimiento de mensajes falsos o con ficheros adjuntos sospechosos; protección a la hora de instalar herramienta o acceder a determinados servicios de Internet; etc.
- Reconocer las técnicas más frecuentes de Ingeniería Social[3], para evitar ser víctimas de este tipo de engaños.
- Conocimiento de sus obligaciones y responsabilidades derivadas del actual marco normativo: LOPD, LSSI, LGT, Código Penal y Protección de la Propiedad Intelectual; etc.
- Cómo gestionar los soportes informáticos y los equipos y dispositivos portátiles.
- Cómo reaccionar ante determinados incidentes que puedan comprometer la Seguridad de la Información.
- Etc.

Estas acciones de formación se podrían completar con la elaboración de un manual básico para los usuarios del Sistema de Información, que incluya las principales recomendaciones de la empresa y recuerde las obligaciones y responsabilidades de los usuarios, así como los límites establecidos por la organización en el uso de los servicios de Internet.

[3] Entendemos por Ingeniería Social ("*Social Engineering*") el conjunto de técnicas y trucos empleadas por intrusos y hackers para extraer información sensible de los usuarios de un sistema informático: intrusos que se hacen pasar por empleados de otros departamentos de la empresa, por personal de un proveedor de servicios de informática, de un operador de telefonía o de acceso a Internet; e-mails que suplantan la identidad de otra persona u organización, o que incluyen textos o ficheros adjuntos a modo de reclamo; usuarios que utilizan foros y chats en Internet para conseguir tener acceso a determinados ficheros sensibles del sistema; "*shoulder surfing*" (espionaje de los usuarios para obtener su nombre de usuario y contraseña); "*dumpster diving*" (revisión de los papeles y documentos que se tiran a la basura y no se destruyen de forma adecuada); etc.

6. CONCLUSIONES

La implantación de un Sistema de Gestión de Seguridad de la Información debería considerar el factor humano como uno de sus elementos clave, contemplando aspectos como la adecuada formación y sensibilización de los empleados, la implicación de los responsables y directivos, la aprobación de un Reglamento Interno sobre el uso de la Informática e Internet en la organización, etc.

Asimismo, deberíamos destacar de forma especial la necesaria implicación y compromiso de la Alta Dirección, para conseguir que los empleados sean conscientes de la importancia que tiene para la organización garantizar la Seguridad de la Información y la adecuada utilización de sus sistemas y servicios informáticos y de comunicaciones.

RESEÑA CURRICULAR DEL AUTOR

Alvaro Gómez Vieites

Ingeniero Técnico Superior de Telecomunicación por la Universidad de Vigo. Especialidades de Telemática y de Comunicaciones. Número uno de su promoción (1996) y Premio Extraordinario Fin de Carrera.

"Executive MBA" y "Diploma in Business Administration" por la Escuela de Negocios Caixanova.

Ha sido Director de Sistemas de Información y Control de Gestión en la Escuela de Negocios Caixanova. Profesor colaborador de esta entidad desde 1996. Responsable de las materias de Ofimática, Internet y e-Business en los cursos y programas Master impartidos en esta entidad.

Socio-Director de la empresa SIMCe Consultores, integrada en el Grupo EOSA.

Autor de varios libros y numerosos artículos sobre el impacto de Internet y las TICs en la gestión empresarial.