pirani

Módulo 2

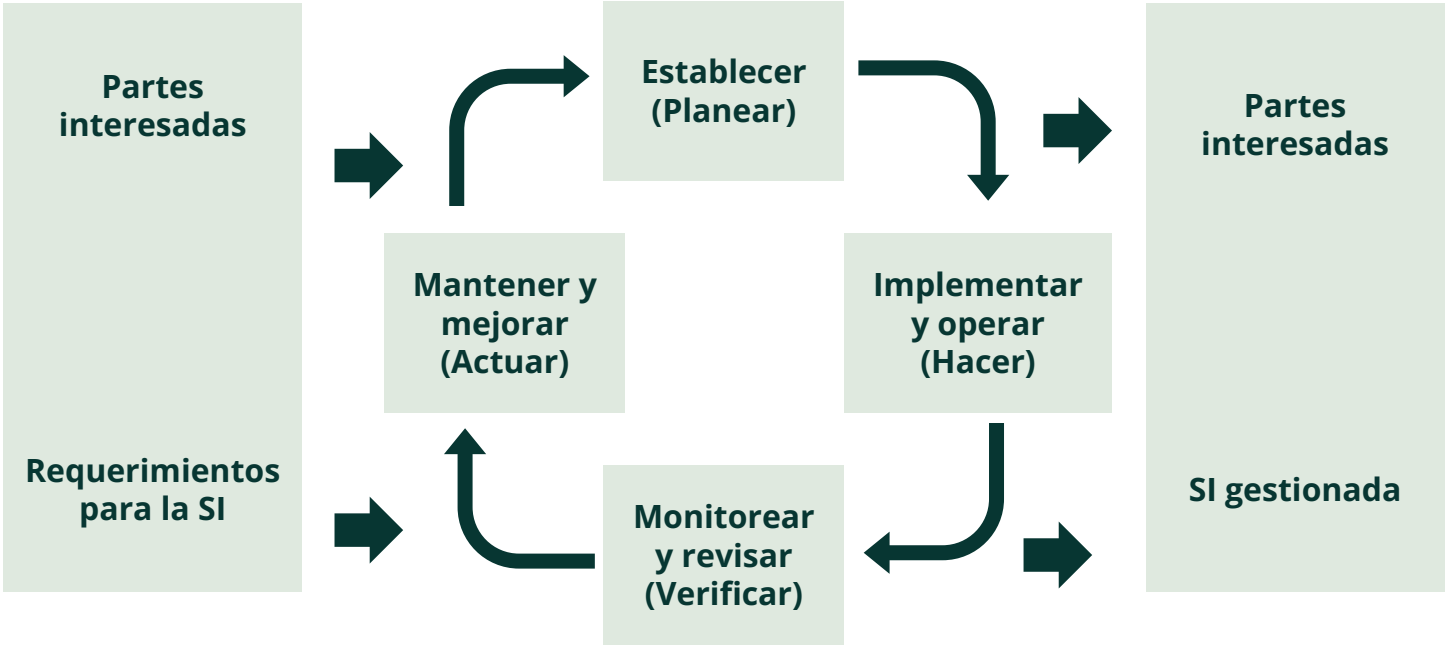
Estructura y gobierno de Seguridad de la Información

CONTENIDO

1. Modelo PHVA aplicado al SGSI
1. Liderazgo en el SGSI
1. Política de Seguridad de la Información
1. Roles y responsabilidades
1. Recursos para seguridad de la información
1. Estructura del SGSI
1. Revisión del SGSI por parte de la alta gerencia

1.
Modelo PHVA en el SGSI

Mejora continua del Sistema de Gestión de Seguridad de la Información



Mejora continua del Sistema de Gestión de Seguridad de la Información

Establecer (Planear)

Establecer la política de SI, los objetivos, las metas, controles, procesos y procedimientos relacionados con la mejora de la SI para obtener resultados que se alinean con las políticas y objetivos generales de la organización.

