Medidas para aumentar la seguridad informática en el centro de trabajo

Javier Arrieta Gutiérrez
Técnico Superior en Informática
Cámara de Comptos de Navarra / Nafarroako Kontuen Ganbara

Introducción

La información va adquiriendo un mayor **valor estratégico** para las Organizaciones. Aumenta la dependencia de los Sistemas de Información y, mientras que la pérdida de instalaciones o equipos puede ser superable si se soporta su valor económico, la pérdida de la información crítica puede llevar a finalizar la actividad de la Organización. La utilización de la informática crece continuamente. Se incrementa tanto el número de ordenadores como el de usuarios. Todo ello en un entorno tecnológico cada vez más complejo. De aquí la necesidad de un mayor control, así como de auditorías informáticas.

1. Seguridad de la información

1.1. Definición de seguridad de la información

Se define la seguridad de la información como la protección de la **CONFIDENCIALIDAD**, **INTEGRIDAD** y **DISPONIBILIDAD** de la misma.

- Por **CONFIDENCIALIDAD** se entiende que la información sea conocida exclusivamente por los usuarios autorizados, en la forma y tiempo determinada.
- Por **INTEGRIDAD** se concibe que la información pueda ser modificada, incluyendo su creación y borrado, sólo por personal autorizado.
- La **DISPONIBILIDAD** significa que la información esté accesible cuando y como lo requieran los usuarios autorizados.

1.2. Objetivos

Los objetivos que se propone alcanzar la Seguridad Informática son los siguientes:

- Incrementar la confianza de los responsables del sistema en que residen sus datos.
- Preservar la confidencialidad de los datos contra terceros.
- Garantizar la continuidad de las actividades de la organización.

1.3. Bienes a proteger

Las distintas categorías de bienes que intervienen en los procesos de Tecnologías de la Información son las siguientes:

- Personas
- Instalaciones
- Material ("hardware")
- Logical ("software")
- Datos

De todas ellas, los últimos son los accedidos por más personas y normalmente su tiempo de vida útil suele ser más corto, lo que los hace más vulnerables.

1.4. Amenazas

Las amenazas que se ciernen sobre los Sistemas de Información pueden ser físicas o humanas.

A su vez las **amenazas físicas** pueden deberse a:

- Desastres naturales:
  - incendios
  - inundaciones
  - terremotos
  - huracanes
  - rayos

- Accidentes
  - ° daños por agua
  - ° fallos en el suministro eléctrico
  - ° interferencias electromagnéticas
  - ° averías en los equipos: ordenadores, discos, sistemas de comunicaciones, líneas telefónicas, etc.
  - ° fallos en el "software" tanto de base como de aplicación

En cuanto a las **amenazas humanas** pueden ser:

- Voluntarias son los fraudes y delitos:
  - ° consulta indebida a datos
  - ° modificación o borrado de datos
  - ° sabotajes
- Involuntarias, son los errores.

1.5. Tipos de controles

Los controles que se pueden establecer sobre las Tecnologías de la Información son análogos a los que se usan en otras áreas y pueden clasificarse en los siguientes tipos:

1) Preventivos: antes de que ocurra un hecho. Por ejemplo, utilizar un programa de control de accesos.
2) Detectivos: para conocer los problemas. Por ejemplo, programas que dejan pistas de auditoría.
3) Correctivos: para rectificar los errores. Por ejemplo, hacer copias de un fichero para poder recuperarlo en caso de que el original resulte dañado.
4) Recuperación: para facilitar la vuelta a la normalidad después de ocurrido un error. Por ejemplo, establecer un Plan de Contingencias.

A mejores controles (no necesariamente mayores), menores riesgos. Dado que la Seguridad de alguna manera puede disminuir la Productividad hay que buscar un equilibrio entre los controles y la productividad - costes - burocracia.

1.6. Medidas de protección

Las medidas de protección que se pueden establecer se pueden clasificar en las cuatro categorías siguientes:

1) SEGURIDAD JURÍDICA
2) SEGURIDAD ORGANIZATIVO-ADMINISTRATIVA
3) SEGURIDAD FÍSICA
4) SEGURIDAD LÓGICA

En los siguientes apartados de este artículo se describe cada uno de estos niveles, comentando alguna de sus características más importantes.

