La Seguridad y la Confidencialidad de la Información y la LORTAD

MIGUEL ANGEL RAMOS

Doctor en Informática. CISA. Vicepresidente de la Organización de Auditoría Informática y del Capítulo Español de la EDP Auditors Association, consultor en seguridad y auditor informático.

1. Introducción

Cada día la información tiene más importancia para las entidades, que basan en mayor medida su gestión en la disponibilidad de una información correcta, completa y a tiempo, por lo que es creciente la importancia de su seguridad y su confidencialidad.

La LORTAD se refiere a la confidencialidad de los datos de carácter personal, pero puede ser una excelente oportunidad para mentalizar a los "propietarios" de la información y directivos en general, ya que muchas de las medidas y controles pueden servir tanto para garantizar la confidencialidad como la seguridad en general, y lógicamente no sólo de los datos de carácter personal sino de todos ellos.

Los objetivos de la seguridad abarcan: las personas (y funciones que desempeñan, con la debida segregación), las propias instalaciones, los equipos y comunicaciones, los programas y, muy especialmente, los datos.

La seguridad y confidencialidad debe tratarse a un nivel corporativo, a través del oportuno Comité, que apruebe políticas y planes al respecto y aporte los medios necesarios para poder abordar con rigor la protección de la información y realizar un seguimiento en el tiempo sin relajaciones.

El primer paso es conocer qué riesgos existen para poder decidir cómo eliminarlos o al menos disminuir su impacto y/o la probabilidad de que se produzcan.

Las protecciones han de ser físicas y lógicas (entre éstas últimas están los paquetes de control de accesos), y existir una separación de entornos y una segregación de funciones, además de una clasificación de la información; y deben existir los medios para garantizar su eficiencia: asignación de responsables de los ficheros, administración de la seguridad, auditoría informática interna (y posible contratación de la externa).

A veces relacionamos seguridad informática con desastres, pero existen también pérdidas, errores, omisiones o filtraciones de información, de menor impacto pero mucha mayor probabilidad.

Por otra parte, la ausencia generalizada de noticias respecto a casos habidos en España no quiere decir que éstos no se produzcan, sino que se mantienen más en secreto que en otros países, para preservar la buena imagen de las entidades, por lo que no salen de círculos reducidos, y no pueden comentarse en conferencias o seminarios.

2. Protagonistas

La seguridad y confidencialidad de los datos automatizados (contenidos en cualquier soporte legible por ordenadores) no debe considerarse un tema puramente técnico. Los "propietarios" de la información y los directivos en general no pueden "abdicar" en los informáticos escudándose en su ignorancia, y deben aportar las líneas maestras (sin entrar en tecnicismos) y tener la garantía de que se están cumpliendo sus requerimientos, por ejemplo en cuanto a quién puede acceder a qué, cuánto tiempo se está guardando determinada información o qué controles existen para garantizar la integridad de los datos más críticos (nos referimos a datos críticos y no "sensibles" como recoge la propia LORTAD, que es una expresión muy usada, y que tal vez deriva de forma indirecta del inglés: "sensitive data").

Además, existirán los administradores de datos y de bases de datos, y los responsables de ficheros, figura recogida en la LORTAD y que expertos más autorizados han tratado en estas Jornadas en ponencias específicas.

Otros protagonistas (indirectos) son los usuarios, a quienes los propietarios habrán de autorizar a qué pueden acceder y cuándo.

Los informáticos son meros administradores de la información que procesan, aunque deben contribuir a garantizar a propietarios y usuarios que existen las medidas adecuadas.

Puede existir una función específica de Administración de la Seguridad (física y/o lógica), como interfaz entre propietarios, usuarios e informáticos.

Además, es deseable que exista la función de auditoría informática interna (y/o contratar auditoría informática externa, que son compatibles y complementarias), para que revisen si existen los controles adecuados, determinen cuáles pueden ser los riesgos y recomienden las medidas a implantar o reforzar. Dichos auditores han de contar con la preparación adecuada, además de la suficiente objetividad e independencia y, lógicamente, no pueden depender de la función de administración de seguridad ni viceversa.

