Capítulo 2.
Sistema de Gestión de Seguridad de la Información (SGSI)
Alcance, Límites y Requerimientos del SGSI

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

Aplicación del SGSI

1. **Definir alcance del SGSI:** en función de características del negocio, organización, localización, activos.
2. **Definir política de seguridad:** que incluya el marco general y los objetivos de seguridad de la información de la organización.
3. **Definir el enfoque de evaluación de riesgos:** definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización.
4. **Inventario de activos:** todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
5. **Identificar amenazas y vulnerabilidades:** todas las que afectan a los activos del inventario.

ESCUELA POLITÉCNICA NACIONAL

Aplicación del SGSI

1. **Identificar los impactos:** los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad.

2. **Análisis y evaluación de los riesgos:** evaluar el daño resultante de un fallo de seguridad (que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable o requiere tratamiento.

3. **Identificar y evaluar opciones para el tratamiento del riesgo:** el riesgo puede ser reducido mediante controles, eliminado, aceptado o transferido.

4. **Selección de controles:** seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior.

5. **Aprobación por parte de la Dirección del riesgo residual**

ESCUELA POLITÉCNICA NACIONAL

Beneficios del SGSI

- **Reducción de riesgos** debido al establecimiento y seguimiento de controles sobre ellos. Con ello lograremos **reducir las amenazas** hasta alcanzar un nivel asumible por nuestra organización. De este modo, si se produce una incidencia, los daños se **minimizan** y la continuidad del negocio está asegurada.

- **Ahorro de costes** derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos.

- La seguridad se considera un sistema y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un **ciclo de vida metódico y controlado**, en el que participa toda la organización.

ESCUELA POLITÉCNICA NACIONAL

Beneficios del SGSI

- La organización se **asegura del cumplimiento de la legislación vigente** y se evitan riesgos y costes innecesarios. La entidad se asegura del cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.

- La certificación del Sistema de Gestión de Seguridad de la Información contribuye a **mejorar la competitividad en el mercado,** diferenciando a las empresas que lo han conseguido y haciéndolas más fiables e incrementando su prestigio.

ESCUELA POLITÉCNICA NACIONAL

Alcance del SGSI

Determinar las partes o procesos de la organización que van a ser incluidos dentro del mismo: determinar cuáles son los procesos críticos para su organización decidiendo qué es lo que quiere proteger y por dónde debe empezar.

El documento debe incluir:

- Actividades de la organización.
- Ubicaciones físicas que van a verse involucradas.
- Tecnología de la organización y las áreas que quedarán excluidas en la implantación del sistema.

Es importante que durante esta fase, se estimen los recursos económicos y de personal que se van a dedicar a implantar y mantener el sistema. De nada sirve que la organización realice un esfuerzo importante durante la implantación si después no es capaz de mantenerlo.

ESCUELA POLITÉCNICA NACIONAL

Actividad de Aprendizaje

- Escriba el Alcance del SGSI aplicado a su caso de estudio.
- Referencia: NTE-ISO-IEC_27003-2012. 5.3 Alcance preliminar del SGSI.

ESCUELA POLITÉCNICA NACIONAL

Política de Seguridad del SGSI

Su principal objetivo es:

- Recoger las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la organización y a la legislación vigente.
- Establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades.

El documento debe:

- delimitar qué se tiene que proteger, de quién y por qué.
- explicar qué es lo que está permitido y qué no.
- determinar los límites del comportamiento aceptable y cuál es la respuesta si estos se sobrepasan.
- identificar los riesgos a los que está sometida la organización

ESCUELA POLITÉCNICA NACIONAL

Requisitos:

- Debe de ser **redactada de una manera accesible** para todo el personal de la organización. Por lo tanto debe ser corta, precisa y de fácil comprensión.
- Debe ser **aprobada por la dirección** y publicitada por la misma.
- Debe ser de **dominio público** dentro de la organización, por lo que debe estar disponible para su consulta siempre que sea necesario.
- Debe ser la **referencia para la resolución de conflictos** y otras cuestiones relativas a la seguridad de la organización.

ESCUELA POLITÉCNICA NACIONAL

Requisitos:

- Debe **definir responsabilidades** teniendo en cuenta que éstas van asociadas a la autoridad dentro de la compañía. En función de las responsabilidades se decidirá quién está autorizado a acceder a qué tipo de información.
- Debe **indicar** que **lo que se protege en la organización** incluye tanto al personal como a la información, así como su reputación y continuidad.
- Debe ser **personalizada** totalmente para cada organización.
- Debe **señalar las normas y reglas** que va a adoptar la organización y las medidas de seguridad que serán necesarias.