2. Seguridad jurídica

Los tres hitos mas importantes desde el punto de vista de marco jurídico para el desarrollo de las actividades de las Tecnologías de la Información son: la Ley de protección de datos conocida como LORTAD, la Ley de protección del "software" y las referencias a la informática en el nuevo código penal. A continuación se realizan algunos comentarios sobre estas 3 Leyes.

2.1. Lortad

La cantidad de datos que se tratan en los sistemas informáticos, junto con el carácter "sensible" de gran parte de los mismos, resaltan la importancia de la confidencialidad.

La Constitución española recoge como derecho fundamental el de la intimidad personal. Este derecho puede ser gravemente amenazado por el mal uso de la informática. Concretamente en su articulo 18.4 del Título I dice que **"La ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".**

La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD) surge a partir del mandato de la Constitución y del empuje de las Directivas de la Comunidad Europea, junto con un incremento de la sensibilidad social.

Hoy en día la información es un recurso que ha adquirido un carácter vital para muchas organizaciones. Es un recurso imprescindible para el desarrollo económico y social, para la eficacia de la gestión administrativa y para la investigación, planificación y toma de decisiones.

El Derecho a la Información es un Derecho Social y el Derecho a la privacidad, es un derecho fundamental de la persona, reconocido por la Constitución. Se presenta una controversia entre dos aspectos: la accesibilidad frente a la confidencialidad. La solución es conciliar ambos derechos mediante Leyes de Protección de Datos que marquen el punto de equilibrio.

En su Artículo 4 sobre **calidad de los datos** prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos y dichos datos no podrán usarse para finalidades distintas para las que se recogieron.

El Artículo 9, **Seguridad de los datos**, dice: "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."

El Artículo 10, **Deber de secreto**, establece que "El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo".

Se crea la **Agencia de Protección de Datos** como organismo encargado de velar por el cumplimiento de la LORTAD pudiendo in-

cluso inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos accediendo a los locales donde se hallen instalados.

Preve la posibilidad de legislación complementaria por parte de las **Comunidades Autónomas**, algunas de las cuales ya la han ejercido.

Una nueva Directiva de la **Comunidad Europea** cambia el carácter estático de la LORTAD, que está orientada al fichero, por una orientación al tratamiento, que es dinámico.

A continuación se señalan algunos de los aspectos que deben comprobarse:

- Los ficheros automatizados con datos de carácter personal existentes en las Administraciones Públicas deben estar amparados por medio de disposiciones **publicadas en el Boletín Oficial** del Estado o diario oficial correspondiente tal y como señala el Artículo 18 para la creación, modificación o supresión de los ficheros de titularidad pública.
- Además, tales ficheros deben estar **inscritos en el Registro General de Protección de Datos** dependiente de la Agencia de Protección de Datos.
- Hay que tener previsto el acceso a los datos en cumplimiento de los Artículos 14 y 15 sobre los **derechos de acceso, rectificación y cancelación** dado que "el afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados" y "los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso".

2.2. Protección del "software"

La protección del "software" ha quedado establecida mediante la Ley sobre protección jurídica de programas de ordenador.

Muchos informes conceden a España el dudoso mérito de ocupar un puesto destacado en el ranking del pirateo de "software", con estimaciones de un bajo porcentaje de programas de ordenador legales.

Tras la publicación de la Ley de programas de ordenador aumentaron considerablemente las denuncias respecto a estas actuaciones. Dicha Ley permite a los fabricantes de programas iniciar acciones legales incluyendo registros sorpresa en las instalaciones de las empresas.

Las organizaciones BSA ("Business Software Alliance") junto con SEDISI (Asociación Española de Empresas de Tecnologías de la Información) han realizado diversas campañas para combatir la piratería informática. La última de ellas entre el 2 de diciembre de 1996 y el 31 de enero de 1997 ha permitido la normalización voluntaria de los programas de ordenador ilegales.

La problemática asociada al uso de programas sin licencia es más amplia y tiene tres vertientes:

1.- Legalidad: se contraviene lo dispuesto por la mencionada Ley.
2.- Productividad: utilización indebida del ordenador.
3.- Disponibilidad: presencia de virus informáticos.

2.3. Nuevo Código Penal

En el Código Penal anterior no existía el delito informático como tal. En el nuevo se añaden coletillas sobre delitos ya definidos, para el caso en que intervenga la informática. Las novedades más importantes son las siguientes:

- Se consideran delitos contra la intimidad, incluso cuando la información está registrada en soportes informáticos.
- Establece una analogía entre el uso de tarjetas magnéticas y llaves.
- Admite como estafa la manipulación informática que interfiera el resultado de un proceso o transmisión de datos.
- Incluye el apoderamiento de soportes informáticos para descubrir secretos empresariales.
- Incorpora la falsedad en documento electrónico dado que un documento puede estar en papel o en otro soporte.

3. Seguridad organizativo-administrativa

Este área abarca distintas medidas de índole organizativo que se pueden adoptar para mejorar la

Seguridad. Incluye aspectos tales como los siguientes:

- Definición de funciones y asignación de responsabilidades.
- Plan de seguridad: políticas, normas y procedimientos.
- Análisis de riesgos.
- Planes de contingencia.
- Clasificación de la información.
- Concienciación y formación de los usuarios.
- Auditoría informática.

A continuación se comentan algunos de los conceptos importantes dentro de este apartado.

3.1. Clasificación de la información según su confidencialidad

La información puede ser clasificada atendiendo a su confidencialidad. Por ejemplo, pueden establecerse los siguientes niveles:

- **NO CLASIFICADA**: cualquier usuario puede acceder a ella.
- **CONFIDENCIAL**: para acceder a esa información hace falta estar debidamente autorizado. Dicha autorización puede darse de manera genérica a todas las personas que realicen una determinada función, o tengan una determinada categoría, u ocupen unos determinados puestos de trabajo. Esto permite establecer grupos funcionales de usuarios de manera que cuando un usuario se da de alta en un grupo automáticamente tiene la autorización para el uso de esa información. Análogamente cuando un usuario deja de realizar una función, basta con desconectarlo del grupo para que automáticamente queden revocadas todas las autorizaciones.
- **RESERVADA**: el acceso a esta información se concede específicamente a unas personas individuales, sin permitirse agrupaciones genéricas como en el caso anterior. En estos casos también pueden realizarse unas agrupaciones de usuarios, pero solamente con fines organizativos.
- **SECRETA**: además de lo anterior en estos casos es obligatorio llevar registros de auditoría.

3.2. Clasificación de la información según su criticidad

Los datos, o mejor aún las aplicaciones que los tratan, deben clasificarse según su criticidad, entendiendo por tal lo necesarias que son para la actividad de la organización. Ello permite establecer unas prioridades que son la base de los **Planes de Contingencia o de Recuperación del Negocio**.

Deben existir copias suficientes de datos y programas que permitan su recuperación en caso de fallos.

Cada información debe residir al menos en dos soportes, para que en caso de que se estropee el original poder restaurarlo desde la copia.

Para prevenir el caso de un desastre, como el incendio total de la instalación, deben existir copias remotas en otro edificio.

3.3. Clasificación de usuarios

Pueden establecerse los siguientes tipos de usuario:

- **PROPIETARIO**: es el nivel más alto de responsabilidad en cuanto el uso de la información.
- **RESPONSABLE**: responsable de tomar y comunicar decisiones con vistas a identificar, clasificar y proteger activos de información. Entre sus responsabilidades hay que destacar la de clasificar los recursos y decidir quién puede acceder a esos recursos.
- **USUARIO**: un individuo autorizado para utilizar activos de información y los servicios disponibles para ello.
- **SUMINISTRADOR DE SERVICIO**: proveedor de servicios de proceso de información. Sirve como custodio de alguno de los activos de información y los proveerá de la seguridad apropiada.

3.4. Normas comunes de seguridad

Todo usuario debe formar parte activa del sistema de seguridad. De hecho algunas medidas externas que se tomen fracasarán sin una adecuada concienciación de los usuarios. Algunas normas en las que todos debemos participar pueden ser las siguientes:

- No compartir la contraseña.
- No escribir las contraseñas, sino memorizarlas.
- Cuidar el material informático: atención al tabaco, comidas y bebidas.
- No dejar el ordenador funcionando sin atender. Apagarlo o bloquearlo.
- No utilizar el ordenador para asuntos particulares.
- Guardar al menos 2 copias de la información crítica.
- Proteger la información confidencial.
- No copiar programas sin licencia.