En cuanto a controles, recordemos que se dice que han de ser: completos a la vez que simples, fiables, revisables, adecuados y rentables; y en cuanto a su coste, hay que considerar el de implantación y el de mantenimiento, frente al coste-riesgo de su no implantación. Los controles en general suelen dividirse en:

- controles preventivos: los que contribuyen a evitar que se produzca el hecho: el incendio, el acceso...

- controles detectivos: los que, una vez que se ha producido, ayudan a conocer el hecho, como la revisión de listados de ordenador con los documentos base como órdenes de clientes, para detectar errores y fraudes,

- controles correctivos: los que contribuyen a restaurar la situación de normalidad, como la recuperación de un fichero dañado a partir de copias de procesos anteriores.

3. La Lortad

La Ley, en su artículo 9 especifica:

1. El responsable del fichero deberá 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.

2. No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley.

El Estatuto de la Agencia de Protección de Datos (Real Decreto 428/93, BOE 4-5-93), en su artículo 28 determina sus funciones inspectoras (se resume el contenido):

- Examinar los soportes de información que contengan los datos personales
- examinar los equipos físicos
- requerir el pase de programas y examinar la documentación y algoritmos de los procesos
- examinar los sistemas de transmisión y acceso a los datos
- realizar auditorías de los sistemas informáticos.

Se trata de una de las pocas referencias que existen a la Auditoría Informática, actividad que no tiene reconocimiento oficial y no está regulada por ahora.

4. Areas

Hay muchos aspectos a considerar en relación con la seguridad y confidencialidad de la información, y algunos tienen una relación muy estrecha.

Entre ellos están:

*La existencia de planes, presupuestos y definición de niveles de responsabilidad. La seguridad y la confidencialidad deben ser una preocupación prioritaria de la Alta Dirección de la entidad, además de serlo de los propietarios de la información de cada área y de los usuarios y administradores.

La realidad es que si ocurre algo siempre se buscan "culpables", pero el enfoque debe ser preventivo, no a hechos consumados.

Es aconsejable que exista un Comité que se ocupe de la seguridad y confidencialidad. Si la entidad es importante puede tener ese cometido en exclusiva; si no, puede ser el propio Comité de Sistemas de Información (o de Informática) o el Comité de Dirección el que trate sobre estos temas en sus reuniones.

Uno de las primeras acciones deberá ser la definición de políticas y la elaboración de planes (plan de seguridad y de confidencialidad, plan de contingencia o de continuidad) y la aportación de los medios necesarios.

La mentalización de todo el personal también es un punto que no se debe pasar por alto, así como la asignación de medios, no sólo económicos sino "tiempo" a quienes tienen que dedicarse a ello, a menudo como otra tarea más a añadir a una larga lista. La colaboración externa puede aportar objetividad, experiencia y ritmo a este tipo de proyectos.

*Administración de la seguridad. Esta función puede tener, entre otros, los cometidos siguientes, que debieran definirse por escrito:

-Proponer políticas y estándares sobre seguridad y confidencialidad de la información,

-"Administrar" la seguridad: formación e información, así como establecimiento y revisión de controles (si existe auditoría informática interna, será ésta la que realice las revisiones),

En cuanto a la seguridad lógica (en contraposición a la física), participación en la selección e implantación de paquetes de seguridad, así como de la

propia seguridad de los diferentes productos y aplicaciones y el correspondiente seguimiento. Mantenimiento de usuarios (altas, bajas y variaciones de perfiles) y revisión de los informes que proporcione el paquete.

*La ubicación del centro de procesos y de los ordenadores: la ubicación ha de ser idónea para garantizar la seguridad y que sólo acceden las personas autorizadas. Si se trata de equipos departamentales o personales aislados igualmente deben estar protegidos para evitar el robo.

Dicho robo puede referirse al propio equipo, que a veces no sería tan importante como de la información que contuviera si no está debidamente respaldada en otro lugar, o si el conocimiento por terceros puede suponer pérdida de competitividad o de imagen.

Las instalaciones, por tanto, han de tener los mecanismos y controles necesarios: sensores, infrarrojos, blindajes, cámaras de televisión (que pueden visualizar vigilantes y que pueden ponerse en funcionamiento cuando se produzca movimiento), exigencia de marcar contraseñas para que se abran las puertas o para otros accesos... y todo ello según la criticidad de la información y la existencia de otros controles.