ESCUELA POLITÉCNICA NACIONAL

Política de Seguridad del SGSI

El documento debe incluir:

- **Definición de la seguridad de la información** y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo de control que permite compartir la información.
- **Declaración por parte de la Dirección** apoyando los objetivos y principios de la seguridad de la información.
- Breve **explicación de las políticas**.
- **Definición de responsabilidades** generales y específicas, en las que se incluirán los roles pero nunca a personas concretas dentro de la organización.
- **Referencias** a documentación que pueda sustentar la política

ESCUELA POLITÉCNICA NACIONAL

Actividad de Aprendizaje

- Escriba una Política de Seguridad aplicado a su caso de estudio.
- Referencia: NTE-ISO-IEC_27002-2009. 5. Política de Seguridad.

ESCUELA POLITÉCNICA NACIONAL

Los activos de la Seguridad de la Información

Las organizaciones poseen información que deben proteger frente a riesgos y amenazas para asegurar el correcto funcionamiento de su negocio. Este tipo de información imprescindible para las empresas es lo que se ha denominado *activo de Seguridad de la Información.* Su protección es el objetivo de todo Sistema de Gestión de Seguridad de la Información.

Los activos pueden dividirse en diferentes grupos según su naturaleza:

- **Servicios**, es decir, los procesos de negocio que ofrece la organización al exterior o al interno, como es el caso de la gestión de nóminas.
- **Datos e información** que se manipula dentro de la organización. Suelen ser el núcleo del sistema, mientras que el resto de activos suelen darle soporte de almacenamiento, manipulación, etc.
- **Aplicaciones de software**

ESCUELA POLITÉCNICA NACIONAL

Los activos de la Seguridad de la Información

- **Equipos informáticos**
- **Personal**, este es el activo principal. Incluye personal interno, subcontratado, clientes, etc.
- **Redes de comunicaciones** que dan soporte a la organización para el movimiento de la información. Pueden ser redes propias o subcontratadas a terceros.
- **Soportes de información**, es decir, los soportes físicos que permiten el almacenamiento de la información durante un largo período de tiempo.
- **Equipamiento auxiliar** que da soporte a los sistemas de información. Por ejemplo, los equipos de destrucción de documentación o los equipos de climatización.
- **Instalaciones** donde se alojan los sistemas de información, como oficinas, edificios o vehículos.

ESCUELA POLITÉCNICA NACIONAL

Los activos de la Seguridad de la Información

Inventario:

- Cada activo del inventario debe incluir, al menos, su descripción, localización y propietario.
- El propietario del activo debe ser quien defina el grado de seguridad que requiere su activo.
- El propietario no tiene, necesariamente, que ser quien va a gestionar el activo o ser su usuario.
  - Por ejemplo: una base de datos de clientes puede pertenecer al Director Comercial de una empresa, su gestión puede estar encargada al área de sistemas y sus usuarios pueden ser los comerciales.

ESCUELA POLITÉCNICA NACIONAL

Los activos de la Seguridad de la Información

- Es necesario realizar una **valoración de los activos** en función de la relevancia que tengan para el negocio y del impacto que una incidencia sobre el mismo pueda causar a la entidad.
  - *Valoración cuantitativa*, se estima el valor económico del activo.
  - *Valoración cualitativa*, se establece de acuerdo a una escala, por ejemplo del 0 al 10 o con valores del tipo: bajo, medio y alto.
  - *Por ejemplo,* si consideramos una base de datos de clientes como un activo de la organización, se debe responder a preguntas como ¿qué impacto tendría para el negocio que alguien tuviese acceso a la base de datos de clientes y modificase los datos de los mismos?

- Existen varias formas de valoración de los activos, sin embargo, la **entrevista** y la **encuesta** son los más utilizados.

- En ambos casos, se debe seleccionar un grupo significativo de personas. Estas personas deben representar a todas las áreas del alcance del SGSI, así como tener diferentes roles.

ESCUELA POLITÉCNICA NACIONAL

Actividad de Aprendizaje

- Determine los activos de seguridad de la información aplicado a su caso de estudio.

ESCUELA POLITÉCNICA NACIONAL

Referencias

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

Implantación de un SGSI en la empresa - Guía de Apoyo
Instituto Nacional de Tecnologías de la Comunicación - INTECO
https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SG

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

ESCUELA POLITÉCNICA NACIONAL