Normatividad y estándares de la ciberseguridad

Existen varios estándares de seguridad informática, incluido el grupo de estándares **ISO/IEC 27000,** que hacen parte de un sistema de administración de seguridad de la información ***(information security management system ISMS)*** que va dirigido a la seguridad de la información, bajo un detallado control administrativo de la misma.

Conocer estos estándares a profundidad, para su aplicación, **es un deber de suma importancia**. Para que usted comience a familiarizarse con ellos, aquí se los enunciamos; tenga presente que puede estudiarlos en detalle, en distintas publicaciones que encontrará en la web o en las variadas fuentes de su confianza.

Comenzamos con el grupo de estándares **NIST**, en el cual se encuentra el **Marco para la mejora de la seguridad cibernética** en infraestructuras críticas.

Estándar ISO 15408

Estándar ISO 15408 permite que diferentes aplicaciones de *software* puedan ser integradas y probadas de forma o manera segura.

Estándar RFC 2196

Estándar RFC 2196 es un memorándum publicado por el ***Internet Engineering Task Force***, para el desarrollo de políticas y procedimientos de seguridad para sistemas de información conectados a Internet.

Para el campo industrial, se inició en el año 2007, con el grupo de trabajo de la ***International Society for Automation (ISA)***, el estándar ***ISA-99 denominado Security for Industrial Automation and Control Systems con la publicación del estándar ANSI/ISA-99.00.01-2007.***

ISA-99

ANSI/ISA-99.02.01-2009

A principios de 2009, fue aprobado por ANSI el estándar **ANSI/ISA-99.02.01-2009**, ***Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.***

Finalmente, en el año 2010, se cambió por el estándar **ISA/IEC 62443** para alinear la numeración de la documentación del estándar con los estándares correspondientes de la ***International Electrotechnical Commission (IEC).***

ISA/IEC 62443

Estándares de la Familia ISO

Es importante adoptar aspectos y lineamientos de la ***ISO 27001:2013 e ISO 27002.***

El Estándar ha sido preparado para otorgar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un **Sistema de Gestión de Seguridad de la Información (SGSI).** Los lineamientos determinados en este Estándar Internacional, son genéricos y fueron diseñados para ser aplicables a todas las organizaciones en general.

¿Cuáles son los objetivos de esta normatividad o estándares?

Mediante la aplicación y observancia de todos estos estándares, en cada caso se busca:

Brindar directrices de referencia que ayuden a obtener una buena gestión de riesgos de la seguridad de la información y de la ciberseguridad.

Propiciar una cultura de seguridad digital partiendo de la concienciación y capacitación del talento humano.

Ayudar a la protección de la triada de la seguridad de la información digital: confidencialidad, integridad y disponibilidad.

Alcance

La adopción de la normatividad y estándares de seguridad de la información y ciberseguridad es adecuada para implementarse en cualquier organización, sin importar las dimensiones, ya sean pequeñas empresas o grandes empresas.

Esto favorece a las organizaciones una adecuada evaluación de riesgos y la aplicación de los controles necesarios para eliminarlos o mitigarlos.

Características

La adopción de normatividad y estándares de seguridad de la información y ciberseguridad otorga una serie de características, entre ellas:

Enfocarse en el continuo proceso de mejora de su Sistema de Gestión de Seguridad de la Información.

Muestra de manera más clara los requisitos para la documentación y archivos.

Valoración de riesgos y procesos de gestión empleando un modelo de proceso, PHVA: Planificar, Hacer, Verificar, Actuar.

Sensibilización

Aplicación

La aplicación de normas y estándares está basada en las fases del ciclo PHVA, planear, hacer, verificar y actuar del Sistema de Gestión de Seguridad de la Información:

Planear: decreta el Sistema de Gestión de Seguridad de la Información (SGSI).

Hacer: opera el Sistema de Gestión de Seguridad de la Información (SGSI).

Verificar: monitorea y revisa el Sistema de Gestión de Seguridad de la Información (SGSI).

Actuar: mantiene y mejora el Sistema de Gestión de Seguridad de la Información (SGSI).