Seminario Profesional:

"Modelo de gestión de identidades para seguridad de la información"

- Profesor: Moisés Toapanta

Guayaquil, 20 de marzo del 2017

Introducción

La seguridad de la información es el principal activo de una empresa o institución del siglo XXI

Una de las razones es que con la información y bajo un plan de contingencia una empresa puede volver a ser productiva así exista un desastre natural a nivel mundial.

La seguridad de la información es importante en todos los niveles operativos, tácticos y estratégicos.

Análisis de un modelo, metodología estándar y normas

Modelo

Un modelo es una representación de un objeto, sistema o idea, de forma diferente al de la entidad misma. El propósito de los *modelos* es ayudarnos a explicar.

Puede considerarse al modelo, en términos generales, como representación de la realidad.

Concepto globalizador de un modelo en las TICs

Metodología

Conocer y aplicar herramientas, recursos y aplicaciones definidas para ejecutar un procedimiento.

Una de las principales es metodologías de Cobit 5.0 donde se encuentra definidos varios estándares y normas.

Estándares:

Normas:

Estándar

Un estándar es un conjunto de reglas a seguir que se define como una norma nacional o internacional

Ejemplos

Modelos:

Modelo de indicadores para el alineamiento de las estrategias corporativas con las estrategias de TIC

Estándar:

ISO 17799 - Personal Definición de Roles y Perfiles Incluir la Seguridad en la responsabilidad de roles Política de perfiles en funciones y cargos. Los *estándares de seguridad* son una herramienta que apoya la gestión de la *seguridad informática.*

NORMAS: Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red organizacional.

Estándares de las Políticas de Seguridad Informática

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. A continuación se incorpora una relación con la serie de normas ISO 27000 y una descripción de las más significativas:

Familia de normas 27000	
Norma ISO/IEC	**Título**
ISO 27000	Gestión de la Seguridad de la Información: Fundamentos y vocabulario.
ISO 27001	Especificaciones para un SGSI.
ISO 27002	Código de Buenas Prácticas.
ISO 27003	Guía de Implantación de un SGSI.
ISO 27004	Sistema de Métricas e Indicadores.
ISO 27005	Guía de Análisis y Gestión de Riesgos.
ISO 27006	Especificaciones para Organismos Certificadores de SGSI.
ISO 27007	Guía para auditar un SGSI.
ISO 2701X	Guías sectoriales.
ISO 27XXX	Futuras normas.

Analizar cómo aplicar la Identificación (AAA)

Preguntas frecuentes:

¿De qué modo la Administración de identidades y accesos basada en contenido puede darme el control que necesito para impulsar mi negocio con confianza?

AAA consiste en tres áreas separadas que trabajan en forma conjunta

Componente clave para comprender la seguridad en el acceso en la base de datos y en las redes.

Autenticación, autorización, auditoria: Conjunto de procesos usados para proteger datos, equipos y confidencializar la información.

Objetivos:

Confidencialidad: el contenido de los datos no debe ser revelado.

Integridad: el contenido de los datos debe permanecer intacto y no debe sufrir alteraciones.

Disponibilidad: el contenido de los datos debe estar accesible cuando se necesite.

Autenticación

Proceso utilizado para verificar que una máquina o usuario que intenta acceder a un recurso es quien dice ser. Generalmente utiliza nombres de usuario, passwords, identificadores únicos, entidades certificantes, o algunos otros elementos para permitir verificar la identidad contra un dispositivo o software que analice y valide esas credenciales

Autorización

Puede ser definido como una política, componente de software o hardware que es usado para permitir o denegar el acceso a un recurso. Esto puede ser un componente avanzado como una tarjeta inteligente, un dispositivo biométrico o un dispositivo de acceso a la red como un router, access point wireless o access server. También puede ser: un servidor de archivos o recursos que asigne determinados permisos como los sistemas operativos de red (Windows, Linux, unix, entre otros)

Auditoria

Es el proceso de registrar eventos, errores, acceso e intentos de autenticaciones en un sistema