La Seguridad en tu Empresa

Investigador Edwin Morales*

2025, v-1.0.0

La seguridad de la información es un concepto amplio que busca proteger los activos de información de una organización. La ciberseguridad se centra en proteger los activos en el ciberespacio, mientras que la seguridad informática se especializa en proteger los sistemas informáticos. La norma ISO/IEC 27000 es la principal referencia global para gestionar la seguridad de la información.

Palabras-Clave: Seguridad, Ciberseguridad, Información, Sistema, Gestión.

Introducción

En esta era digital, la protección de la información se ha vuelto fundamental para todos principalmente para las empresas que tiene que cuidar no solo la reputación de su empresa sino la proteger a sus clientes. La ciberseguridad, la seguridad informática y la seguridad de la información son términos a menudo usados indistintamente como que fueran un solo tema a tratar, pero que se refieren a conceptos distintos. La ISO/IEC 27000 es una norma internacional que provee un marco para gestionar la seguridad de la información en las empresas.

[1].

1 Desarrollo del Tema

Hoy en dia muchos de nosotros escuchamos el tema de seguridad y en ocasiones se trata de enfocar el tema de seguridad en estos 3 conceptos que referencian al tema de seguridad, pero hay que aclarar que cada uno de ellos conlleva temas independientes y alcances en las diferentes areas de las empresas, estas son, laCiberseguridad, Seguridad Informática y la Seguridad de la Información.

Acá podremos aterrizar mejor cada uno de estos conceptos para enforcarnos en el alcance de cada uno de ellos.

*emoralesm@miumg.edu.gt

[1] <http://www.latex-project.org/lppl.txt>

2 Seguridad de la Información

Es un término más amplio. Se enfoca en la protección de la información, sin importar su formato (digital o físico). Su objetivo es mantener la confidencialidad, la integridad y la disponibilidad de los datos. Esto incluye documentos en papel, conversaciones orales e información digital.

2.1 Seguridad Informática

Es una parte de la seguridad de la información. Su alcance se limita a la protección de los sistemas informáticos y los datos que contienen. Incluye la protección de hardware, software y redes contra daños, accesos no autorizados o interrupciones.

2.2 Ciberseguridad

A esta la podemos identificar como una disciplina, aún más específica y que se enfoca en proteger de ataques cibernéticos los activos en el ciberespacio; esto incluye sistemas, redes, programas y datos de la empresa o clientes.

2.3 Marco de Referencia

Esta norma ISO/IEC 27000 es una familia de normas internacionales que ayuda a las organizaciones a gestionar la seguridad de la información. No es una herramienta técnica, sino un marco de gestión que provee directrices y requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La 27001: Es la norma principal y contiene los requisitos para establecer un SGSI. Una organización puede obtener una certificación en esta norma, lo que demuestra su compromiso con la seguridad de la información en su compañia.

ISO/IEC 27002: Es una norma complementaria que proporciona un código de buenas prácticas para la implementación de controles de seguridad de la información.

Muy importante saber que estas 2 ultimas, una gestiona el Qué? "27001", en esta ISO se establecen los requisitos para un SGSI, su principal objetivo es proporcionar a las empresas un marco para **identificar, analizar y gestionar los riesgos de seguridad de la información**. Al implementar esta norma, una empresa se compromete a:

Identificar sus activos de información: Saber qué información es valiosa y necesita ser protegida.

Evaluar los riesgos: Determinar las amenazas y vulnerabilidades que podrían afectar a esos activos.

Seleccionar los controles adecuados: Elegir las medidas de seguridad para mitigar los riesgos.

Monitorear y mejorar: Revisar constantemente la efectividad del SGSI y hacer los ajustes necesarios.

A este ISO se le llama el "libro de reglas"para la seguridad. Te obliga a establecer un plan de gestión de riesgos y a documentar todo el proceso.

En contraparte se encuentra la 27002 "el Cómo?"; esta ISO no es certificable, pero es una guía de buenas prácticas que proporciona un conjunto detallado de controles de

seguridad de la información a la empresas. la **27002** te da ejemplos concretos de cómo implementar ese control. Los controles se dividen en cuatro categorías:

Controles Organizacionales: Guías sobre políticas de seguridad, roles y responsabilidades. Por ejemplo, te orienta sobre cómo crear una política de seguridad para el trabajo remoto.

Controles de Personas: Abordan el comportamiento humano. Por ejemplo, cómo capacitar a los empleados para que reconozcan un ataque de phishing o cómo gestionar las responsabilidades de los empleados al terminar su contrato.

Controles Físicos: Se refieren a la seguridad de las instalaciones y los equipos. Te da pautas para la protección de servidores, el control de acceso a oficinas y la eliminación segura de equipos para evitar un mal uso de ellos.

Controles Tecnológicos: Se centran en la tecnología. Aquí encuentras lineamientos sobre el uso de criptografía, la seguridad de las redes, la gestión de la capacidad de los sistemas y la protección contra malware.

2.4 Dónde se puede utilizar?

En la gestión de accesos Clasificación de los datos Incidentes de seguridad Continuidad y Riesgos Vulnerabilidades, malwares Concientización

Casos de Uso: Protección de datos de clientes, randsomwares, protección de la infraestructura, etc.

3 Conclusiones

La protección de la información es un proceso complejo que requiere un enfoque multifacético. La seguridad de la información es el concepto general, la seguridad informática y la ciberseguridad son sus componentes. La implementación de un SGSI basado en la ISO/IEC 27000 permite a las organizaciones gestionar eficazmente los riesgos y garantizar la continuidad de sus operaciones en un entorno cada vez más digital y vulnerable..

La Seguridad en tu Empresa

Investigador Edwin Morales[†]

2025, v-1.0.0

Key-words: Seguridad, Ciberseguridad, Información, Sistema, Gestión.

Referências

ISO official website ISO/IEC 27000 Agencias de Seguridad Gubernamentales: "NIST cybersecurity frameworkCISA cybersecurity guidance"

Organizaciones Profesionales: "ISACA publications(ISC)2 resources"

[†]emoralesm@miumg.edu.gt