# Capítulo 2.
# Sistema de Gestión de Seguridad de la Información (SGSI)
## Modelo PDCA y su Relación con los Objetivos de la Empresa

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

# Objetivos y Metas del Negocio

Importancia:

- Establecer políticas de seguridades de la información.
- Definir objetivos y actividades de seguridad.
- Alinerar la estrategia de seguridad de la información con la cultura organizacional.
- Obtener apoyo y compromiso visible por parte de todos los niveles de la administración.
- Entender los requerimientos de protección de activos de información para aplicar la estrategia de gestión de riesgos de seguridad de la información.
- Concientizar a los empleados acerca la importancia de la seguirdad de la información.
- Definir programas de entrenamiento, educación e información para los empleados.

ESCUELA POLITÉCNICA NACIONAL

# Compromiso de la Dirección

Una de las bases fundamentales para iniciar un proyecto de este tipo es el **apoyo claro y decidido de la Dirección de la organización**. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso, hacen necesario el impulso constante de la Dirección.

ESCUELA POLITÉCNICA NACIONAL

- Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma **metódica, documentada** y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

- El propósito de un SGSI es, por tanto, **garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados** por la organización de una forma **documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios** que se produzcan en los riesgos, el entorno y las tecnologías.

ESCUELA POLITÉCNICA NACIONAL

# Sistema de Gestión de Seguridad de la Información

- La norma ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) es certificable y especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI.
- El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye la Norma ISO 27001.
- **Adopta la metodologia PDCA.**

ESCUELA POLITÉCNICA NACIONAL

# Objetivos - SGSI

Objetivos:

- Ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición menor al nivel de riesgo que la propia organización ha decidido asumir.
- Gestiona el volumen de información corporativa.
- Identifica los activos de información empresariales.
- Identifica riesgos que puedan impedir el correcto funcionamiento de los activos de información.
- Gestiona los riesgos mediante objetivos de control.
- Alinea las metas del negocio con los objetivos de seguridad. Las metas del negocio usualmente están delineadas en su Plan Estratégico.

ESCUELA POLITÉCNICA NACIONAL

# ¿Qué incluye un SGSI?


Fuente: www.ISO27000.es

- **Documentos de Nivel 1:** *Manual de seguridad:* por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

- **Documentos de Nivel 2:** *Procedimientos:* documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

ESCUELA POLITÉCNICA NACIONAL

# ¿Qué incluye un SGSI?

- **Documentos de Nivel 3:** *Instrucciones, checklists y formularios:* documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

- **Documentos de Nivel 4:** *Registros:* documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

ESCUELA POLITÉCNICA NACIONAL

# ¿Cómo se implementa un SGSI?


- Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad:
  - **Plan (planificar)**: establecer el SGSI.
  - **Do (hacer)**: implementar y utilizar el SGSI.
  - **Check (verificar)**: monitorizar y revisar el SGSI.
  - **Act (actuar)**: mantener y mejorar el SGSI.

ESCUELA POLITÉCNICA NACIONAL

# Fase de Planificación

La Fase de Planificación incluye las siguientes actividades:

- determinación del alcance del SGSI.
- identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos.
- identificación de activos, vulnerabilidades y amenazas.
- evaluación de la magnitud de los riesgos.
- selección de controles para el tratamiento de riesgos.
- obtención de la aprobación de la gerencia para la implementación del SGSI.
- redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables.

ESCUELA POLITÉCNICA NACIONAL

# Fase de Implementación

La Fase de Implementación incluye las siguientes actividades:

- redacción de un plan de tratamiento del riesgo que describe quién, cómo, cuándo y con qué presupuesto se deberían implementar los controles correspondientes.
- implementación de un plan de tratamiento del riesgo.
- implementación de los controles de seguridad correspondientes.
- determinación de cómo medir la eficacia de los controles.
- realización de programas de concienciación y capacitación de empleados.
- gestión del funcionamiento normal del SGSI.
- gestión de los recursos del SGSI.
- implementación de procedimientos para detectar y gestionar incidentes de seguridad.

ESCUELA POLITÉCNICA NACIONAL

# Fase de Verificación

La Fase de Verificación incluye las siguientes actividades:

- implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.
- revisiones periódicas de la eficacia del SGSI.
- medición de la eficacia de los controles.
- revisión periódica de la evaluación de riesgos.
- auditorías internas planificadas.
- revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras.
- actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión.

ESCUELA POLITÉCNICA NACIONAL

# Fase de Mantenimiento y Mejora

La Fase de Mantenimiento y Mejora incluye las siguientes actividades:

- implementación en el SGSI de las mejoras identificadas.
- toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros.
- comunicación de actividades y mejoras a todos los grupos de interés.
- asegurar que las mejoras cumplan los objetivos previstos.

ESCUELA POLITÉCNICA NACIONAL

# Roles y Responsabilidades en el SGSI

- **El Responsable de Seguridad**, es la persona que se va a encargar de coordinar todas las actividades en materia de seguridad dentro de la empresa.

- **El Comité de Dirección**, estará formado por los directivos de la empresa, tendrá las máximas responsabilidades y aprobará las decisiones de alto nivel relativas al sistema.

- **El Comité de Gestión**, controlará y gestionará las acciones de la implantación del sistema colaborando muy estrechamente con el responsable de seguridad de la entidad. Este comité tendrá potestad para asumir decisiones de seguridad y estará formado por personal de los diferentes departamentos involucrados en la implantación del sistema.

ESCUELA POLITÉCNICA NACIONAL

**FASE 1:** Obtención de Aprobación de la Dirección para Implementar un SGSI

- **Entradas:**
  - Carta de Solicitud
- **Salidas:**
  - Carta de compromiso de la dirección
  - Copia del plan estratégico de la organización

ESCUELA POLITÉCNICA NACIONAL

**FASE 2:** Identificar Objetivos y Metas con Respecto al SGSI

- **Entradas:**
  - Plan estratégico.
  - Orgánico funcional.
  - Diagrama de infraestructura tecnológica.
  - Requerimientos legales, contractuales y regulatorios que rigen a la empresa.
  - Lista de activos de información (servicios/aplicaciones) que tiene la empresa.
- **Salidas:**
  - Documento resumen de objetivos y metas del negocio con respecto a la seguridad de la información.
  - Lista de requerimientos regulatorios que rigen a la empresa.
  - Caracterización de la empresa: misión, visión, orgánico Funcional, nivel de decisión de la Unidad Informática.

**Seguir los pasos de la actividad 5.2 de la norma NTE-ISO-IEC 27003.**

# Actividad de Aprendizaje

- Identificar 2 casos exitosos de la implementación de un SGSI en diversas organizaciones, con el fin de establecer cuáles fueron las experiencias en su planificación, ejecución, verificación y acciones correctivas.

ESCUELA POLITÉCNICA NACIONAL

# Referencias

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


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

¿Qué es la norma ISO 27001?
*27001 Academy*
http://www.iso27001standard.com/es/que-es-la-norma-iso-27001


ESCUELA POLITÉCNICA NACIONAL