De la seguridad informática a la seguridad de la información

Mª Jesús Recio
Responsable de Calidad de Servicios de Infraestructura, dentro del Área Calidad Operativa - Operaciones TI de la Dirección de Calidad y Medio Ambiente de Indra

Desde hace ya algunos años la información está definida como el activo más valioso de una compañía (los costes derivados de pérdida de seguridad no son sólo costes económicos directos, sino que también afectan a la imagen de la empresa), por lo que, cada vez más, la seguridad de la información forma parte de los objetivos de las organizaciones y, sin embargo, y a pesar de esa concienciación generalizada, muchas compañías no se enfrentan a este aspecto con la globalidad con la que debiera tratarse.

Además de esta falta de visión global, existe otro factor que afecta a la estrategia de seguridad de una organización: la dispersión de las inversiones de seguridad en múltiples nichos desalineados con el objetivo global, de modo que la focalización en cuestiones concretas de seguridad hace olvidar el objetivo estratégico.

Cuando una empresa define la seguridad de la información como prioridad, estableciendo medidas que ayuden a conseguirla, de manera inmediata se plantea la necesidad de instalar mecanismos, llamémosles físicos, que permitan controlar los riesgos asociados a la seguridad más inmediata; mecanismos entre los que se encuentran desde las medidas físicas aplicables al espacio en el que se ubican los sistemas que contienen la información (control de acceso al CPD, video-vigilancia, etc.) hasta las medidas físicas asociadas a la arquitectura de su red (cortafuegos, sistemas de detección y prevención de intrusión, antivirus, control de contenidos), dejando a un lado aspectos muy relevantes sin los cuales no se puede considerar una buena gestión de la seguridad. Básicamente se centra en la aplicación de una "seguridad informática" y no en la aplicación de una "seguridad de la información".

El punto fundamental de partida para el establecimiento y mantenimiento con garantías de éxito de la seguridad de la información es la definición clara de objetivos a partir de los cuales desarrollar las políticas y procedimientos que definan el marco en el que situar las medidas de seguridad a implantar, teniendo en cuenta aspectos como las leyes que rigen en materia de seguridad el espacio geográfico en el que se ubica la organización

(LOPD, por ejemplo, en España), los compromisos con terceros en el cumplimiento de normas que tenga la compañía (SAS70, 27001, etc.) y, por supuesto, el día a día del negocio.

Construyendo la seguridad. El punto de partida: establecimiento de responsables y definición de objetivos

Como se ha mencionado anteriormente, el punto de partida siempre debe ser la definición de los objetivos que, en materia de seguridad, quieren alcanzarse y el grado de consecución de los mismos; como en casi todo, el nivel de seguridad objetivo será proporcional a la inversión que se realice para conseguirlo. La pregunta que debe regir la definición de este grado es: "¿cuánto vale mi información?".

Igualmente es fundamental conocer otros aspectos como son el punto de partida (en qué punto se encuentra la seguridad), los riesgos de la seguridad que pueden potencialmente afectar a la compañía en función de aspectos como el negocio o el espacio geográfico, el tratamiento o asunción de estos riesgos y el impacto de los mismos, materializados todos ello en un análisis de riesgos. Debe considerarse, por tanto, el análisis de riesgos perfectamente alineado con la visión de la organización y dentro de su entorno de operación como el punto central para el establecimiento en detalle de las medidas (controles) de seguridad que deben implantase y con ello el grado de consecución de los objetivos de seguridad establecidos.

El objetivo marcado, la identificación de riesgos y con ello la de controles a implantar, el grado de consecución y los plazos establecidos para lograrlo determinan, además de la inversión necesaria, el equipo de trabajo que debe establecerse para la implantación de todas las medidas. Por regla general este equipo de seguridad debe ser multidisciplinar, formado por ingenieros de sistemas, sociólogos, abogados y consultores en la materia, dado que hay que enfrentarse a tareas dentro de todas y cada una de estas áreas de especialización.

Una vez establecido el objetivo, y definido el equipo de seguridad, será necesario diseccionar dicho objetivo a través del desarrollo de una normativa compuesta por políticas y procedimientos, que van desde la política de seguridad de la compañía (documento global en el que se recogen dichos objetivos, se definen controles genéricos de seguridad [en función del resultado obtenido en el análisis de riesgos] y se establecen directrices básicas acordes tanto a los requisitos del negocio como a la legislación y normativa vigente) hasta procedimientos e instrucciones técnicas que recojan las directrices de seguridad a cumplir en el uso de las activos de la compañía, todo ello encaminado a la implantación de los controles de seguridad precisos y necesarios según el análisis de riesgos realizado, y siempre teniendo en cuenta la actividad diaria de la organización.