Otra medida complementaria es la contratación de seguros, más bien a los efectos de la recuperación económica, lo que no evita que se haya producido una pérdida irrecuperable de información y con las consecuencias indirectas que puede suponer.

*Hemos hablado de seguridad lógica, es decir de los accesos a través de terminales, locales o remotos. Es necesario decidir (los propietarios han de determinarlo o al menos las reglas generales) quién puede acceder a qué, para qué (lectura, borrado, variación...) y cuándo. También deben determinarse las pistas necesarias que han de quedar para poder hacer revisiones por otras personas.

A propósito de los accesos es importante la asignación de contraseñas, que son uno de los medios más comunes (y económicos) de identificarse ante un sistema, sobre todo ante una aplicación o un paquete de control de accesos, que dé la posibilidad de acceder o no a determinados recursos.

La identificación ante un sistema puede ser:

-Por algo "que se es": apariencia / foto del individuo. En algunos casos se está usando la biométrica, en base a los caracteres diferenciadores de los individuos, como retina o huella dactilar,

-por algo que se realiza: la firma, por ejemplo; existen sistemas automáticos de reconocimiento de firmas, con porcentajes muy pequeños de error,

-por algo que se tiene: por ejemplo, una tarjeta; cada vez se utilizan más las tarjetas "inteligentes" (el adjetivo puede no ser el más adecuado aunque sea la traducción más usada de "smart cards"), que tienen grabada información y que pueden contener la fotografía del individuo y/o la firma digitalizadas,

-por algo que se sabe, como la propia contraseña. El problema radica en poder garantizar que la persona que está marcando una contraseña es aquella a la que se asignó y no un "suplantador", que ha conocido la contraseña de forma casual o se la han cedido. De ahí la utilidad de combinar las contraseñas con biométrica u otros sistemas.

A propósito de las contraseñas, está demostrado que cada vez es menor el número de casos en que alguien "entra" en un sistema a base de intentos hasta acertar la contraseña, ya que se limita el número de ellos.

Así, por ejemplo, si después de tres intentos fallidos no ha sido capaz de acceder al sistema, el usuario como tal queda inactivo, y el administrador del sistema lo reactivará después de averiguar qué está pasando: es posible que el verdadero usuario haya vuelto de vacaciones y haya olvidado su contraseña, pero también puede ocurrir que alguien no autorizado, suplantando al verdadero usuario, esté intentando acceder. Si sabe que al tercer intento el sistema bloqueará ese código de usuario hará dos intentos cada día, pero esto también puede registrarlo un paquete de control de accesos y pasar esta información a un administrador para que investigue.

Las contraseñas, que tanta relación tienen con la seguridad de la mayoría de los sistemas que existen hoy en día, deben ser fáciles de recordar por su "propietario", para evitar tener que escribirla (como ocurre a veces con las que asignan de forma aleatoria los sistemas). Así, costará recordar una contraseña como "L3*2P7".

Si la asigna su "propietario" y no el sistema, debe ser difícil de imaginar por los demás, evitando datos obvios como el número de empleado, el de la matrícula de su coche o el nombre del cónyuge.

Deben tener una longitud mínima y poder combinar cifras y letras. Con una longitud de seis caracteres, y si contamos las letras, las cifras del 0 al 9 y algunos símbolos especiales, tenemos 42^6 posibilidades.

Algunos sistemas sofisticados (por ejemplo el paquete RACF de IBM), permiten forzar a los usuarios a que no reasignen ninguna de las "n" contraseñas anteriores. El número "n" lo asigna el administrador.

La caducidad es otro de los puntos importantes, ya que cuanto mayor sea la vida de una contraseña más vulnerable será: cada entidad debe fijar criterios al respecto, y un periodo de un mes puede constituir un plazo razonable. Existen sistemas más críticos con contraseñas de un día de vida (un turno de trabajo, por ejemplo) e incluso contraseñas de un solo uso.

Las contraseñas deben estar criptografiadas internamente en los ficheros y no aparecer "en claro" en las pantallas ni en los listados.

