Capítulo 2.
Sistema de Gestión de Seguridad de la Información (SGSI)
Dominios de la Norma ISO 27000
Dominios Técnicos

Dra. Jenny Torres
jenny.torres@epn.edu.ec

Departamento de Informática y Ciencias de la Computación
Facultad de Sistemas
Escuela Politécnica Nacional

ESCUELA
POLITÉCNICA
NACIONAL

Contenido

ESCUELA POLITÉCNICA NACIONAL

Dominios Técnicos de la Norma

- Política de seguridad
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad de los recursos humanos

- Seguridad física y del entorno

- Gestión de comunicaciones y operaciones

- Control de accesos

- Adquisición, desarrollo y mantenimiento de sistemas

- Gestión de los incidentes de la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

ESCUELA POLITÉCNICA NACIONAL

Seguridad física y del entorno

Objetivo

- Prevenir el acceso no autorizado, daño e interferencia a los establecimientos comerciales y a su información.
- Las instalaciones de procesamiento de información que apoyan las actividades del negocio críticas o sensibles deben ser alojadas en areas seguras.

ESCUELA POLITÉCNICA NACIONAL

Controles físicos de entrada

- Son áreas seguras que están protegidos con controles adecuados.
- Permiten que las áreas protegidas deben ser resguardadas por adecuados controles que permitan garantizar que solo se admita el paso de personal autorizado a los sistemas de información.

ESCUELA POLITÉCNICA NACIONAL

Seguridad de oficinas, despachos e instalaciones

- Se debe asignar y aplicar la seguridad física para oficinas, despachos y recursos.
- Detallar donde se encuentran lugares con restricción acceso.

ESCUELA POLITÉCNICA NACIONAL

Trabajo en areas seguras

- Se debe diseñar y aplicar proteccion fisica y pautas para trabajar en las areas seguras.
- Se debe asignar y aplicar medidas de protección física contra incendios, inundaciones, terremotos y otras formas de desastre natural.

ESCUELA POLITÉCNICA NACIONAL

Seguridad de los equipos

- Evitar pérdida, daño, robo o puesta en peligro de los activos, y la interrupcion de las actividades de la organización.
- Los equipos deben estar protegidos contra amenazas físicas y ambientales.
- El equipo debe situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno así como las oportunidades de acceso no autorizado.
- Proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.
- Proteger el cableado de energía y telecomunicaciones contra posibles interceptaciones o daños.
- Se debe mantener adecuadamente los equipos para garantizar su disponibilidad.
- Se debe aplicar seguridad a equipos fuera de las instalaciones de la organización considerando los diversos riesgos.
- Se debe revisar cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato o software con licencia se haya eliminado.
- No debe sacarse equipos, información o software fuera del local sin una autorización.

ESCUELA POLITÉCNICA NACIONAL

Actividad de Aprendizaje

- Liste ejemplos de 1 datacenter (nacional o extranjero) que cumple la norma TIER4.
- Indique los controles internos de seguridad fisica y del entorno en el datacenter de ejemplo.
- Indicar los controles para el perímetro de seguridad del datacenter.
- Para el caso de su empresa si usted instalaria un datacenter, que elementos de seguridad fisica colocaria y porque.

ESCUELA POLITÉCNICA NACIONAL

Objetivo

- Promover la comunicación entre los miembros de la organización.
- Facilitar la integración entre las tareas personales y las institucionales.
- Reducir el conflicto interno.
- Contribuir a la creación de espacios de información, participación y opinión.

- Se deber documentar los procedimientos de operación y hacerlo disponible para todos los usuarios que necesitan de ellos.
- Los procedimientos de operación deberían especificar las instrucciones necesarias para la ejecución detallada de cada tarea, incluyendo:
  a) el proceso y utilización correcta de la información;
  b) respaldo;
  c) los requisitos de planificación, incluyendo las interdependencias con otros sistemas, con los tiempos de comienzo y final posibles de cada tarea.

ESCUELA POLITÉCNICA NACIONAL

Objetivo

- Evitar la modificación por usuarios no autorizados.
- Evitar la modificación no autorizada o no intencional por parte de usuarios autorizados.
- Preservación de la consistencia interna y externa.

- Controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad y negocio.
- Se debe contemplar:
  a) requisitos de seguridad de cada aplicación de negocio individualmente;
  b) identificación de toda la información relativa a las aplicaciones;
  c) políticas para la distribución de la información y las autorizaciones;
  d) coherencia entre las políticas de control de accesos y las políticas de clasificación de la información en los distintos sistemas y redes.

ESCUELA POLITÉCNICA NACIONAL

Actividad de Aprendizaje

- Indique el procedimiento con su respectiva documentación de su empresa al aplicar el Control de Acceso a la Información.
- Describa cómo gestiona su empresa el acceso a usuarios para aplicaciones internas
- Indique cómo aplicaria los controles de acceso al desarrollo de sus sistemas.

ESCUELA POLITÉCNICA NACIONAL

Objetivo

- Todos los **requisitos de seguridad**, incluyendo las disposiciones para contingencias, la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuario; deben ser identificados y justificados en la fase de requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información.

- *Análisis y especificación de los requisitos de seguridad:* Los requisitos y controles de seguridad deberían reflejar el valor de los activos de información implicados y el posible daño a la organización que resultaría de fallos o ausencia de seguridad.
- La estimación del riesgo y su gestión son el marco de análisis de los requisitos de seguridad y de la identificación de los controles y medidas para conseguirla.
- *Controles criptográficos - Autenticación de mensajes:* La autenticación de mensajes es una técnica utilizada para detectar cambios no autorizados.
- Procesamiento correcto de las aplicaciones.
- Seguridad de los archivos del sistema.
- Seguridad en los procesos de desarrollo y soporte.

ESCUELA POLITÉCNICA NACIONAL

Referencias

Material didáctico elaborado con la colaboración del Dr. Walter Fuertes y el PhD. Denys Flores.

Sistema de Gestión de la Seguridad de la Inofmración
www.iso27000.es
http://www.iso27000.es/download/doc_sgsi_all.pdf

Código de buenas prácticas de seguridad. UNE-ISO/IEC 17700
Antonio Villalón Huerta
http://www.shutdown.es/ISO17799.pdf

ISO 27000
Norma ISO 27000
http://www.iso27000.es

ESCUELA POLITÉCNICA NACIONAL