Es fundamental en el desarrollo de esta normativa tener en cuenta el modo en el que se lleva a cabo la actividad diaria para que asegurar que el cumplimiento de esta normativa no impacte de manera severa en el funcionamiento de la organización.

Las siguientes tablas recogen, a modo de ejemplo, un listado de posibles documentos a definir por la compañía en materia de seguridad, divididos por políticas, procedimientos e instrucciones técnicas.

Cuadro 1. Metodología para el análisis de riesgos

Entrevistas: mediante este tipo de aproximación a la organización, se busca entender los diferentes aspectos que la conforman, tanto en el aspecto tecnológico como en los procesos críticos, los cuales, a su vez, son soportados por las aplicaciones y la infraestructura tecnológica.
Evaluación de riesgo: la evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información sobre la plataforma tecnológica de una organización con el fin de generar un plan de implementación de los controles que aseguren un ambiente seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información. Los dos puntos importantes a considerar son: la probabilidad de una amenaza y la magnitud del impacto sobre el sistema si ésta llega a materializarse.
Determinación de la probabilidad: con el fin de derivar una probabilidad o una estimación de la ocurrencia de un evento, se deben tener en cuenta dos factores: fuente de la amenaza y capacidad y naturaleza de la vulnerabilidad.
Magnitud del impacto: determina el impacto adverso para la organización como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad; para ello se deben considerar los siguientes aspectos: consecuencias de tipo financiero, es decir, pérdidas causadas sobre un activo físico o lógico determinado y consecuencias provocadas por la inoperatividad del activo afectado, la criticidad de los datos y el sistema (importancia a la organización) y, cómo no, la sensibilidad de los datos y el sistema.
Identificación de controles: se evalúa la matriz de riesgo obtenida previamente con el fin de identificar los controles que mitiguen los riesgos detectados.

Cuadro 2. Definiciones

Riesgo: posibilidad de sufrir algún daño o pérdida.
Activo: datos, infraestructura, *hardware, software,* personal y su experiencia, información, servicios.

Tabla 1

POLÍTICAS	ALCANCE DEL DOCUMENTO
Política de seguridad de la compañía	Objetivos de seguridad de la compañía
Para aquellas afectadas por la LOPD, documento de seguridad y manuales de seguridad asociados	Cumplir con lo establecido en la Ley Orgánica de Protección de Datos
Política de copias de seguridad	Establecer la política para la realización de *backups* de la información
Política de uso de Internet y correo electrónico	Recoger las reglas generales de utilización de estas herramientas
Política de gestión de contraseñas	Recoger las medidas de seguridad que rigen la gestión de contraseñas (longitud, caracteres, caducidad, almacenamiento, etc.)
Política de antivirus	Gestión de antivirus, activación, etc.
Política de publicación en Internet	Normativa para disponer máquinas en Internet
Código de uso aceptable	Normativa general a cumplir por todos los usuarios en materia de seguridad

Tabla 2

PROCEDIMIENTOS	ALCANCE DEL DOCUMENTO
Procedimiento de copias de seguridad	Detalle de cómo realizar las copias
Procedimiento de altas/bajas de usuario	Detalle de cómo gestionar usuarios
Procedimiento de cifrado de información	Detalle de cuándo y cómo debe cifrarse la información
Tipología de redes	Requisitos técnicos de seguridad de las posibles arquitecturas de red
Procedimiento de auditoría de vulnerabilidades	Detalle de realización de auditorías de vulnerabilidades
Procedimiento de usuarios administradores	Detalle de gestión de usuarios administradores
Procedimiento de actuación ante la pérdida de un equipo portátil con información	Detalle, para todos los empleados, de los pasos a dar cuando se extravía un equipo con información delicada

Tabla 3

INSTRUCCIONES TÉCNICAS
• Guía de securización de sistemas
• Guía de securización de BBDD
• Guía de securización de comunicaciones
• Guía de securización de elementos de comunicaciones
• Guía de securización de *software* adicional (navegadores, servidores web, servidores de aplicaciones, aplicaciones basadas en SAP…)

Ya definidas las políticas, procedimientos e instrucciones técnicas, se debe proceder a la distribución de todos los estamentos de la organización, así como a la concienciación para el cumplimiento de las medidas definidas.

Son muchas las compañías que, si bien han cumplido con la definición de estos documentos y su difusión, no han sabido concienciar a sus empleados. Se debe tener presente que por mucho que se definan y se difundan medidas de seguridad, si la compañía no es capaz de concienciar adecuadamente para su cumplimiento, se habrá fracasado en la consecución de los objetivos marcados, sean éstos cualesquiera.

