**LA INFORMACIÓN COMO ACTIVO ESTRATÉGICO:**

**SEGURIDAD Y PROTECCIÓN**

## 1. INTRODUCCIÓN

La información es uno de los **activos** más importantes de las entidades, y de modo especial en algunos sectores de actividad.

Es indudable que cada día las entidades dependen en mayor medida de la información y de la tecnología, y que los sistemas de información están más soportados por la tecnología, frente a la realidad de hace pocas décadas.

Por otra parte, hace unos años la protección era más fácil, con arquitecturas centralizadas y terminales no inteligentes, pero hoy día los entornos son realmente complejos, con diversidad de plataformas y proliferación de redes, no sólo internas sino también externas, incluso con enlaces internacionales.

Entre las **plataformas** físicas ("hardware") pueden estar: ordenadores grandes y medios, ordenadores departamentales y personales, solos o formando parte de redes, e incluso ordenadores portátiles. Esta diversidad acerca la información a los usuarios, si bien hace mucho más difícil proteger los datos, especialmente porque los equipos tienen filosofías y sistemas operativos diferentes, incluso a veces siendo del mismo fabricante.

Al hablar de seguridad hemos preferido centrarnos en la información misma, aunque a menudo se hable de seguridad informática, de seguridad de los sistemas de información o de seguridad de las tecnologías de la información.

En cualquier caso hay tres aspectos principales, como distintas vertientes de la seguridad:

La **confidencialidad**: se cumple cuando sólo las personas autorizadas (en un sentido amplio podríamos referirnos también a sistemas) pueden conocer los datos o la información correspondiente.

Podemos preguntarnos ¿qué ocurriría si un soporte magnético con los datos de nuestros empleados o clientes fuera cedido a terceros? ¿cuál podría ser su uso final? ¿habría una cadena de cesiones o ventas incontroladas de esos datos, que podrían incluir datos como domicilios o perfil económico, o incluso datos médicos?

¿Y si alguien se hiciera con un "disquete" con lo que perciben los directivos de nuestra entidad?

La **integridad**: consiste en que sólo las personas autorizadas puedan variar (modificar o borrar) los datos. Además deben quedar pistas para control posterior y para auditoría.

Pensemos que alguien variara datos de forma que perdiéramos la información de determinadas deudas a cobrar (o que sin perderla tuviéramos que recurrir a la información en papel), o que modificara la última parte de los domicilios de algunos clientes.

Algunas de estas acciones se podrían tardar en detectar, y tal vez las diferentes copias de seguridad hechas a lo largo del tiempo estarían "viciadas" (corruptas decimos a veces), lo que haría difícil la reconstrucción.

La **disponibilidad**: se cumple si las personas autorizadas pueden acceder a tiempo a la información.

El disponer de la información después del momento necesario puede equivaler a la no disponibilidad. Otro tema es disponer de la información a tiempo pero que ésta no sea correcta, e incluso que no se sepa, lo que puede originar la toma de decisiones erróneas.

Otro caso grave es la no disponibilidad absoluta, por haberse producido algún desastre. En ese caso a medida que pasa el tiempo el impacto será mayor, hasta llegar a suponer la no continuidad de la entidad, como ha pasado en muchos de los casos producidos (más de un 80% según las estadísticas), ya que las incidencias son frecuentes, y tenemos cercano el caso de los daños en el área de Acapulco.

En relación con ello deben existir soluciones alternativas, basadas en medios propios o contratados, copias actualizadas de la información crítica y de programas en un lugar diferente, y un verdadero **plan de continuidad** que permita restablecer las operaciones en un tiempo inferior o igual al prefijado.

Para ello los usuarios habrán determinado previamente la **criticidad de las aplicaciones** y el impacto en sus áreas, y a un nivel corporativo, idealmente por parte de un comité, se habrán determinado las **prioridades**.

En la preparación −y actualización− del plan debemos pensar en situaciones posibles y en el impacto que tendrían en nuestra entidad (en su caso en las de nuestros clientes), especialmente si no disponemos de la información necesaria almacenada en lugares alternativos.

La seguridad tiene varios **estratos**:

El **marco jurídico** adecuado.

