

CURSO INTRODUCCIÓN A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN


1. CONCEPTOS BÁSICOS SOBRE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información cuenta con numerosos vocablos que no son de uso cotidiano y que dificultan a veces el entendimiento de los conceptos. Vamos a clarificar en primer lugar estos términos para que los distintos aspectos que se van a tratar sean fácilmente comprensibles.

1.1 CONCEPTOS BÁSICOS

1.1.1 ¿Qué entendemos por seguridad de la información?

Para comprender qué es la seguridad de la información, en primer lugar, debemos conocer que la información en esta área es referida a los activos de información (es decir, los datos por supuesto, pero también los equipos, las aplicaciones, las personas, que se utilizan para crear, gestionar, transmitir y destruir la información), que tienen un valor para la organización.

En las complejas organizaciones de hoy en día,  se recogen, gestionan y transmiten multitud de datos a través de diferentes medios, a mucha gente, y todas las acciones relacionadas con ello pueden necesitar protección.

No se debe confundir la seguridad de la información con la seguridad informática ya que la seguridad de la información abarca muchas más áreas mientras que la seguridad informática se encarga de la protección de las infraestructuras TIC que soportan el negocio. Por tanto la seguridad de la información abarca la seguridad informática.

La seguridad de la información, por tanto, se puede definir como la protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización.

Estos tres parámetros básicos de la seguridad se definen como:

- **Confidencialidad:** A la información solo pueden acceder las personas autorizadas para ello.
- **Integridad:** La información ha de estar completa y correcta en todo momento.
- **Disponibilidad:** La información estará lista para acceder a ella o utilizarse cuando se necesita.



Figura 1. Parámetros básicos de la seguridad de la información

Dependiendo de los modelos utilizados o de las necesidades del negocio, también son parámetros a tener en cuenta:

- **Autenticidad:** La información es lo que dice ser o el transmisor de la información es quién dice ser.
- **Trazabilidad:** Poder asegurar en todo momento quién hizo qué y cuándo lo hizo.

En cualquier organización existen datos de clientes o usuarios, esta información necesita protección:

Si accediera a ella alguien de la competencia podría utilizarla para conseguir beneficios económicos, o bien denunciar a la organización ante la Agencia de Protección de Datos para que se le impusiera una multa si se demuestra que se vulneró la Ley de Protección de Datos de Carácter Personal, o publicarla en la prensa para dañar la imagen de la organización. Un fallo de confidencialidad puede ser tremendamente dañino.

Si la información se corrompe, se podrían enviar cartas o facturas erróneas a los clientes, con la confusión y las quejas de los afectados que acarrearía, más el trabajo y el tiempo que habría que emplear para corregir los errores y restaurar a su estado correcto la información. Que la información permanezca íntegra en todo momento es más importante de lo que a primera vista pueda parecer.

Si el equipo en el que reside esta información se estropea y no se puede acceder a ella, simplemente no se puede funcionar, no se puede dar servicio, lo que implica que se deja de ganar dinero y en casos extremos se puede perder, si el cliente decide marcharse y adquirir el servicio en otro proveedor. Un fallo de disponibilidad tiene siempre un impacto económico directo en la organización, por leve que sea, ya que se deja de trabajar, hay una parte de la organización que ha parado, por lo que ha dejado de generar beneficio.

1.1.2 ¿Qué entendemos por seguridad de la información?

Un fallo de seguridad es cualquier incidente que la compromete, es decir que pone en peligro cualquiera de los parámetros con los que se valora la seguridad: la confidencialidad, la disponibilidad o la integridad de la información. Con la actual complejidad de los sistemas de información, con una economía y un comercio que se basan en intercambios y comunicaciones a lo largo y ancho del mundo, con un número creciente de usuarios que no sólo se conectan desde dentro sino también desde fuera de la organización, es fácil hacerse una idea del reto que presenta evitar que sucedan cosas como:

- Fallos en las comunicaciones.
- Fallos en el suministro eléctrico.
- Fallos humanos de usuarios internos, usuarios externos, administradores, programadores, etc.
- Fallos en los sistemas de información: redes, aplicaciones, equipos, etc.
- Virus informáticos, gusanos, troyanos, etc. que inundan la red.
- Accesos no autorizados a los sistemas o la información.
- Incumplimiento de una ley o un reglamento.

