NORMAS Y ESTANDARES EN SEGURIDAD INFORMATICA

Fader Beltrán Ramos, Andrés Cuervo Montoya, Ana Milena Ruiz, Evelyn Patiño, Juan David Ramírez

Documento académico, donde se explican las Normas y Estándares en Seguridad Informática.

UNAD

Grupo: 301122_84

Octubre 2018

Normas y Estándares en Seguridad Informática

En la actualidad los ataques informáticos han aumentado considerablemente, razón por la cual se han creado Normas y Estándares de seguridad cuyo propósito es servir de herramienta para implementar buenas prácticas de seguridad informática en las empresas u organizaciones.

Cuando intercambiamos información a través de internet, se abren canales de comunicación que deben ser manejados correctamente porque de lo contrario se pueden dejar puertos abiertos los cuales pueden ser utilizados por los hackers para recopilar información del sistema. Una vez detectadas las vulnerabilidades del sistema y con la información obtenida, los hackers aprovechan para lanzar sus ataques informáticos.

En seguridad informática las Normas y Estándares buscan asegurar que se proteja la información. La protección de dicha información se logra gracias a la implementación de lineamientos de seguridad desde el ámbito internacional. Por ejemplo, estándares como ISO 27000, COBIT e ITIL establecen directrices de mejores prácticas para que las empresas las implementen y gestionen en buena forma el control de los sistemas de información.

El estándar ISO 27000 es un referente mundial para la seguridad en las organizaciones. Hace parte de una familia de estándares sobre Sistemas de la Gestión de Seguridad de la Información (SGSI). Como Estándar establece en su portafolio certificaciones, directrices, tratamiento de la gestión del riesgo, acreditación de las organizaciones, auditoria, técnicas de seguridad y gestión de incidentes.

De igual forma COBIT es una guía de mejores prácticas orientada al control de la información, Tecnologías de la Información y los riesgos que conllevan. El propósito de COBIT es ayudar a las organizaciones a satisfacer con éxito los desafíos de los negocios.

En cambio ITIL es un marco de referencia para gestionar los niveles de servicios de Tecnologías de la información.

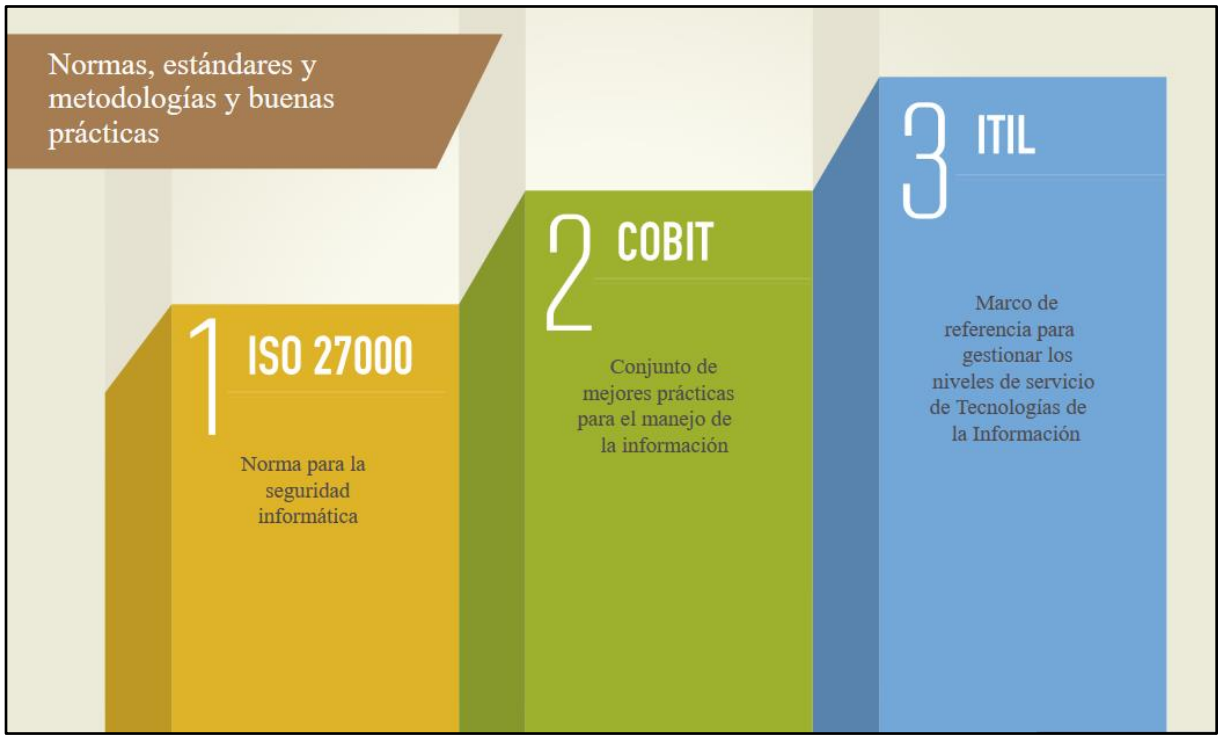

Imagen 1. Normas, Estándares y metodologías y buenas prácticas. Tomada de http://virtual.umng.edu.co/distancia/ecosistema/ovas/asso/seguridad_informatica/unidad_2/medios/graficos/p3.svg

Estándares ISO 27000, COBIT e ITIL

ISO 27000

Es una norma mundialmente aceptada para la seguridad informática. Corresponde a una serie de normas y estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La Norma ISO 27000 tiene como objetivo definir requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), con el fin de garantizar la selección de controles de seguridad adecuados, protegiendo así la información. Es recomendable para cualquier empresa grande o pequeña.