La concienciación es una tarea muy difícil de gestionar, sobre todo en organizaciones que por su tamaño y dispersión geográfica impiden una relación directa entre el equipo de seguridad y el resto de los empleados.

Algunas medidas que pueden ayudar a esta concienciación son:

- Realización de charlas formativas periódicas.
- Envío regular de píldoras informativas con pequeños resúmenes a través del correo electrónico.
- Publicación en las intranets corporativas de las presentaciones.
- Foros divulgativos sobre seguridad.

Todas ellas aplicadas siguiendo una premisa básica: “cercanía al destinatario”.

Gráfico 1

Buscando la seguridad física

Es evidente que las medidas para la seguridad física (seguridad informática) siempre formarán parte de las medidas generales de seguridad a implantar. En este punto se debe tener presente que proteger la información supone aplicar aquellas medidas destinadas a garantizar la integridad, confidencialidad, disponibilidad, autenticidad y no repudio de la información, por lo que las medidas físicas deben seleccionarse para asegurar estos aspectos, sin olvidar las consecuencias directas e indirectas que la puesta en marcha de las mismas pudieran provocar en la operativa diaria de la organización.

Cuadro 3

Confidencialidad: aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Integridad: garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

Disponibilidad: aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Cuadro 4

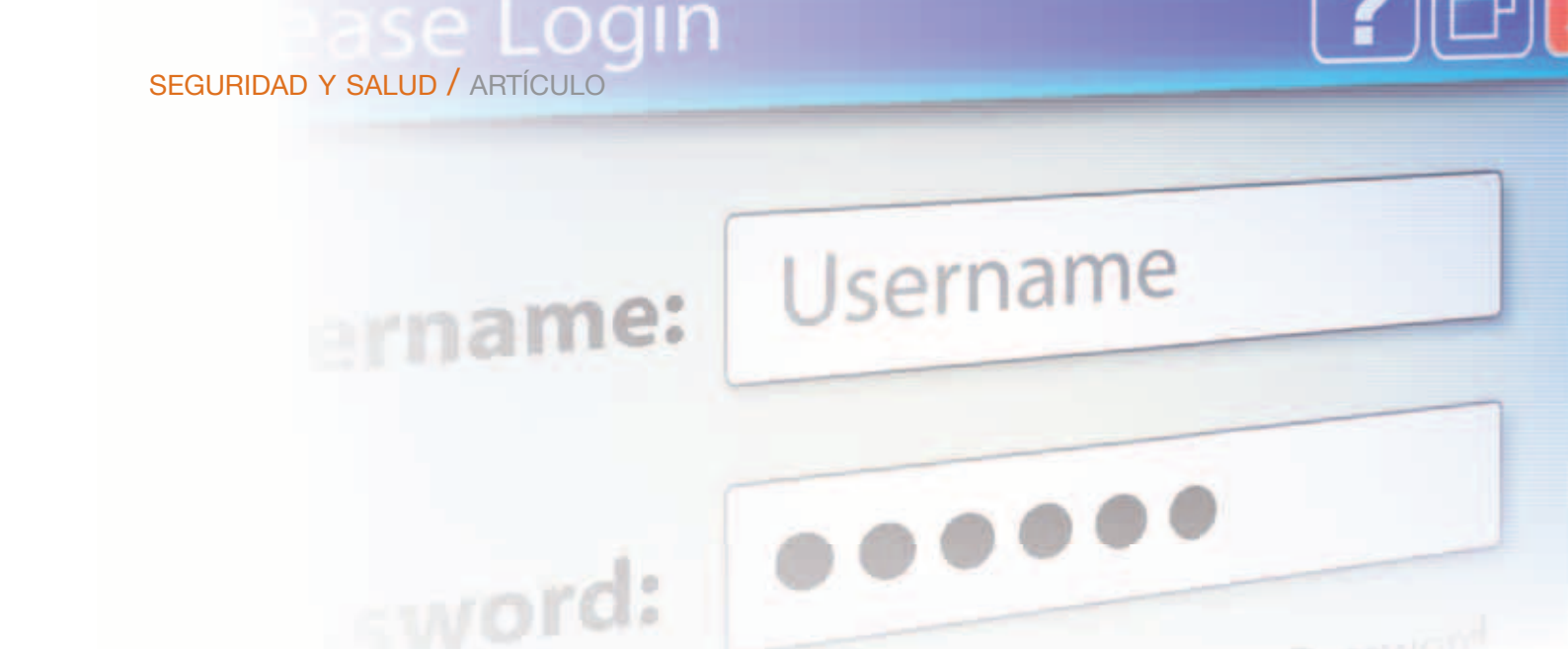
- La confidencialidad busca prevenir la revelación no autorizada, intencional o no, del contenido de un mensaje o de información en general.
- La integridad asegura que:
  - No se realizan modificaciones de datos en un sistema por personal o procesos no autorizados.
  - No se realizan modificaciones no autorizadas de datos por personal o procesos autorizados.
  - Los datos son consistentes, es decir, la información interna es consistente entre sí misma y respecto de la situación real externa.
- La disponibilidad asegura que el acceso a los datos o a los recursos de información por personal autorizado se produce correctamente y en tiempo. Es decir, la disponibilidad garantiza que los sistemas funcionan cuando se les necesita.