Implementar y operar (Hacer)

Implementar y operar la política de SI, controles, procesos y procedimientos.

Mejora continua del Sistema de Gestión de Seguridad de la Información

Monitorear y revisar (Verificar)

Monitorear y revisar el desempeño de la política de SI y objetivos, informar los resultados a la gerencia para su revisión, y determinar y autorizar las acciones de rehabilitación y mejora.

Mantener y mejorar (Actuar)

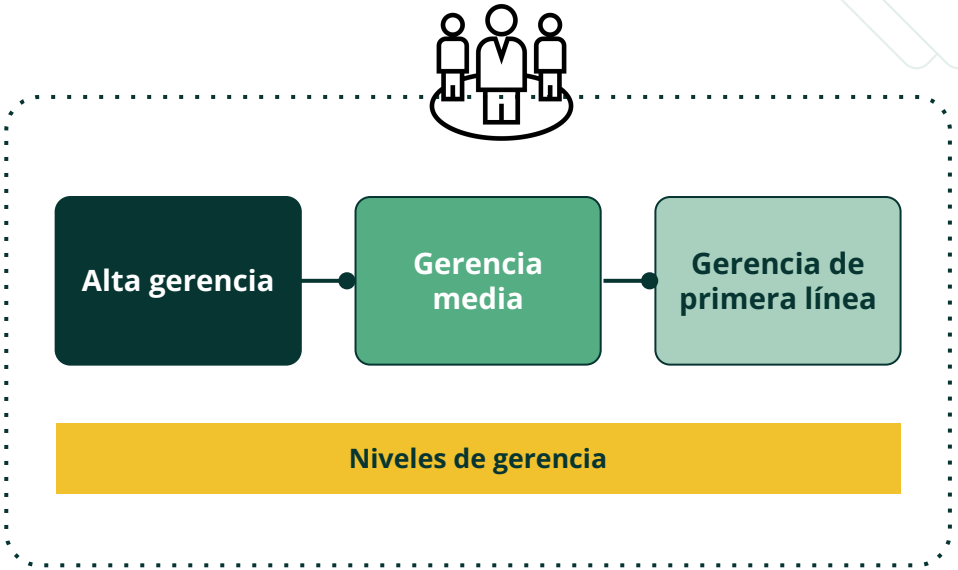
Mantener y mejorar el SGSI adoptando las medidas correctivas con base en los resultados de la revisión de la gerencia, el reajuste del alcance del SGSI, la política de SI y los objetivos.

2.
Liderazgo en el SGSI

Liderazgo / Gerencia

La alta gerencia como elemento principal para el gobierno de la gestión de la seguridad de la información, **define, implementa y comunica la Política del SGSI**.

De igual forma establece **los roles, responsabilidades y autoridades del sistema** mediante la estructura de gobierno de seguridad de la información, proporcionando así un esquema de relacionamiento claro entre los funcionarios involucrados en el manejo y gestión de un incidente que afecte el funcionamiento normal de los procesos críticos.



Liderazgo / Gobierno corporativo

La función principal de la estructura de gobierno consiste en **coordinar, ejecutar y controlar** todas las actividades que conduzcan a disminuir el impacto que pueda producir la ocurrencia de un incidente, además, **poner en marcha la seguridad de la información de manera efectiva.**

3.

Política de Seguridad de la Información

¿Qué es la Política de Seguridad de la Información?

La **Política de Seguridad de la Información** es un documento de alto nivel que denota el compromiso de la alta gerencia con la seguridad de la información.

Contiene la definición de la seguridad de la información desde el punto de vista de la organización.

- Debe ser enriquecida y compatible con otras políticas dependientes de esta, objetivos de seguridad, procedimientos, controles, protocolos.
- Debe estar fácilmente accesible, de forma que todos los empleados estén al tanto de su existencia y entiendan su contenido.
- Puede ser también un documento único o inserto en un manual de seguridad.
- Se debe designar un propietario que será el responsable de su mantenimiento, su actualización y de cualquier cambio que se requiera.
- De la política principal se desprenden muchas políticas adjuntas.