Los fallos de seguridad son ocasionados muchas veces por la errónea percepción de que si la seguridad física está razonablemente asegurada, no tiene por qué haber problemas. O que protegiendo únicamente las aplicaciones y las bases de datos ya está garantizada la seguridad. Con esos supuestos se dejan desprotegidas muchas áreas de la organización, muchos activos de información que pueden ser fácilmente dañados o destruidos, ya que no se han tenido en cuenta todos los aspectos de la seguridad de la información: la seguridad física, la seguridad lógica y las medidas organizativas.

1.1.3 ¿Qué son los Sistemas de Gestión de la Seguridad de la Información (SGSI)?

Hasta ahora lo más común ha sido ir parcheando los agujeros de seguridad con medidas puntuales, descoordinadas y poco proporcionadas al riesgo que reducen. Se trata de medidas cuya implantación y efectividad no son llevadas a cabo y controladas de manera planificada. El resultado es obvio, se siguen manteniendo altos niveles de riesgo frente a las amenazas.

Todos estos incidentes que amenazan la seguridad de la información requieren, cada día más, de sistemas de gestión acordes con el valor de la propia información y de los sistemas informáticos que los tratan. Las directrices, procedimientos y controles de seguridad que se utilizan para gestionar esta seguridad es lo que conocemos por Sistema de Gestión de Seguridad de la Información o SGSI.

De una manera más estricta, un Sistema de Gestión de Seguridad de la Información es aquella parte del sistema general de gestión de una organización que comprende:

- la política.

ING. FERNANDO CARPENTIERI
SISTEMAS DE GESTIÓN
CAPACITACIÓN Y ASISTENCIA TÉCNICA

- la estructura organizativa.
- los procedimientos.
- los procesos y
- los recursos necesarios,

para implantar la gestión de la seguridad de la información.

Con un sistema de gestión de seguridad de la información nos aseguraremos de cubrir todos los aspectos de seguridad tomando medidas encaminadas a reducir paulatinamente los riesgos a los que la organización se enfrente.

A pesar de lo que puede parecer en un principio, la definición e implantación de un SGSI no debería ser ni un coste ni un esfuerzo relevantes, máxime teniendo en cuenta los beneficios que conlleva. Un SGSI debe ajustarse tanto a los requisitos del negocio como a los recursos disponibles y debe solucionar los problemas que tiene planteados el negocio pero siempre dentro de lo razonable en cuanto a esfuerzos y costes.

Como cualquier sistema de gestión, el SGSI debe ayudar a conseguir los objetivos de la organización, no convertirse en un impedimento para ello.

Un SGSI contiene en primer lugar, las pautas que se van a seguir en la organización para garantizar la seguridad de la información y las responsabilidades de cada cual al respecto.

El SGSI recoge los objetivos que se pretenden obtener y los medios con que se va a contar para ello. Para determinar ambas cosas, se realiza un análisis de riesgos que da la medida de hasta qué punto los activos están expuestos a que les ocurran fallos de seguridad y cuál sería el impacto en caso de que lleguen a ocurrir.

Con esa información se establece el punto de partida, cual es el estado en el que está la seguridad y se decide cual se pretende conseguir, así como cuál es el objetivo para un periodo de tiempo determinado. A partir de ahí, se deciden las acciones a tomar para reducir esos riesgos al nivel que se decidió que sea el objetivo. Por ejemplo, si se ha averiguado que un determinado servidor es un activo expuesto a un gran riesgo y debe estar funcionando 24 horas al día, para reducir el riesgo de que se pare, puede ser necesario instalar un SAI o incluso una línea alternativa de suministro eléctrico, realizar un mantenimiento exhaustivo mensual, instalar un equipo duplicado de manera que si falla uno el otro siga funcionando, etc.

Las acciones que se tomen deben documentarse dentro del SGSI, mediante procedimientos y planes para su ejecución.

Por tanto, definiremos un Sistema de Gestión de Seguridad de la información (SGSI) como la manera en la que una organización **conoce** los **riesgos** a los que está sometida su **información** y los **gestiona** mediante una **sistemática** definida, documentada y conocida por todos, **que se revisa y mejora constantemente**.