Ejemplos de medidas encaminadas a garantizar estos tres aspectos son: puesta en marcha y mantenimiento periódico de mecanismos de vigilancia y control de acceso para los CPD de equipos que garanticen la redundancia de elementos críticos (alimentación del CPD, sistemas de mantenimiento de temperatura), de sistemas de control de incendios, inundaciones y de todos aquellos elementos que por la naturaleza de la organización y el entorno sean relevantes.

Gráfico 2

Un paso más: seguridad lógica

Una vez protegido el espacio físico en el que se disponen las infraestructuras que contienen la información, será necesario aplicar las medidas definidas en las políticas e instrucciones técnicas referentes a la arquitectura. Algunas de estas



medidas son: segregación en niveles, implantación de dispositivos encaminados a garantizar la protección como cortafuegos, sistemas de prevención y detección de intrusión.

Igualmente se debe considerar la aplicación de medidas encaminadas a la protección de los equipos con los que se accede a los sistemas que contienen la información a proteger mediante la utilización de antivirus, controles de acceso a páginas no confiables, restricción de la utilización de correos no corporativos, prohibición de utilización de *software* sin licencia, etc.

Por último, y a este nivel, deben establecerse requisitos de seguridad en las aplicaciones que serán soportadas por la infraestructura: de nada sirven elementos como los mencionados si el nivel que se instala sobre ellos provoca la necesidad de crear agujeros de seguridad en los mismos.

Otros controles de seguridad

Anteriormente se ha mencionado que seguridad de la información no es seguridad informática; se puede decir que la seguridad de la información engloba medidas de seguridad entre las que se encuentran medidas asociadas a la seguridad informática.

No sólo hay que proteger los sistemas y el espacio que los contiene; hay que crear una mecánica de trabajo global que asegure el mantenimiento de las medidas de seguridad y el cumplimiento de las políticas e instrucciones establecidas.

Medidas como la aplicación de caducidad y complejidad en las contraseñas, el control de dispositivos externos a la red, la segregación lógica de acceso a la información son ejemplos de otras medidas imprescindibles para garantizar el aseguramiento de la información.

Mantenimiento de la seguridad

La implantación de todas estas medidas siempre debe ir seguida por su mantenimiento, evolución y adaptación constante, llevados a cabo a través de la revisión periódica de los controles de seguridad implantados, la realización continua del análisis de riesgos, la adaptación a los resultados obtenidos en éste, la corrección de fallos de seguridad detectados, la implantación de nuevas medidas desarrolladas para paliar nuevos riesgos y las auditorías periódicas encaminadas a la detección de desviaciones en el cumplimiento de las medidas establecidas.

Un papel protagonista en el mantenimiento de la seguridad lo tiene sin duda alguna la difusión y concienciación en materia de seguridad: unas medidas implantadas y olvidadas son un fracaso. Es fundamental llevar a cabo una concienciación permanente en esta materia mediante el acercamiento al negocio y al usuario.

En muchas ocasiones, si bien se trabaja en la divulgación de las medidas de seguridad, éstas se encuentran en un plano tan alejado del día a día de las diferentes áreas que su aplicación no resulta inmediata, provocando un incumplimiento de las mismas.

Costes colaterales

Todo lo que se ha mencionado hasta ahora va encaminado a construir la seguridad de una organización, pero ¿qué impacto económico tiene más allá de la inversión inicialmente planificada?

Además del inmediato, es decir, además del derivado de la inversión en las infraestructuras y medios necesarios para la identificación y puesta en marcha de las mismas, sin olvidar el mantenimiento y evolución de éstas, existen otros costes que pueden denominarse "colaterales" que deben ser tenidos muy en cuenta.