4.

Roles y responsabilidades en seguridad de la información

Roles y responsabilidades

Los roles y responsabilidades de seguridad de la información son vitales y fundamentales para el buen funcionamiento y mantenimiento de la estrategia y lineamientos de seguridad de la información.

Los roles son actividades, atributos, especificaciones, procedimientos y controles expresados en los diferentes cargos de las organizaciones.

Estos roles y responsabilidades están definidas según el rango, cargo, toma de decisiones, equipo, entre otros.

Encargada	Comité Técnico	Comité General
Encargado de control interno	Jefe departamento Informática Jefe unidad de Soporte y Redes Coordinador de Redes Encargado Seguridad de la Información	Director SSMSO Subdirector administrativo Subdirector de gestión asistencial Subdirector de gestión de desarrollo de personas Jefe departamento Informática Jefe departamento Finanzas Encargado Seguridad de la Información

Roles y responsabilidades

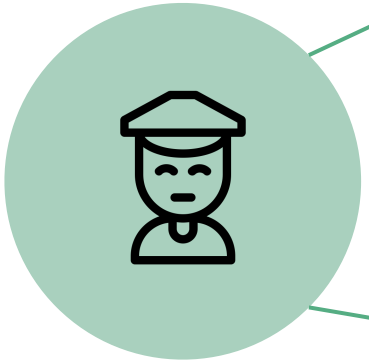
Los principales roles en seguridad de la información están enfocados en:

- Líder
- Oficial
- Analista
- Ejecutor

Rol del oficial o administrador de la seguridad de la información

Quien tenga el rol de responsable y administrador de la seguridad de información en la organización debe tener claridad y entendimiento de los siguientes aspectos en los cuales se debe enfocar y debe administrar:

Oficial SGSI



Reportar al alto nivel
Es independiente al área de Tecnología
Mantener comunicación interna y externa

Protocolos
Procedimientos
Políticas

Trabajar con base en la gestión de riesgos y activos de información

Procedimientos
Documentos
Archivo físico y magnético
Minería de datos
Incidentes de seguridad
Comunicaciones
Información interna y externa
Riesgos

5.

Recursos para seguridad de la información

Recursos

Para que la seguridad de la información funcione al interior de las organizaciones es muy importante **contar con los recursos necesarios para su buen funcionamiento.**

Estos recursos pueden ser **físicos, tecnológicos, tangibles, intangibles**, y los que la organización considere oportunos y necesarios para el mantenimiento de la seguridad de la información.

Herramientas

Tecnología
Puntos de control
Auditoría
Sistemas de información
Políticas
Procedimientos
Controles
Capacidad instalada