4. Seguridad física

Ya hemos hablado de las **amenazas físicas** tales como:

- ° inundaciones
- ° fuego
- ° terremotos
- ° sabotajes
- ° cortes eléctricos
- ° interferencias electromagnéticas
- ° interferencias en las líneas telefónicas
- ° etc.

La Seguridad Física abarca las **medidas de protección externas** al ordenador y su entorno para pro-

tegerlo de las amenazas físicas, tales como:

- ubicación de los ordenadores
- normas de construcción y de instalaciones
- control de accesos físicos
- detección y extinción de incendios
- detección de humedad
- sistemas de alimentación ininterrumpida
- apantallamiento eléctrico de equipos y cableado
- doble suministrador de energía eléctrica o grupos electrógenos
- control de temperaturas y aire acondicionado
- etc.

5. Seguridad lógica

Las medidas técnicas agrupadas bajo el concepto de Seguridad Lógica, tratan de proteger tanto el "software", sea de base o de aplicación, como los datos.

5.1. Control de accesos

Criterio del **mínimo privilegio**: que cada persona tenga acceso solamente a lo que realmente necesita para llevar a cabo su función y en cada momento.

El **sistema operativo** tiene que:

1.- **controlar el acceso**: hay 2 modelos básicos:

1.1.- Modelos de matriz de acceso: objetos, sujetos y tipos de acceso. Se deben identificar todos los sujetos y objetos del sistema y debe haber un conjunto de reglas, que permitan determinar que sujetos pueden acceder a qué objetos.

1.2.- Modelos multinivel: La información se clasifica en niveles de seguridad: por ejemplo no-clasificada, confidencial, secreto y alto secreto. Además la información se subdivide en categorías: personal, finanzas, etc. También los usuarios se clasifican asignándoles niveles de seguridad y categorías. Cada usuario accede a la información según la categoría a que pertenece y siempre que el nivel de seguridad sea suficiente.

1.- **identificar y autentificar**: los sujetos individuales deben ser identificados. Autenticación mediante:

- algo que se sabe: contraseña
- algo que se tiene: tarjeta
- algo que se hace: sistemas de reconocimiento de la firma
- algo que se es: sistemas biométricos de reconocimiento de la voz, huella dactilar, mapa de retina

3.- **contabilizar y auditar**: un sistema fiable debe registrar todos los acontecimientos relevantes, a efectos de seguridad, en un diario de auditoría.

Gestor de base de datos: El sistema operativo se encarga de aspectos generales y primarios de la seguridad, pero estos deben ser complementados con la seguridad específica del gestor de base de datos.

5.2. Criptografía

Tiene sus principales aplicaciones en la **transmisión de datos**, pero también es útil en su **almacenamiento**. Hay 2 métodos principales para cifrar información:

- **Sistemas simétricos de clave única o secreta**: la misma clave se utiliza para cifrar y descifrar. El algoritmo más utilizado es el **DES** "Data Encryption Standard".
- **Sistemas asimétricos o de clave pública** donde cada participante en las comunicaciones posee dos claves, una pública conocida por toda la comunidad y otra privada solamente conocida por cada uno. El algoritmo más utilizado es el **RSA** de Rivest, Shamir y Adleman.

Seguridad de las comunicaciones: EDI ("Electronic Data Interchange") el intercambio electrónico de datos se basa en la **firma digital** para proveer servicios de confidencialidad, integridad, autenticidad y no-repudio.

Para enviar un mensaje confidencial el emisor lo cifra con la clave pública del receptor. El mensaje solamente puede ser descifrado por el receptor, pues para hacerlo debe utilizar su clave privada.

Si además el emisor cifra el mensaje con su clave privada el receptor puede descifrarlo mediante la clave pública del emisor. Esto le garantiza que el mensaje fue realmente enviado por el emisor.

5.3. Desarrollo de aplicaciones

Desde el punto de vista de la seguridad, es necesario añadir una **"Fase de Seguridad"** durante el diseño de una aplicación, en la que junto con el usuario, se determinen los requerimientos de seguridad que debe contemplar la aplicación.