Estos costes se producen a partir de la aplicación de medidas de seguridad principalmente centradas en controlar uno de los aspectos que hemos mencionado anteriormente: la protección de los equipos con los que se accede a los sistemas que contienen la información (descargas ilegales de *software*, utilización de correo público, evolución del *software* hacia versiones mantenidas, etc.).

La tabla siguiente recoge un resumen de algunos de estos "costes colaterales", reflejando las medidas y el impacto económico que producen la aplicación de las mismas.

Tabla 4. Controles e impacto

CONTROL DE SEGURIDAD	IMPACTO
Descarga de *software* no adquirido (Acrobat Reader, Winzip…)	Coste directo de la inversión en la adquisición de este *software* imprescindible para el funcionamiento de la organización
Negación de acceso a correo no corporativo	Coste directo de la inversión en la ampliación del tamaño de los buzones corporativos (muchas veces los empleados utilizan sus correos personales, sin límite en el tamaño de los correos, para intercambiarse información ante la imposibilidad de utilizar las cuentas corporativas por sus limitaciones
Evolución de todo el *software* a versiones en activo por los fabricantes	Costes derivados de la propia adquisición de nuevas licencias en activo Costes derivados de la adaptación de otro *software* dependiente de este *software* de base (aplicaciones corporativas hechas a medida y no mantenidas y evolucionadas)
Control de acceso a determinadas páginas	Costes derivados de la aplicación y mantenimiento de dicho control Costes derivados del impacto en el día a día de la aplicación de este control de manera generalizada Costes derivados de las vulnerabilidades ocasionadas por los empleados para "saltar" este control

En resumen

La seguridad de la información es esencial. Los fallos de seguridad producen impacto tanto económico como en la imagen para la compañía. El aseguramiento de la información pasa por el compromiso de la dirección, la concienciación de la compañía, el establecimiento de objetivos y la dotación de medios tanto económicos como humanos para la consecución de los mismos.

La definición de una política global de seguridad debe ser la primera materialización de los objetivos marcados. A dicha política habrá que sumar todos los procedimientos e instrucciones que sean necesarios para dar cobertura a todos aquellos aspectos de seguridad a tratar.

Conocer el punto al que se quiere llegar en esta materia es fundamental; conocer el punto de partida también lo es. Este punto de partida se obtiene a partir del análisis de diferentes factores como negocio, información que se maneja, espacio geográfico, legislación que aplica y compromisos de seguridad. El estudio de estos aspectos se materializará en un análisis de riesgos que arrojará como resultado la identificación de las amenazas sobre los activos de información. Llegados a este punto, la dirección deberá gestionar o asumir dichos riesgos. El tratamiento de los mismos impactará en la definición de los controles de seguridad a implantar.

Las medidas o controles de seguridad a implantar deben estar orientados tanto a los sistemas que contienen los datos como a los sistemas que se utilizan para acceder a los mismos, así como al espacio físico en el que están albergados, siempre teniendo en cuenta que tales medidas estarán encaminadas a mitigar los riesgos (impacto, probabilidad).

No sólo se debe pensar en medidas orientadas a la seguridad informática, sino que es necesario crear todo un engranaje de seguridad sobre el que pivoten todas las actividades llevadas a cabo en la compañía.

La seguridad de la información necesita de un continuo mantenimiento, evolución y adaptación. La divulgación y concienciación son elementos fundamentales para garantizar el éxito.

Conclusiones

Hoy en día la continuidad de un negocio pasa por la definición, implantación, mantenimiento y evolución de una estrategia de seguridad global marcada por la dirección de la compañía y seguida por toda la organización. Esta estrategia debe contemplar todos los aspectos (generales, técnicos, normativos, legislativos, económicos) en los que deben aplicarse medidas de seguridad, es decir, debe de ser una estrategia para la seguridad de la información y no una estrategia de seguridad informática. Esta estrategia de seguridad de la información debe incluir tanto medidas orientadas a garantizar la seguridad informática como medidas más generalistas, todas ellas definidas de manera adaptada la negocio.

La dirección de una compañía debe mostrar un compromiso firme con la seguridad de la información, evitando la creación de nichos de seguridad no alineados con los objetivos marcados.

El mantenimiento, evolución y adaptación de la seguridad deben ser una constante en las organizaciones; la concienciación tiene un papel protagonista.

La implantación, mantenimiento y evolución de esta estrategia de seguridad tiene asociados unos costes directos e indirectos que deben estar presentes a la hora de definir objetivos y establecer el presupuesto con el que se dota, sin olvidar la criticidad de la seguridad que hemos revisado en el presente artículo y las consecuencias nefastas que una estrategia errónea y limitada pueden suponer para la compañía. ■