Implantación y organización de Sistema de Gestión de Seguridad de la Información (SGSI)

Adrián García García
Fundamentos de criptografía y seguridad informática

Índice

Introducción

En la actualidad, la mayoría de empresas, organizaciones, tiendas locales e, incluso, particulares ponen a nuestra disposición productos y servicios a través de Internet, obligándonos a poner para ello determinada información valiosa que no queremos que salga a la luz. Es raro ver que alguien no haya realizado una compra online, no haya aceptado cookies o, directamente, no se haya registrado nunca en ningún lugar de la red.

Nos encontramos en una situación en la que se podría decir que las empresas tienen más información nuestra que nosotros mismos. Sin embargo, hemos visto a lo largo de los años como se ha filtrado, han vendido o incluso han chantajeado por determinada información confidencial. ¿Creéis que las empresas distribuyen correctamente la información? ¿Consideráis que nuestros datos personales se encuentran seguros ante cualquier riesgo?

A continuación, se expone como las empresas, organizaciones o particulares pueden garantizar que los activos de información de los que disponen se encuentren seguros ante cualquier riesgo mediante los Sistemas de Gestión de Seguridad de la Información.

Desarrollo

Antes de hablar de lo que es un Sistema de Gestión de Seguridad de la Información, debemos dejar claro que es lo que entendemos por información o activos de una empresa y/o organización. La información o activos consiste en el conjunto de datos organizados y completos que se encuentran en poder de una empresa y/o organización y se considera importante, independientemente de la fecha de su creacción, su localización geográfica, su origen y su modo de propagación. Cualquier organización, independientemente de su lugar geográfico, tamaño y tipo de negocio, recopila, almacena y distribuye información, todos ellos activos importantes para lograr los objetivos de la organización.

La definición exacta de los Sistemas de Gestión de Seguridad de la Información que se muestra a continuación ha sido extraída de la página oficial del estandar ISO 27000:

“Un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales.

Un SGSI desde la visión de el estándar internacional ISO/IEC 27001 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio (p.ej. en empresas públicas, organizaciones sin ánimo de lucro, ...).”

Un Sistema de Gestión de Seguridad de Información, en adelante SGSI, se basa en el manejo de la protección de los activos de una empresa con el fin de alcanzar los objetivos de negocio. Para garantizar un correcto funcionamiento, los SGSI deben realizar continuamente los siguientes pasos:

1. Analizar los requisitos de seguridad y los activos de información. En este paso se debe tener en cuenta el tamaño, el modelo de negocio, los objetivos generales y la distribución geográfica de la empresa.
2. Evaluar los posibles riesgos que pueden sufrir dichos activos, teniendo en cuenta las amenazas, los factores que pueden ser vulnerables, las posibles consecuencias del incidente, confidencialidad, integridad y disponibilidad.
3. Evaluar, seleccionar y aplicar los controles y las medidas necesarias para gestionar los posibles riesgos que no se puedan aceptar. Los riesgos se pueden gestionar de cuatro formas:
    1. Aceptar el riesgo
    2. Reducir el riesgo
    3. Transferir el riesgo a un lugar seguro
    4. Evitar el riesgo suprimiendo las causas que puedan ocasionarlo
4. Analizar, mejorar y mantener todo lo expuesto en los anteriores pasos para mantener una gran eficacia en la seguridad de los activos.

Una correcta implementación del SGSI consiste en como analizar los requisitos necesarios para la protección de la información y los controles, pruebas y supervisiones que garanticen dicha protección.

La implantación de estos sistemas y su mantenimiento debe ser considerado un nuevo proyecto que controla la organización y/o empresa. Dicha implantación presenta grandes beneficios. Entre ellos destacan la reducción de riesgos de seguridad de la información, reduce la probabilidad y el impacto de los riesgos, cumple la certificación del estándar internacional y presenta ventajas de marketing.

El ISO/IEC 27001 supone un estándar internacional donde se especifica, mediante un enfoque de mejora continua, un plan para mejorar, implantar, mantener y establecer un SGSI con el nombre Ciclo de Deming. Este ciclo está compuesto de cuatro fases:

1. Planificar (Plan): fase de diseño donde se localizan los posibles riesgos de seguridad y se seleccionan los controles más adecuados a la organización.
2. Hacer (Do): fase donde los controles se establecen y operan.
3. Controlar (Check): fase donde se analiza y controla la efectividad y el desempeño del SGSI.
4. Actuar (Act): con el fin de obtener el máximo beneficio de los SGSI, se analizan posibles puntos donde la eficacia es menos deseada y se aplican diferentes cambios que puedan obtener el máximo rendimiento posible.

