Centro de Especializaciones Noeder

*Diploma de Especialización Internacional*

# IMPLEMENTADOR Y AUDITOR SEGURIDAD DE LA INFORMACIÓN - ISO 27001 Y CONTINUIDAD DEL NEGOCIO - ISO 22301

## MÓDULO I

## INTERPRETACIÓN DE LA NORMA ISO 27001

**CLASE 02**

Mg. Ing. Julio Pereyra Rosales

# 1. Liderazgo y compromiso en el SGSI

# 1. Liderazgo

## 5.1 Liderazgo y compromiso

**La Alta Dirección debe:**

Establecer la política y objetivos del SGSI y que sean compatibles con la dirección estratégica.

Integración del SGSI en los procesos del negocio.

Apoyar a otros roles de la dirección para la eficacia del SGSI.

Asegurarse que los recursos necesarios del SGSI estén disponibles.

# 1. Liderazgo

## 5.1 Liderazgo y compromiso

**La Alta Dirección debe:**

- Comunicación de la importancia del SGSI.
- Asegurarse que el SGSI cumpla lo planificado.
- Comprometerse, dirigir y apoyar a las personas para contribuir a la eficacia de SGSI.
- Promover la mejora continua.

# 1. Liderazgo

## 5.2 Política


- Adecuada al propósito de la organización
- Marco de referencia para los objetivos del SGSI.
- Compromiso de cumplir requisitos aplicables al SGSI.
- Incluye compromiso de mejora continua del SGSI.

- Comunicarse dentro de la empresa.
- Disponible a las partes interesadas, según corresponda

Disponible

Información documentada

**La Alta Dirección debe establecer una Política de SGSI que:**

# 1. Liderazgo

## 5.3 Roles, responsabilidades y autoridad

La Alta Dirección debe asegurar la responsabilidad y autoridad para los roles importantes se asignen y se comuniquen al interior de la organización, a fin de:

Asegurarse que el SGSI cumple la norma ISO 27001.

Informar sobre el desempeño del SGSI a la Alta Dirección.

# 2. Planificación del SGSI

# 2. Planificación

## 6.1 Acciones para abordar riesgos y oportunidades

### 6.1.1 Consideraciones generales

La organización debe determinar :

- Cuestiones internas
- Cuestiones externas
- Partes interesadas
- Riesgos y oportunidades


A fin de :

- Asegurar que el SGSI cumpla lo previsto.
- Prevenir o reducer efectos no deseados.
- Lograr la mejora continua.

# 2. Planificación

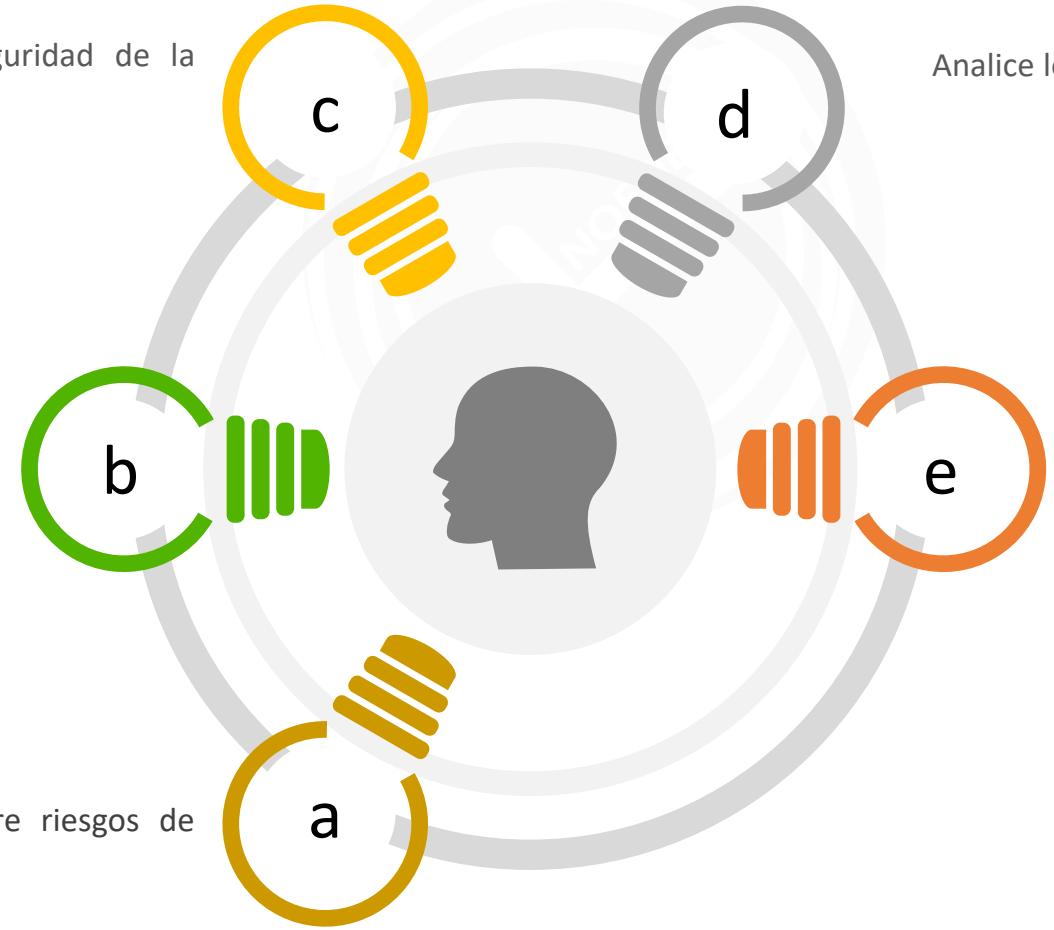
## 6.1 Acciones para abordar riesgos y oportunidades

### 6.1.2 Evaluación de los riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que:

Identifique los riesgos de seguridad de la información.