Las entidades deben recordar a sus empleados mediante procedimientos la prohibición de ceder la contraseña, ya que se pierde la "imputabilidad"; no será fácil atribuir una operación o transacción si varias personas en un departamento comparten una misma contraseña.

Por tanto, los sistemas deben obligar a los usuarios a identificarse y éstos "salirse" del sistema para obligar a otros a identificarse antes de comenzar su consulta o marcaje de datos.

Con demasiada frecuencia las contraseñas se ceden temporalmente o se teclean a la vista de otros (si se averiguan algunos de sus caracteres, o al menos que se trata, por ejemplo, de la parte izquierda superior del teclado, el número posible de combinaciones disminuye); debe existir la mentalización adecuada en cada entidad sobre el uso y custodia de las contraseñas.

También contribuye a incrementar la seguridad el hecho de que los terminales queden inactivos después de varios minutos sin uso, para evitar que otras personas no autorizadas conozcan lo que se muestra en la pantalla o incluso accedan a las aplicaciones y datos a que tienen acceso los usuarios primarios por abandono momentáneo de éstos.

*El desarrollo de aplicaciones: los desarrolladores, tanto internos como externos contratados, no tienen por qué conocer los datos "reales" críticos: contables, de empleados, de clientes... y de ahí que deba existir una separación de entornos suficiente, tanto física como lógica.

Y en los casos en que pueda ser necesario hacer pruebas con datos reales confidenciales, pueden existir programas que "camuflen" dichos datos, susti-

tuyendo los campos críticos para que, sin perder sus características, no contengan domicilios, nombres o saldos reales.

Por otra parte, en el momento del desarrollo pueden incorporarse algunos controles que ayuden a garantizar la integridad de la información y que avisen de situaciones anómalas que se detecten, por mal funcionamiento de programas o por accesos indebidos.

*Los datos: además de la clasificación (de uso restringido, departamental, confidencial...) debe existir segregación de funciones en cuanto a las diferentes fases del ciclo de vida de los datos y revisiones posteriores para confirmar que son veraces y están respaldados por, según los casos, órdenes de clientes, autorizaciones de pago...

También debe vigilarse que los datos en soportes magnéticos o en papel estén protegidos, incluso cuando ya no son necesarios (porque pueden seguir siendo confidenciales); así, el papel habrá de ser destruido, en vez de tirarlo o venderlo, y los soportes magnéticos deben borrarse expresamente mediante varias pasadas de grabación o, mejor aún, desmagnetizarse con dispositivos al efecto, ya que de lo contrario puede quedar información no "machacada" accesible por rutinas especiales o incluso leerse la que ha estado grabada previamente "debajo" con dispositivos muy sofisticados.

Tanto en los datos almacenados como en los transmitidos por línea puede usarse la criptografía, para que los que puedan acceder a los datos no estando autorizados para ello, encuentren dificultades y les resulte virtualmente imposible conocer la información; aunque en la práctica dependerá de la vulnerabilidad de los métodos empleados y de los medios con que cuenten los criptoanalistas.

En instalaciones más complejas puede convenir instalar arcos detectores de soportes magnéticos, que avisarían de los que tanto empleados o visitantes puedan intentar sacar de la instalación.

En cuanto al transporte de soportes magnéticos, puede realizarse por empresas especializadas o, en entornos menos sofisticados, en dispositivos cerrados y cuya llave y/o clave no esté en poder de las personas que realizan el transporte o esté suficientemente protegida (por ejemplo en sobre lacrado).

5. Riesgos

En definitiva, deben establecerse los procedimientos y controles necesarios para poder garantizar que cada usuario sólo accede:

-a lo que esté autorizado (instalaciones, programas, bases de datos, ficheros, campos...)

-para lo que esté autorizado: lectura, variación, borrado...

-cuando esté autorizado, en cuanto a fechas y horas.

Para prever situaciones de emergencia, es preferible no abrir excesivamente los perfiles de acceso, sino que existan usuarios con posibilidades excepcionales, incluso no asignados de forma permanente sino que cuando sean necesarios se entreguen en sobre cerrado a quienes lo necesiten, dejando constancia de ello, por ejemplo a través de un vigilante de seguridad física que custodiara el sobre, para que se pueda verificar después el uso de la contraseña especial y si su uso estaba justificado.

Esto puede ser útil en situaciones que pueden presentarse fuera de los horarios normales de trabajo, para recuperación de información o variaciones de programas o tablas por emergencias, y salir de situaciones de bloqueo que impidan la continuación de los procesos.

Los riesgos principales son:

-los accesos no autorizados, por las causas ya comentadas,

-la destrucción o "corrupción" de datos: por ejemplo las tablas de devengos, los porcentajes de liquidación, los domicilios, borrado de "pistas" en ficheros históricos...

-la manipulación de programas, que puede traducirse en destrucción o variación de datos, incluso pasado un tiempo alcanzada una circunstancia (lo que se denomina "bomba lógica", en contraposición a física), y que puede manifestarse, por ejemplo, llegada una fecha o cuando un campo alcance un valor determinado, por lo que puede resultar una lotería macabra; puede manifestarse cuando el autor ya no está en la entidad, que es a veces la finalidad: producir el daño pero no sufrir las consecuencias,

-En ocasiones lo que se persigue es el propio beneficio, por ejemplo la copia de programas o de datos, en el primer caso para evitar gastos y en el

segundo para conocerlos y así saber la situación de la entidad o los datos de sus clientes, por ejemplo, o bien para cederlos a terceros a cambio de un beneficio económico.

Ante cualquier incidencia es necesario investigar las consecuencias que ha habido para tratar de solucionarlas y averiguar qué ha fallado: si los controles no son rígidos, si ha habido encubridores, si los procedimientos son adecuados pero no se han cumplido...

6. Conclusiones

Es evidente que existe una necesidad de garantizar la seguridad y confidencialidad de la información, que será mayor según lo crítica que ésta sea en cada entidad, lo que vendrá determinado en buena medida por el sector.

La LORTAD es una buena ocasión para reforzar los mecanismos de protección que puedan garantizar la seguridad y confidencialidad de la información hasta unos niveles prefijados, ya que muchos de esos mecanismos son comunes.

Las consecuencias del incumplimiento de la LORTAD pueden traducirse en multas de hasta cien millones de pesetas, pero, además, hay que considerar otras posibles pérdidas: en cuanto a la falta de confidencialidad la pérdida de imagen y hasta de clientes; en lo que se refiere a la seguridad como tal, en los casos más graves, hasta la posible discontinuidad del funcionamiento de la entidad.

No obstante, la inversión en seguridad (y debemos hablar de inversión y no de gasto) es baja en España, salvo en algunas entidades aisladas, sobre todo del sector financiero o entornos militares y algunas multinacionales extranjeras.

Algunas de las medidas no son caras y es por ellas por las que debemos empezar; así, el conocer los riesgos y el implantar controles simples y procedimientos suelen constituir medidas de coste bajo y rentabilidad alta.

Podemos preguntarnos: ¿es mayor el coste de las medidas para garantizar la seguridad y confidencialidad o que no existan?. Antes de contestar, debemos considerar las pérdidas indirectas que podemos sufrir, así como que la falta de seguridad puede suponer como decíamos, ante una incidencia informática importante, la pérdida de toda la información vital y posiblemente el fin de la actividad de la entidad.

Bibliografía

- Auerbach: Data Security Manual

- Datapro: Computer Security (tres tomos). 1991

- Del Peso Navarro, Emilio. Prevención vs fraude: la Auditoría Informática. Actas del III Congreso Iberoamericano de Informática y Derecho. Mérida, 1992.

- Pfleeger, Charles P. Security in Computing. Prentice-Hall, 1989

- Ramos, Miguel Angel. Tesis Doctoral "Contribución a la mejora de las técnicas de auditoría informática mediante la aplicación de métodos y herramientas de ingeniería del conocimiento". F. de I. de la U.P.M.

- Ramos, M.A. La importancia de la seguridad informática. Computerwold, marzo 1990.

- Ramos, M.A. La Auditoría de la Seguridad. CHIP, marzo 1992.

- Ramos, M.A. Ponencias en Securmática en 1991 y 1992 y material de seminarios propios.

- S. Rao Vallabhanenei. Auditing Computer Security. John Willey & Sons, 1989.