Cuando se habla de la seguridad de la información se debe hacer hincapié en las dimensiones fundamentales representadas en el ISO/EC 27001. Estos fundamentos son los siguientes (los tres incluidos como requisito fundamental en el ISO/EC 27001):

- Confidencialidad: acceso a la información solo por quienes están autorizados.

- Disponibilidad: acceso continuo a los activos siempre que se requiera.
- Integridad: mantenimiento de la información de forma completa y exacta.

Un SGSI debe determinar si conviene incluir alguna dimensión más de forma opcional basándose en las necesidades de la empresa, como por ejemplo el no repudio, autenticidad o trazabilidad entre muchas otras. Partiendo de que conseguir completa inmunidad es imposible (incluso cuando se cuenta con presupuesto ilimitado), lo que se busca con el estándar mencionado anteriormente y los SGSI es garantizar la confidencialidad, disponibilidad e integridad de la información y que los posibles riesgos que puedan existir sean conocidos, analizados, gestionados y resueltos.

A la hora de implantar el estándar ISO/IEC 27001, todas aquellas organizaciones y/o empresas que hayan añadido rigurosamente las exigencias legales de protección de datos parten de una situación más ventajosa. En España, nos encontrados con dos exigencias legales en torno a la protección de datos: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y Ley de Servicios de la Sociedad de la Información(LSSI).

La LOPDGDD obliga a las personas, organismos y empresas tanto públicas como privadas a cumplir una serie de requisitos por sus datos personales (aquella información que identifique a una persona) y, dependiendo del tipo e importancia de datos que posean, aplicar unas medidas u otras. Su finalidad es proteger la integridad, privacidad e intimidad de los individuos y garantizar seguridad en los intercambios de información.

La LSSI es la ley que se establece para regular todas las actividades comerciales que tienen lugar en Internet. Dichas actividades engloba a todos los servicios y productos ofrecidos en las páginas web, en los correos electrónicos y en las tiendas online. Su finalidad es que todas las transacciones online tengan el mismo trato que las realizadas en un entorno físico. Para ello, se debe informar al comprador (incluyendo el aviso legal, la política de privacidad y la política de cookies), durante las comunicaciones comerciales está prohibido el uso de sus datos personales si no hay consentimiento y, a la hora de la contratación, se debe incluir las condiciones generales de contratación.

A partir de estas leyes, también es recomendable incluir el estándar X.800. El estandar X.800 describe las características necesarias para que la conexión entre dos sistemas sea segura. No es una implementación, solamente describe los aspectos básicos para proteger las comunicaciones. Los servicios de seguridad que se detallan en el estándar son:

1. Autenticación: verifica que la entidad, organización o persona conectadas en la comunicación son verdaderas.
2. Control de acceso: protege el acceso no autorizado a los recursos.
3. Confidencialidad (explicada anteriormente)
4. Integridad (explicada anteriormente)
5. No repudio: este servicio proporciona la verificación del envío de mensajes o recepción de ellos.

Para el cumplimiento de estos servicios, el estándar X.800 nos plantea varios mecanismos de seguridad. Entre estos, destaca realizar cifrados, utilizar la firma digital, añadir padding adicional,

realizar un proceso de autenticación o mantener el control de enrutamiento. Todos estos mecanismos por separado no cumplen los 5 servicios esenciales que se tratan en el estándar, por lo que lo ideal sería utilizar varios de ellos.

Un Sistema de Gestión de Seguridad Informática se encarga del análisis, manejo y clasificación de los riesgos contra los activos de una empresa y/o organización y del desarrollo de controles que puedan mantener segura la información. Según el estándar internacional ISO/IEC 27001, los SGSI deben garantizar, al menos, la confidencialidad, la integridad y la disponibilidad de los activos.

Conclusión

Además del estándar ISO/IEC 27001, se debe cumplir las exigencias legales de protección de datos que correspondan (en España la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales y la Ley de Servicios de la Sociedad de la Información). Para añadir aún más seguridad, es recomendable incluir el estándar X.800 para aumentar la seguridad en las comunicaciones y transferencia de activos.

Bibliografía

[1] https://www.ceupe.com/blog/sistema-de-gestion-de-la-seguridad-de-la-informacion.html

[2] https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

[3] https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/

[4] https://www.iso27000.es/sgsi.html

[5] https://es.wikipedia.org/wiki/ISO/IEC_27001

[6] https://www.normas-iso.com/iso-27001/

[7] https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/

[8] https://ayudaleyprotecciondatos.es/2019/03/15/guia-sobre-lssi-ce-que-es-como-cumplir-la-ley-este-2019/

[9] https://protecciondatos-lopd.com/empresas/lssi-ce/

[10] https://es.wikipedia.org/wiki/X.800

[11] https://www.youtube.com/watch?v=6EzxwyTObKg