Analice los riesgos de seguridad de la información.




Asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables.

Evalúe los riesgos de seguridad de la información.

Establezca y mantenga criterios sobre riesgos de seguridad de la información.

Conservar

**Información documentada**

# 2. Planificación

## 6.1 Acciones para abordar riesgos y oportunidades

### 6.1.2 Evaluación de los riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que:

a

Establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:

1

Los criterios de aceptación de los riesgos.

2

Los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información.

Conservar

**Información documentada**

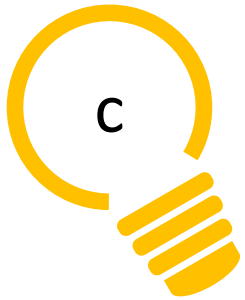
# 2. Planificación

## 6.1 Acciones para abordar riesgos y oportunidades

### 6.1.2 Evaluación de los riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que:

Identifique los riesgos de seguridad de la información:




Identificar riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información.



Identificando os dueños del riesgo

Conservar

**Información documentada**

# 2. Planificación

## 6.1 Acciones para abordar riesgos y oportunidades

### 6.1.2 Evaluación de los riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que:


Analice los riesgos de seguridad de la información:

1) Valorar las posibles consecuencias que resultarían si los riesgos llegan a materializarse.

2) Valorar de forma realista la probabilidad de ocurrencia de los riesgos identificados.

3) Determina los niveles de riesgo.

Conservar

**Información documentada**

# 2. Planificación

## 6.1 Acciones para abordar riesgos y oportunidades

### 6.1.2 Evaluación de los riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que:

e Evalúe los riesgos de seguridad de la información:

1. Comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos.
2. Priorizando el tratamiento de los riesgos analizados.

**Información documentada**

Conservar

# 2. Planificación

## 6.1.3 Tratamiento de los riesgos de seguridad de la información

La organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información:

**a.** Seleccionar las opciones adecuadas de tratamiento de riesgos de SI , teniendo en cuenta la apreciación de los riesgos.

**b.** Determinar todos lo controles necesarios para implementa la opción elegida de tratamiento de riesgos de SI.

**c.** Comparar los controles determinados con el anexo A y comprobar que no se ha omitido controles.

**d.** Elaborar una “Declaración de Aplicabilidad”

**e.** Formular un plan de tratamiento de riesgos de SI.

**f.** Obtener la aprobación del plan de tratamiento de riesgos de SI y la aceptación de los riesgos residuales de SI por parte de los dueños de los riesgos.

Conservar

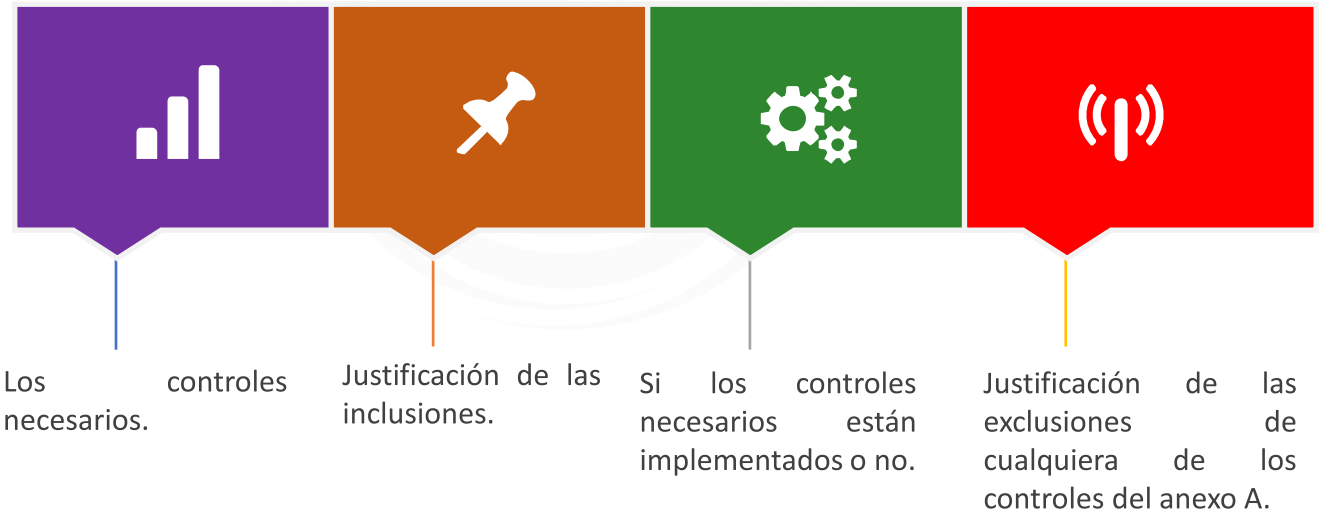
**Información documentada**

# 2. Planificación

## 6.1 Acciones para abordar riesgos y oportunidades

### 6.1.3 Tratamiento de los riesgos de seguridad de la información

DECLARACIÓN DE APLICABILIDAD
(contenido)



# ¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón