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

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

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

Contenido

ESCUELA POLITÉCNICA NACIONAL

Norma ISO/IEC 27000

- Es un conjunto de estándares de la ISO (International Organization for Standardization) e IEC (International ElectrotechnicalCommission).
- Es un sistema de gestión de seguridad de la información (SGSI).
- Establece un proceso metodológico, documental y orientado a objetivos de seguridad y gestión de riesgos.
- Es adaptable a cualquier proceso informático dentro de cualquier tipo de organización, pública o privada, grande o pequeña.

Objetivos

- Proteger la información de toda organización.
- Proteger los sistemas de información.

ESCUELA POLITÉCNICA NACIONAL

Familia de Normas ISO/IEC 27000

- **ISO 27000:** Contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede hacer uso para entender con claridad tanto la serie como la relación entre los distintos documentos que la constituyen.

- **UNE-ISO/IEC 27001:2007:** es la norma principal de Requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIsdeberán ser certificados por auditores externos a las organizaciones.

- **ISO 27002:** es una guía de buenas prácticas. Realiza una descripción de los objetivos de control y controles recomendables en cuanto a seguridad de la información. Está constituida por 11 dominios, 39 objetivos de control y 133 controles (2005).

ESCUELA POLITÉCNICA NACIONAL

Familia de Normas ISO/IEC 27000

- **ISO 27003:** posee una guía de implementación de SGSI e información que hace referencia tanto al uso del modelo PDCA como de los requisitos de sus diferentes fases.

- **ISO 27004:** detalla en forma específica las métricas y las técnicas de medida que se aplican para determinar la efectividad de la implantación de un SGSI y de los controles relacionados.

- **ISO 27005:** es una guía para la Gestión del Riesgo de la Seguridad de la Información y sirve de apoyo a la ISO 27001 y a la implantación de un SGSI.

- **ISO 27006:** presenta los requerimientos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

ESCUELA POLITÉCNICA NACIONAL

Familia de Normas ISO/IEC 27000

- **ISO 27007:** es una guía de auditoría de un SGSI.
- **ISO 27011:** es una guía específica de Gestión de Seguridad de la Información para Telecomunicaciones.
- **ISO 27031:** es una guía de Continuidad de Negocio referente a las Tecnologías de la Información.
- **ISO 27032:** posee una guía relacionada con la Ciber-seguridad.
- **ISO 27033:** es una guía constituida para la gestión de seguridad de redes.
- **ISO 27034:** es una guía de Seguridad en Aplicaciones.
- **ISO 27799:** hace referencia a un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799.

ESCUELA POLITÉCNICA NACIONAL

Estructura de la Norma

- Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información.
- Para cada uno de los controles se indica asimismo una guía para su implantación.
- Está constituida por 11 dominios, 39 objetivos de control y 133 controles.
- Cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

ESCUELA POLITÉCNICA NACIONAL

Niveles de Seguridad

- **Seguridad Lógica:** confidencialidad, integridad y disponibilidad del software y datos de un SGSI.
- **Seguridad Organizativa:** relativa a la prevención, detección y corrección de riesgos.
- **Seguridad Física:** protección de elementos físicos de las instalaciones: servidores, PCs, etc.
- **Seguridad Legal**: cumplimiento de la legislación vigente

ESCUELA POLITÉCNICA NACIONAL

Estructura de la Norma

ISO/IEC 17799 (2000) establece **diez dominios de control**, la **27002 (2005)** establece **once**, que cubren por completo la Gestión de la Seguridad de la Información mientras que la norma **27002 (2013)** cubre **catorce**:

1. Política de la seguridad
2. Organización de la seguridad de la información
3. Gestión de activos
4. Seguridad de los recursos humanos
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones
7. Control de accesos
8. Adquisición, desarrollo y mantenimiento de sistemas
9. Gestión de los incidentes de la seguridad de la información
10. Gestión de la continuidad del negocio
11. Cumplimiento

ESCUELA POLITÉCNICA

NTE-ISO-IEC_27002-2009

Actividad de Aprendizaje

- Realice una comparación entre las Normas ISO 27001 (2005) y 27001 (2013).

ESCUELA POLITÉCNICA NACIONAL

Dominios Administrativos 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

Objetivo

- Proporcionar orientación y apoyo de la dirección para la seguridad de la información de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.
- Dirigir y dar soporte a la gestión de la seguridad de la información.

- La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.
- La política se constituye en la base de todo el sistema de seguridad de la información.
- La alta dirección debe apoyar visiblemente la seguridad de la información en la compañía.

ESCUELA POLITÉCNICA NACIONAL

Organización de la seguridad de la información

Objetivo

- Gestionar la seguridad de la información dentro de la organización.
- Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros.
- Mantener la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

- Debe diseñarse una estructura organizativa dentro de la compañía que defina las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma.
- Se debe asignar a los recursos de la organización, propietarios quienes serán los responsables de mantener una protección adecuada.

ESCUELA POLITÉCNICA NACIONAL

Propiedad de los recursos:

Todos los recursos de tratamiento de la información y los activos de información de la organización deben ser de propiedad de una parte designada. El dueño del recurso debe ser responsable de:

- asegurar que recursos de tratamiento de la información y los activos de información sean apropiadamente clasificados;
- definir y revisar periódicamente las restricciones de acceso y clasificación, tomando en cuenta políticas de control de acceso aplicables.

ESCUELA POLITÉCNICA NACIONAL

Gestión de activos

Objetivo

- Mantener una protección adecuada sobre los activos de la organización.
- Asegurar un nivel de protección adecuado a los activos de información.

- Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad en la organización.

ESCUELA POLITÉCNICA NACIONAL

Gestión de activos

Asegurar que cada persona dentro de la organización comprenda sus responsabilidades, ya que es un factor que influye en la preservación de la seguridad de la información. Los usuarios deben:

- actuar de acuerdo con las políticas de seguridad de información;
- proteger los activos de accesos no autorizados, divulgación, modificación, destrucción e interferencia;
- reportar eventos de seguridad o eventos potenciales u otros riesgos para la organización.

ESCUELA POLITÉCNICA NACIONAL

Seguridad de los recursos humanos

Objetivo

- Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios.
- Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.
- Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

- Las implicaciones del factor humano en la seguridad de la información son muy elevadas.
- Todo el personal, tanto interno como externo a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.
- Diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc.
- Procesos de notificación de incidencias claros, ágiles y conocidos por todos.

Gestión de los incidentes de la seguridad de la información

Objetivo

- Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.
- Es conveniente establecer el reporte formal del evento y los procedimientos de escalada.

- Comunicación de eventos y debilidades en la seguridad de la información.
  - Comunicación de eventos en seguridad
  - Comunicación de debilidades en seguridad
- Gestión de incidentes y mejoras en la seguridad de la información.
  - Identificación de responsabilidades y procedimientos
  - Evaluación de incidentes en seguridad
  - Recogida de pruebas

ESCUELA POLITÉCNICA NACIONAL

1. **Identificación y registro de la incidencia**
   - *Descripción de la incidencia:* Asignar un número único y recoger datos de ubicación y/o localización. Establecer una tipología y codificación de incidencias para facilitar su análisis cualitativo y cuantitativo posterior. Hacer una valoración para priorizar la gestión (leve, grave, muy grave). Detallar la incidencia incluyendo la fecha.
   - *Registro*

2. **Análisis de la incidencia**
   - *Análisis del origen, causa y consecuencias*
   - *Identificación y valoración de riesgos derivados*

ESCUELA POLITÉCNICA NACIONAL

3 **Intervención sobre la incidencia**

- *Plan de acción:* identificada y valorada la incidencia, el plan de acción determinará qué se va a hacer. Variará en función del nivel de criticidad, urgencia y otros parámetros que marcarán la prioridad.
- *Acciones preventivas:* para mitigar los efectos no deseados de la incidencia y acotar sus consecuencias.
- *Determinación de un responsable para seguimiento y subsanación:* siempre deberá haber un recurso técnico responsable de la misma, con la capacidad de actuación y los medios adecuados para su resolución o, en caso contrario, un protocolo alternativo si no se puede contener el efecto indeseado.
- *Plazo de actuación:* como cualquier otra tarea planificada deberá tener un calendario de actuación tentativo aprobado.
- *Plan de información a afectados:* las incidencias podrían afectar a diversos grupos de trabajo y será imprescindible mantener informados a todos del proceso de resolución.

ESCUELA POLITÉCNICA NACIONAL

4 **Seguimiento y control de la incidencia**

- *Establecer un procedimiento de vigilancia y seguimiento*

5 **Propuestas de mejora**

- *Sintetizar el problema*
- *Analizar el impacto y proponer mejoras*
- *Explicar los beneficios*

ESCUELA POLITÉCNICA NACIONAL

Actividades de Aprendizaje

1. Describa 2 ejemplos de amenazas y 2 ejemplos de incidentes de seguridad dentro de la empresa.
2. Indicar 2 ejemplos de herramientas de software para la gestión de incidentes en la seguridad (explicación corta).
3. Elabore una matriz de responsabilidad para la gestión de incidentes en la seguridad de la información. Por ejemplo que indique: área, rol, nombre del responsable y responsabilidades.
4. Buscar un ejemplo del proceso de gestión de incidentes de seguridad informática en una empresa, indicar que pasos realizan y explicar cada uno de ellos.

ESCUELA POLITÉCNICA NACIONAL

Objetivo

- Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres.

- Todas las situaciones que puedan provocar la interrupción de las actividades del negocio deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados.
- Los planes de contingencia deben ser probados y revisados periódicamente.
- Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

ESCUELA POLITÉCNICA NACIONAL

1. **Identificar y ordenar las amenazas**
   - *Crear una lista de los incidentes de interrupción de la actividad que constituyan las amenazas más probables para la empresa.*
   - *crear una lista de escenarios ordenados por probabilidad de ocurrencia y por potencial de causar un impacto negativo.*

2. **Realizar un análisis del impacto en la empresa**
   - *Determinar qué partes de la empresa son las más críticas.*
   - *Determinar el impacto.*

3. **Crear un plan de respuesta y recuperación**
   - *Catalogar datos clave sobre los bienes involucrados en la realización de las funciones críticas.*
   - *Documentar todos los acuerdos vigentes para mudar las operaciones a ubicaciones e instalaciones de TI temporales.*

4. **Probar el plan y refinar el análisis**
   - *Probar el plan al menos una vez al año.*

ESCUELA POLITÉCNICA NACIONAL

Actividades de Aprendizaje

1. Plantear un ejemplo de plan de continuidad de negocio en una empresa basada en TI.
2. Buscar una plantilla (secciones a,b,c?) para un plan de continuidad del negocio y explicar las secciones más importantes que usted aplicaría a su empresa de caso de estudio y por qué.

ESCUELA POLITÉCNICA NACIONAL

Cumplimiento

Objetivo

- Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad.
- Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma.
- Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas.

- Se debe identificar convenientemente la legislación aplicable a los sistemas de información corporativos, integrándola en el sistema de seguridad de la información de la compañía y garantizando su cumplimiento.
- Se debe definir un plan de auditoría interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.

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