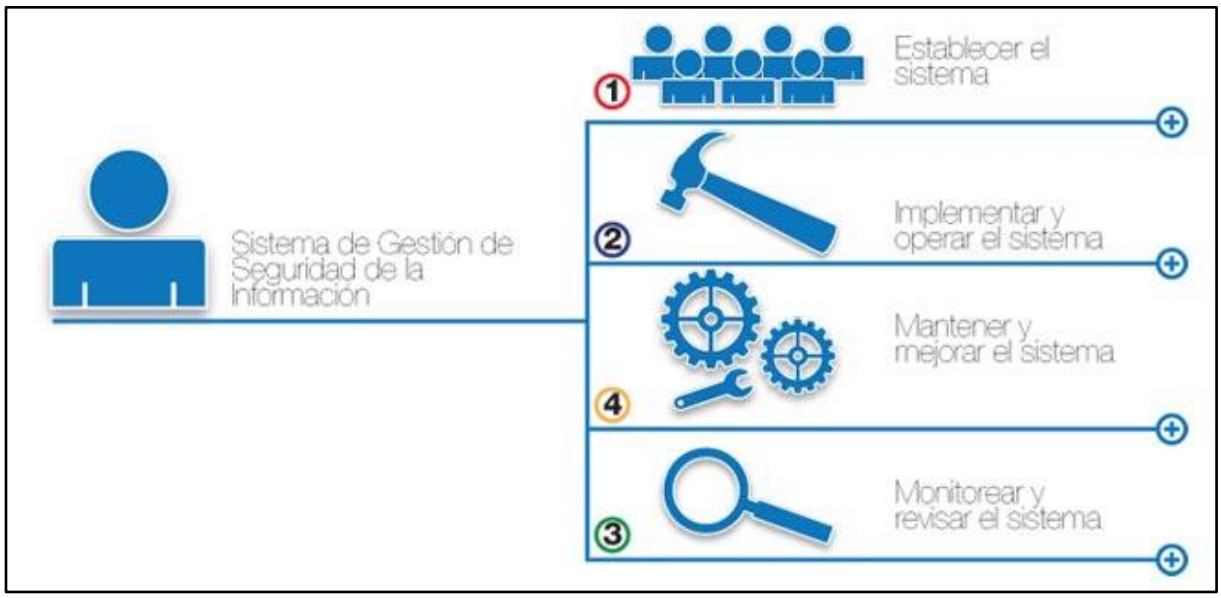

Imagen 2. Sistema de Gestión de Seguridad de la Información. Recuperado de http://www.magazcitum.com.mx/wp-content/gallery/magazcitum-2-4/hectoracevedo_iso_fig_1.jpg

COBIT

Es un Estándar de referencia el cual contiene una Guía de mejores prácticas para la dirección de Tecnologías de la Información (TI). Desarrollado por la asociación ISACA, orientado a las empresas, el cual funciona como herramienta de soporte que permiten a la gerencia conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio generando confianza en los sistemas de información y permitiendo entender cómo dirigirlos y gestionarlos estableciendo códigos de buenas prácticas que debe ser utilizado por los proveedores de los sistemas.

COBIT contribuye a reducir las diferencias existentes entre los objetivos del negocio y los beneficios, riesgos, necesidades de control y aspectos técnicos propios de un proyecto TIC, proporcionando un marco referencial para su dirección efectiva.

Imagen 3. Gobierno de TI. Tomada de https://cristian1701212362.files.wordpress.com/2017/06/que-es-cobit.jpg?w=736

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

ITIL

Es la Biblioteca de Infraestructura de Tecnologías de Información ITIL (InformationTechnologyInfraestructureLibrary), es un marco de referencia para gestionar los diferentes niveles de servicios de Tecnología de la Información.

ITIL proporciona un conjunto de mejores prácticas, extraídas de organismos referentes del sector público y privado a nivel internacional.

A través de buenas prácticas especificadas en ITIL se hace posible para departamentos y organizaciones reducir costos, mejorar la calidad del servicio, tanto a clientes externos como internos y optimizar al máximo las habilidades y destrezas del personal mejorando su productividad.

Imagen 4. Administración de servicios de TI: integrando gente, procesos y tecnología. Tomado de http://www.magazcitum.com.mx/?p=50#.W8-VtfZRfIU

Referencias Bibliográficas

Revista Pensamiento Americano. (Junio, 2011). *La gestión en la seguridad de la información según Cobit, Itil e Iso 27000.* Recuperado de: https://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/57/53

Universidad Militar Nueva Granada. (2017). *Sistema de Gestión de la Seguridad de la Información (SGSI).* Recuperado de: http://virtual.umng.edu.co/distancia/ecosistema/odin/odin_desktop.php?path=Li4vb3Zhcy9hc3NvL3NlZ3VyaWRhZF9pbmZvcm1hdGljYS91bmlkYWRfMi8=

Acevedo, H. (2010). *ITIL: ¿qué es y para qué sirve?* Recuperado de http://www.magazcitum.com.mx/?p=50#.W8-ZtfZRfIU

Rodríguez, C. (2017). *¿Qué es COBIT?* Recuperado de https://cristian1701212362.wordpress.com/2017/06/03/que-es-cobit/

Aponte, L. & Gómez, J. (2013). *Norma ISO 27000*. Recuperado de https://es.slideshare.net/haroll1/norma-iso-27000