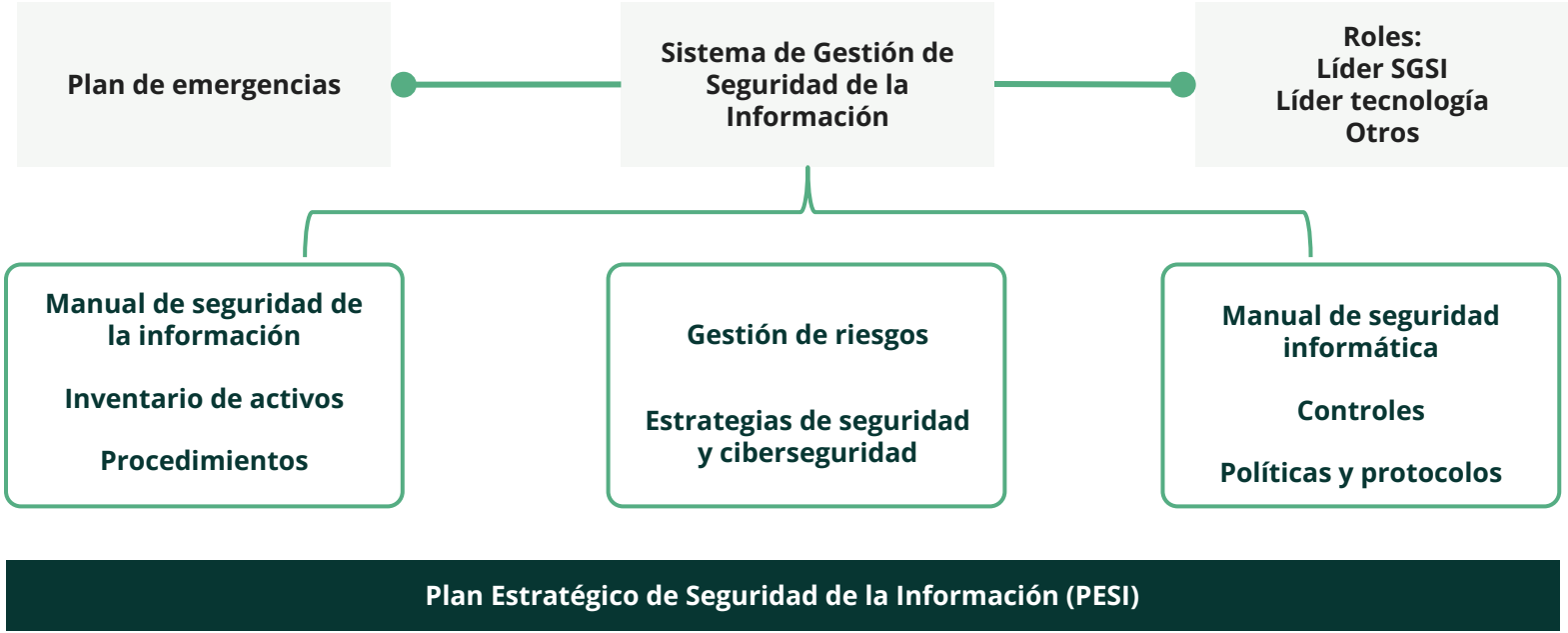
Personal

Capacitado
En toma de conciencia
Liderazgo
Roles
Responsabilidades
Carácter
Idóneo

6.
Estructura del SGSI

Estructura de seguridad de la información

La estructura organizacional y documental de un Sistema de Gestión de Seguridad de la Información debe estar definido acorde con el tamaño de la empresa, productos, servicios, sedes, capacidad económica, recursos disponibles, herramientas tecnológicas, entre otros.



Estructura documental

Se define la estructura adoptada dentro del SGSI para gestionar la documentación asociada al mismo de forma tal que se **garantice la calidad y la oportunidad de la información allí contenida**, además de garantizar su disponibilidad en los casos en que deba ser utilizada o consultada.

Como factor adicional se define la **relación jerárquica que guarda la documentación definida** dentro del sistema de gestión con el fin de facilitar la comprensión de su papel y funcionalidad dentro del mismo.

7.

Revisión del SGSI por parte de la alta gerencia

Revisión del SGSI por parte de la alta gerencia

La alta dirección debe revisar el SGSI a intervalos planificados, como mínimo cada año, y cuando se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia.

Como insumo para la revisión de la gerencia al SGSI, **se tienen en cuenta los siguientes aspectos:**

A. El estado de acciones de las revisiones previas de la gerencia.

B. Cambios relevantes externos e internos que puedan afectar el SGSI.

C. Información sobre el desempeño del SGSI, incluyendo tendencias en:

2. No conformidad y acciones correctivas.
3. Resultados de la evaluación de medición y monitoreo.
4. Resultados de auditorías.
5. Oportunidades para el mejoramiento continuo.

¡Gracias!

pirani | www.pirani.co/es