Fecha: 30-6-2024
Autor: Jorge Chinea
Empresa: INTECO-CERT (Instituto Nacional de Tecnologías de la Comunicación)
Edición: 1

Seguridad de la Información

¿Qué es?

Se entiende por seguridad de la información (SI en adelante) a todas aquellas medidas preventivas y reactivas de una organización que permitan resguardar y proteger la información buscando mantener las siguientes características de la información:

• Su Confidencialidad: consiste en evitar que personas, programas o sistemas no autorizados puedan acceder a ella sin autorización.

• Su Integridad: es la característica de la información relativa a su fiabilidad. Su protección consiste en que la información no sea alterada o modificada sin autorización.

• Su Disponibilidad: este aspecto hace referencia a que la información esté accesible, es decir, disponible para su utilización cuando sea necesaria.

La SI tiene en cuenta no solamente la seguridad tecnológica, sino también otras facetas de la seguridad, como son la seguridad desde el punto de vista jurídico, desde el punto de vista normativo y desde el punto de vista organizativo.

¿Para qué sirve?

- Ayuda a identificar los riesgos y las amenazas de una organización
- Es un camino para identificar malos hábitos y usos inadecuados de la información
- Permite reducir al mínimo las interrupciones de la actividad de una organización
- Genera confianza en los clientes que depositan información relevante en la organización

Explicación

La Seguridad de la Información se basa en un marco legal relacionado con las tecnologías de la información que está compuesto por un conjunto de normativas y leyes vigentes en España. La más conocida es la LOPD (Ley Orgánica 15/1999, de 13 de diciembre de protección de datos), que tiene por objeto garantizar y proteger el tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Además, existen otras normativas importantes como

- Ley de servicios de la Sociedad de la Información y de comercio electrónico (LSSI) que regula el comercio electrónico en España
- Ley para el impulso de la Sociedad de la Información (LISI)
- Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos
- Ley de Firma Electrónica, etc.

Se recomienda contar con asesores profesionales que nos ayuden a determinar qué normativas nos aplican y qué debemos cumplir en función de nuestro sector de actividad, tipo de datos que manejamos, procesos, etc.La SI aplicada al negocio tiene tres facetas principales: responsabilidad y productividad, imagen y competitividad y contingencias y continuidad de la actividad.

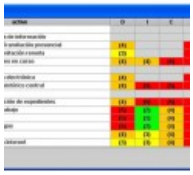
- La responsabilidad y la productividad deben ser una parte fundamental de cualquier organización. La SI ayuda a fomentarlas y reduce los riesgos de seguridad derivados de la falta de éstas. La SI además promueve los buenos hábitos, las buenas prácticas y las políticas de seguridad además de fomentar la responsabilidad entre todos los miembros de una organizació
- La SI puede ayudarnos a conseguir una mejor imagen de cara a nuestros clientes, proveedores y usuarios. La SI es capaz de que logremos una diferenciación ante nuestros competidores, mediante el cumplimiento de normativas o la aplicación de estándares de seguridad, como un SGSI. Es de mencionar que la SI es una labor de todos los empleados y tiene que existir conciencia e implicación por parte de todos los miembros de una organización.
- La capacidad para superar contingencias es otra característica necesaria para las organizaciones por la que se pretende reducir al mínimo las interrupciones de la actividad debido a incidentes de seguridad. La continuidad del negocio se ocupa de la supervivencia de una organización ante cualquier incidente o contingencia que pueda poner en peligro su continuidad a corto, medio o largo plazo. En la implantación de planes de contingencia o de continuidad de negocio es fundamental conocer los riesgos a los que estamos expuestos y el tiempo de recuperación en caso de producirse un incidente o contingencia.

La SI además ayuda a identificar los riesgos y las amenazas a las que está expuesta una organización, en qué medida pueden afectar al trabajo y a los objetivos de organización y cómo se pueden minimizar. En el caso de que se produzca algún problema, nos ayuda a establecer pautas y procedimientos para reducir sus consecuencias.La SI también es un camino para identificar malos hábitos y usos inadecuados de los recursos de la organización, y buscar la manera de implementar buenas prácticas y hábitos más correctos y responsables.

Estos hábitos no tienen por qué ser necesariamente perjudiciales pero pueden poner en riesgo la actividad de una organización en forma de pérdida de tiempo, retrasos en la actividad, uso inadecuado de los recursos disponibles, etc. Todo ello puede generar riesgos para la seguridad y por tanto, puede acarrear problemas relacionados con la integridad, la disponibilidad y la confidencialidad de la información.

Si quiere conocer otros conceptos de gestión, puede acceder a la plataforma abierta y gratuita http://sugestion.quned.es/ que es un proyecto de Responsabilidad Social Intelectual de la Cátedra de Calidad de la Universidad Nacional de Educación a Distancia (UNED) compartido con los profesionales que han redactado las fichas.

Ejemplos prácticos



Aplicaciones y soportes frecuentes

REDER	Algunas Aplicaciones	Algunos Soportes Observables
R	Establecer criterios de tolerancia en variables críticas de información	Estándares en variables críticas
E	Preparar acciones preventivas y correctivas (de choque) para posibles situaciones críticas	Plan de Seguridad en la Información
D	Comunicación para la concienciación y adquisición de buenos hábitos	Guía de buenas prácticas
E	Evaluación de riesgos y ejecución del plan	Informes de riesgos y de desarrollo del Plan
R	Análisis de impactos	Informes de Amenazas e Impactos

Cuestiones clave para autoevaluar

¿Existe ambiente de seguridad en su organización?	1 2 3 4 5 6 7 8 9 10
¿Cuenta su organización de plan de seguridad?	1 2 3 4 5 6 7 8 9 10

¿Se realizan en su organización auditorías de seguridad periódicas?	1	2	3	4	5	6	7	8	9	10
¿Se realizan en su organización campañas de concienciación de seguridad periódicas?	1	2	3	4	5	6	7	8	9	10
Dispone su empresa de un responsable de Gestión de la Información	1	2	3	4	5	6	7	8	9	10
¿Se hecho en su organización una evaluación de riesgos de seguridad?	1	2	3	4	5	6	7	8	9	10
¿Dispone su organización de un plan de contingencia?	1	2	3	4	5	6	7	8	9	10
¿Se encuentran definidos en algún sitio los activos de información de su organización?	1	2	3	4	5	6	7	8	9	10
¿Realizan los trabajadores cursos de seguridad de la Información?	1	2	3	4	5	6	7	8	9	10
¿Se investigan los incidentes de seguridad y se toman las medidas necesarias para que no vuelvan a ocurrir?	1	2	3	4	5	6	7	8	9	10

Información adicional del autor

Autor: Jorge Chinea — Cargo:

Empresa/organización: INTECO-CERT (Instituto Nacional de Tecnologías de la Comunicación)

Actividad: Apoyo preventivo y reactivo en materia de Seguridad en TIC — Contacto: www.cert.inteco.es