**Medidas técnico−administrativas**, como la existencia de políticas y procedimientos, o la creación de funciones, como administración de la seguridad o auditoría de sistemas de información interna.

Ambas funciones han de ser independientes y nunca una misma persona podrá realizar las dos ni existir dependencia jerárquica de una función respecto a otra.

En cuanto a la administración de seguridad pueden existir, además, coordinadores en las diferentes áreas funcionales y geográficas de cada entidad, especialmente si la dispersión o la complejidad organizativa o el volumen de la entidad así lo demandan.

En el caso de multinacionales o grupos de empresas nacionales no está de más que exista coordinación a niveles superiores.

En todo caso, debe existir una definición de funciones y separación suficiente de tareas; no tiene sentido que una misma persona autorice una transacción, la introduzca, y revise después los resultados (un diario de operaciones, por ejemplo), porque podría planificar un fraude o encubrir cualquier anomalía; por ello deben intervenir funciones / personas diferentes y existir controles suficientes.

La **seguridad física**, como la ubicación de los centros de procesos, las protecciones físicas, el control físico de accesos, los vigilantes, las medidas contra el fuego y el agua, y otras similares.

La llamada **seguridad lógica**, como el control de accesos a la información exigiendo la identificación y autenticación del usuario, o el cifrado de soportes magnéticos intercambiados entre entidades o de respaldo interno, o de información transmitida por línea. (Puede haber cifrado de la información por dispositivos físicos o a través de programas, y en casos más críticos como la red SWIFT existen los dos niveles).

La **autenticación** suele ser mediante contraseña, si bien sería más lógico, aunque los costes resultan aún altos para la mayoría de sistemas, que se pudiera combinar con **características biométricas** del usuario, para

impedir la suplantación. Entre éstas pueden estar la realización de la firma con reconocimiento automático por ordenador, el análisis del fondo de ojo, la huella u otras.

**2. RIESGOS**

Al margen de la seguridad, nos parece que el mayor riesgo, aun teniendo un entorno muy seguro, es que la Informática, y la Tecnología de la Información en general, no cubran las necesidades de la entidad: no estén **alineadas con el Plan de "Negocio"**.

Limitándonos a la seguridad propiamente dicha, los riesgos pueden ser múltiples: el primer paso es conocerlos, y el segundo es tomar decisiones al respecto; el conocerlos y no tomar decisiones no tiene sentido y debiera crearnos una situación de desasosiego.

Como las medidas tienen un coste, a veces los directivos se preguntan, o nos preguntan a los consultores, cuál es el riesgo máximo que podría soportar su entidad, si bien la respuesta no es fácil, porque depende de la criticidad del sector y de la entidad misma, de su dependencia respecto a la información, y del impacto que su no disponibilidad pudiera tener en la entidad.

Si nos basamos en el impacto nunca debería aceptarse un riesgo que pudiera llegar a poner en peligro la propia continuidad de la entidad, pero este listón es demasiado alto.

Por debajo de ello hay daños de menores consecuencias, siendo los errores y omisiones la causa más frecuente, normalmente de poco impacto pero frecuencia muy alta, y otras el acceso indebido a los datos (a veces a través de redes), la cesión no autorizada de soportes magnéticos con información crítica (algunos dicen "sensible"), los daños por fuego, por agua (del exterior como puede ser una inundación, o una tubería interior), la variación no autorizada de programas, su copia indebida, y tantos otros, persiguiendo el propio beneficio o el causar un daño, a veces por venganza.

Otra figura es la del *hacker*, que intenta acceder a los sistemas más para demostrar (a veces sobre todo para demostrarse a sí mismo/a) de qué es capaz, así como que puede superar las barreras de protección que le hayan establecido.

Alguien podría preguntarse por qué no se citan también los virus, cuando han tenido tanta incidencia; afortunadamente ésta es menor ahora que hace unos años, si bien existe un riesgo constante porque de forma continua aparecen nuevas modalidades, que no son detectadas por los programas antivirus hasta que las nuevas versiones los contemplan. Y un riesgo adicional es que los virus puedan llegar a afectar a los grandes sistemas, sobre todo a través de las redes, pero esto es realmente difícil −no nos atrevemos a decir que imposible− por las características y complejidad de los grandes equipos y las características de diseño de sus sistemas operativos.