2. BENEFICIOS

Existen numerosas e importantes razones para afrontar el desarrollo y la implantación de un Sistema de Gestión de la Seguridad:

Reducción de costes. Esta debería ser una de las principales motivaciones para llevar a cabo la implantación de un SGSI, ya que incide directamente sobre la rentabilidad económica de una organización. No suele serlo porque lo que se ve en un principio es el coste del mismo, sin embargo, en un breve plazo, se puede observar como el SGSI evita varias situaciones que suponen un coste, a veces importante. Al detectar los principales focos de fallos y errores, y eliminarlos o reducirlos hasta donde es posible, se evitan costosos incidentes de seguridad, que hasta entonces se asumían como cosas que pasan. A veces se evitan incidentes que hubieran ocurrido de no haber tomado las medidas a tiempo, y eso es difícil de cuantificar, pero no por ello es menos real. A veces los beneficios surgen de manera imprevista, como la reducción de primas de seguros en algunas pólizas debido a la justificación de la protección de los activos asegurados.

Optimizar los recursos y las inversiones en tecnología. Con un SGSI las decisiones se tomarán en base a información fiable sobre el estado de los sistemas de información y a los objetivos de la organización. Habrá una motivación de negocio detrás de estas decisiones, por lo que la dirección podrá comprenderlas y apoyarlas de manera más consciente. La organización dejará de depender exclusivamente de la experiencia o pericia del responsable de informática, o más peligroso aún, del proveedor habitual de informática, a la hora de valorar las distintas opciones de compra.

Protección del negocio. Con un SGSI en marcha se evitan interrupciones en el flujo de ingresos, ya que se está asegurando de una manera eficaz la disponibilidad de los activos de información y, por lo tanto, de los servicios que la organización ofrece. Esto en cuanto a la actividad cotidiana, pero también se está preparado para recuperarse ante incidentes más o menos graves e incluso garantizar la continuidad del negocio, afrontando un desastre sin que peligre el negocio a largo plazo.

Mejora de la competitividad. Cualquier mejora en la gestión de la organización redundará en beneficio de la eficacia y la eficiencia de la misma, haciéndola más competitiva. Además hay que considerar el impacto que suponen el aumento de la confianza de los clientes en nuestro negocio, la diferenciación frente a los competidores y una mejor preparación para asumir retos tecnológicos.

Cumplimiento legal y reglamentario. Cada vez son más numerosas las leyes, reglamentos y normativas que tienen implicaciones en la seguridad de la información. Gestionando de manera coordinada la seguridad tenemos un marco donde incorporar los nuevos requisitos y poder demostrar ante los organismos correspondientes el cumplimiento de los mismos.

Mantener y mejorar la imagen corporativa. Los clientes percibirán la organización como una empresa responsable, comprometida con la mejora de sus procesos, productos y

servicios. Debido a la exposición de cualquier organización a un fallo de seguridad que pueda acabar en la prensa, este punto puede ser un catalizador de esfuerzos, ya que nadie quiere que su marca quede asociada a un problema de seguridad o una multa por incumplimiento, por las repercusiones que acarrea.

Beneficios de la implantación de un SGSI



Figura 2. Beneficios de la implantación de un SGSI

3. DELITOS TECNOLÓGICOS

3.1 Definición y tipos de delitos tecnológicos

Con la expresión delito tecnológico se define a todo acto ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

Una clasificación puede ser:

ING. FERNANDO CARPENTIERI

SISTEMAS DE GESTIÓN CAPACITACIÓN Y ASISTENCIA TÉCNICA

- Ataques que se producen contra el derecho a la intimidad. Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos.
- Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor. Especialmente la copia y distribución no autorizada de programas informáticos y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas.
- Falsificación de documentos. Entendiendo documento como todo soporte material que exprese o incorpore datos, aunque se extiende también a la falsificación de moneda y a las tarjetas de débito y crédito. También pertenece a este grupo la fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad
- Sabotajes informáticos. Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. • Fraudes informáticos. Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito.
- Amenazas. Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal).
- Calumnias e injurias. Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión.
- Pornografía infantil. Existen varios delitos en este epígrafe:
 - La inducción, promoción, favorecimiento o facilitación de la prostitución de una persona menor de edad o incapaz.
 - La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido.
 - La facilitación de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...).
 - La posesión de dicho material para la realización de dichas conductas.