Un primer concepto a tener en cuenta y que resulta ser fundamental para la seguridad, es el conocido como **segregación de funciones**:

Sobre un Sistema de Información se pueden ejecutar distintos tipos de funciones. **Estas funciones deben estar suficientemente segregadas para que puedan ser ejecutadas por distintos tipos de usuario**, lo cual supone un refuerzo importante de la confidencialidad e integridad de los sistemas.

Procesos de consulta. Normalmente los procesos de consulta se descomponen según criterios lógi-

cos, agrupando en la misma pantalla los campos que correspondan a un mismo concepto. También se tienen en cuenta criterios estéticos, por ejemplo, si una pantalla presenta demasiados campos puede resultar incómoda a la hora de trabajar por lo que se descompone en dos o más pantallas.

La confidencialidad nos da un concepto importante a la hora de agrupar los campos a visualizar en una misma pantalla. Los campos que deban ser vistos por diferentes tipos de usuario deben separarse en distintas pantallas gobernadas por diferentes transacciones para que mediante un sistema de control de accesos pueda asociarse a cada transacción el grupo de usuarios autorizados.

Procesos de actualización. Análogamente a lo dicho a los procesos de consulta sucede con los de actualización que afectan además de la confidencialidad a la integridad. Se deben diseñar distintos procesos de actualización gobernados por distintas transacciones de manera que puedan asignarse a diferentes tipos de usuario.

Por ejemplo, en un sistema contable puede haber un primer tipo de usuarios capaces de introducir apuntes que quedarán en una situación provisional. Otro tipo de usuarios puede tener la posibilidad de aprobar esos apuntes pasándolos a una situación definitiva, sin embargo no estarán autorizados a introducir apuntes provisionales.

En cuanto a la **disponibilidad** de la información se ve afectada por los procedimientos de respaldo y recuperación de las aplicaciones.

5.4. Fases de pruebas e implantación

Dentro del ciclo de vida del desarrollo de un Sistema de Información es necesario resaltar de cara a la seguridad la importancia de las fases de pruebas e implantación. Una forma de reforzar la integridad de los sistemas de información es insistiendo en unos buenos procesos de prueba antes de ponerlos en Producción.

Las pruebas deben darse con **datos ficticios** especialmente preparados para ello. En primer lugar, por razones de confidencialidad no deben utilizarse datos reales, pero es que además hay que garantizar que se reproducen todas las situaciones posibles con las que se pueden encontrar los programas.

Para la implantación de un nuevo proceso debe comprobarse su funcionamiento en un entorno real. Estas pruebas deben ser realizadas por los usuarios, con datos reales. Deben estar previstos los procedimientos de recuperación para el caso en que sea necesaria la marcha atrás.

5.5 Pistas de auditoría

Una opción interesante desde el punto de vista de la seguridad es la de utilizar ficheros con pistas de auditoría. Su uso es bastante frecuente en procesos de actualización, los cuales suelen marcar cada modificación de un registro mediante parámetros como la fecha y la hora y el código del usuario que ha realizado la operación.

Esta técnica puede aplicarse también al caso de procesos de consulta de ficheros cuya confidencialidad sea importante. Puede registrarse en un fichero de auditoría todas las consultas realizadas contra el fichero maestro, identificando el registro consultado y el usuario que realiza la consulta junto con algún parámetro más como la fecha y la hora.

Habrá que añadir los procesos necesarios para la gestión de este registro de auditoría de manera que los usuarios responsables del fichero maestro puedan consultar o listar el registro de auditoría. Como estos ficheros pueden crecer rápidamente habrá que tener en cuenta los procesos de respaldo o borrado de los registros de auditoría cuando ya no sean necesarios.

5.6. Separación de los entornos de desarrollo y producción

El Control de Cambios se encarga de controlar las modificaciones a programas, cadenas y ficheros. Es importante que exista una segregación de funciones entre los informáticos que realizan el desarrollo, los usuarios finales de la aplicación y el personal encargado de realizar los cambios. ■

	DESARROLLO	CONTROL DE CAMBIOS	PRODUCCIÓN
TIPO DE USUARIO	personal informático	encargado del control de cambios	usuario final
TIPO DEL "SOFTWARE"	"software" en creación o modificación	instalación del "software" preparado	"software" estable
DATOS UTILIZADOS	datos de prueba		datos reales