En definitiva, las amenazas hechas realidad pueden llegar a impactar en los datos, en las personas, en los programas, en los equipos, en la red... y alguna incidencia en varios de ellos, como puede ser un incendio.

Podríamos hacernos una pregunta difícil **¿qué es lo más crítico a proteger?** La respuesta de la mayoría probablemente sería que las personas somos lo más crítico, y el valor de una vida humana no se puede comparar con los ordenadores, las aplicaciones o los datos de cualquier entidad.

Ahora bien, por otra parte, podemos determinar que los datos son aún más críticos si nos centramos en la continuidad de la entidad.

Como consecuencia de cualquier incidencia se pueden producir unas **pérdidas**, que pueden ser no sólo **directas** (y éstas es más fácil que puedan cubrirlas los seguros), sino también **indirectas,** como la no

recuperación de deudas al perder los datos, o no poder tomar las decisiones adecuadas en el momento oportuno por carecer de información.

Sabemos que se producen casos en gran parte de entidades, pero en general no conocemos a cuáles han afectado (o lo sabemos pero no podemos difundirlo), porque por imagen no se hacen públicos los casos, y el hecho de que se conozcan muchos más referidos a Estados Unidos y otros puntos lejanos que respecto a nuestros países no significa que estemos a salvo, sino que nuestro pudor es mayor y los ocultamos siempre que podemos.

**3. PROTECCIÓN DE ACTIVOS VITALES**

Son activos vitales todos aquellos relacionados con la continuidad de la entidad, como pueden ser: planes estratégicos, fórmulas magistrales, diseño de prototipos, resguardos, contratos, pólizas... y **datos estratégicos**, que son los que más nos interesan bajo la perspectiva de la seguridad de la información.

Y debemos protegerlos pensando en los intereses de los accionistas, de los clientes, y también pensando en los empleados y en los proveedores.

Cabe preguntarse el coste de la seguridad frente al coste de la no seguridad, si bien con antelación no es fácil saber qué alternativa es mejor, pero no se trata de buscar la mayor rentabilidad económica, porque hay razones de otra índole.

Y debemos pensar que se trata de **INVERSIONES en seguridad**, aunque en algunos casos se nos diría que no es fácil reflejarlas como activos contables y que cual es su rentabilidad; necesariamente hemos de estar de acuerdo, pero ¿cuál es la rentabilidad de blindar la puerta de acceso a nuestro domicilio, o la de instalar un antirrobo sofisticado en nuestro coche? Esa rentabilidad la podemos determinar si los dispositivos o controles han servido para evitar la agresión, pero a veces habrá constituido una medida disuasoria y no llegaremos a enterarnos de su efecto positivo.

En todo caso la seguridad puede tener un impacto favorable en la imagen de las entidades, aunque ello sólo no suela justificar sus costes, y tanto para clientes y posibles clientes como para los empleados. Unos y otros pueden sentirse más protegidos, así como considerar más protegidos sus activos.

Y la protección no ha de basarse sólo en dispositivos y medios físicos, sino en formación e información adecuada al personal, empezando por los directivos para que, "en cascada", afecte a todos los niveles de la pirámide organizativa.

Además, la existencia de funciones específicas cuando el entorno lo justifica, contribuye a incrementar la seguridad. Entre ellas las citadas de administración de la seguridad y auditoría de sistemas de información interna.

Porque deben existir los tres niveles de protección:

El **CONTROL INTERNO**, basado en objetivos de control y llevado a cabo por los supervisores a distinto nivel,

La **AUDITORÍA DE SISTEMAS DE INFORMACIÓN INTERNA**, objetiva e independiente y con una preparación adecuada, como control del control,

La **AUDITORÍA DE SISTEMAS DE INFORMACIÓN EXTERNA**, contratada cuando se considera necesaria, y como un nivel de protección más. Igualmente objetiva e independiente.

Los informes de auditores, internos o externos, han de señalar las posibles deficiencias e indicar, en su caso, las recomendaciones correspondientes.

**4. CONCLUSIÓN**

Cabe preguntarse qué hacer, qué pasos dar. No hay soluciones únicas, sino que dependen de la entidad y del momento, por lo que se indican pasos generales.

Debe partirse de una **política corporativa** sobre la seguridad.

El paso siguiente puede ser la designación de personas concretas para funciones determinadas.

Y si no existe una idea clara de cuáles son los riesgos debe hacerse una **evaluación de dichos riesgos**, por personas objetivas e independientes y técnicamente preparadas, que pueden ser internas, externas, o formando un equipo mixto.

Una vez conocidos los riesgos han de tomarse decisiones, tendentes a eliminarlos, que no siempre es posible, a reducirlos, a transferirlos (a una compañía de seguros por ejemplo), o bien aceptarlos, a un nivel suficientemente alto y corporativo.

La contratación de seguros es necesaria si bien es evidente que, respecto a la información, pueden resarcirnos de la pérdida económica en el caso de incidencias pero si no disponemos de los datos no podremos procesar y, como se ha indicado, se puede poner en peligro incluso la continuidad de la entidad.

Después la entidad ha de crear un **modelo** de seguridad (o adoptar uno existente) así como definir una **estrategia** a seguir, establecer un **plan** y aportar los medios necesarios, que además de presupuesto son el reconocimiento de la importancia de la seguridad, y que no quede como tarea "de relleno" para cubrir tiempos de ocio de los técnicos.

Uno de los primeros productos ha de ser un conjunto de **objetivos de control interno**, que nos gusta definir como "declaraciones sobre el resultado final deseado o del propósito a ser alcanzado mediante la implantación de procedimientos de control".

Para ello la entidad puede basarse en publicaciones como los "Control Objectives", de la Information Systems Audit and Control Association, que cuenta con varios Capítulos en México, así como en otros países iberoamericanos y en España.

Podemos decir que un **sistema de control interno** puede constar de procesos, funciones, actividades, subsistemas y dispositivos, cuya finalidad (total o parcial) sea garantizar que se alcanzan los mencionados objetivos de control.

Finalmente se han de definir **proyectos concretos**, con actividades, responsables, resultados y costes.

Entre dichos proyectos pueden estar:

. Creación de normas,

. Separación de entornos: desarrollo de aplicaciones y su explotación,

. Consideración del **marco legal** aplicable en cada país y en qué afecta,

. Determinación de los **propietarios** de la información, y clasificación de ésta. Al respecto podemos decir que

los propietarios de la información son los clientes, proveedores, empleados... pero debemos además definir, dentro de la entidad, quiénes habrán de ser verdaderos administradores y en cierto modo "dueños" de los datos; al margen del Consejo de Administración, debemos llegar a niveles operativos, como podrían ser el Director de Recursos Humanos para los datos de empleados, o el de Marketing o de Productos para la información de determinados clientes / productos.

Y la **clasificación de la información** sirve para diferenciar los datos de libre acceso por todos los empleados, los restringidos a departamentos o niveles verticales, o los que pueden ser altamente confidenciales; cada entidad debe definir estos niveles, no más de cuatro o cinco. Y los paquetes de control de accesos pueden incorporar las clasificaciones para dejar acceder o no según los usuarios a qué datos y para qué (sólo lectura, variación, ejecución de programas...).

La información sobre salud de los empleados, por poner un ejemplo, sólo debe estar accesible al servicio médico.

. **Plan de continuidad**: es la culminación de la seguridad, si bien puede suponer una gran complejidad y un coste elevado, pero es necesario que la entidad pueda asegurar la continuidad de sus operaciones, por medios propios o ajenos, si ocurre una incidencia importante.

Queremos finalizar recordando la importancia de los controles, para lo que debemos distinguir entre:

Controles **preventivos**, como exigir una contraseña antes de permitir el acceso

Controles **de detección**, como los que avisan de incendios en sus fases más tempranas, a veces sin verse el fuego aún

Controles **de corrección**, como las copias de información para restaurar una situación.

Podemos decir que la seguridad de la información ha de ser una preocupación constante de las entidades, a un nivel suficientemente alto, que no es exclusivamente un problema técnico y de los técnicos, y que se trata de un camino para el que puede haber indicaciones, pero que será diferente según la entidad y el momento. Como decía el poeta Antonio Machado: "...se hace camino al andar...".