Centro de Especializaciones Noeder

Diploma de Especialización Internacional

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

CLASE 01

INTERPRETACIÓN DE LA NORMA ISO 27001

Mg. Ing. Julio Pereyra Rosales

1.Objeto y campo de aplicación

Proporciona:

- Una decisión estratégica para la organización.
- Confidecialidad, integridad y disponibilidad de la información mdiante el proceso de gestión de riesgos.
- Brinda confianza a las partes interesadas.
- Integración de los procesos de negocio.

2.Normas para consulta

ISO 27002: 2022

Buenas practicas de seguridad de la información.

ISO 27003: 2017

Guía para implementar el sistema de gestión de seguridad de la información

ISO 31000: 2018

Gestión del riesgo.

ISO 27000:2018

Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.

ISO 19011: 2018

Directrices para auditorías de sistemas de gestión

3.Términos y definiciones

3.1
Control de acceso
Medios para garantizar que el acceso a los activos está autorizado y restringido en función de la actividad empresarial y la seguridad

3.2
Ataque
Intentar destruir, exponer, alterar, inutilizar, robar u obtener acceso no autorizado a un activo o hacer un uso no autorizado del mismo.

3.23
Gobernanza d la seguridad de la información
Sistema por ele cual las actividades de seguridad de la información de una organización se dirigen y controlan.

3.28
Seguridad de la información
Preservación de la confidencialidad, integridad y disponibilidad de la información.

3.29
Continuidad de la seguridad de la información
Procesos y procedimientos para garantizar la continuidad de las operacioes de seguridad de la información.

3.30
Evento sobre seguridad de la información
Aparición identificada de un estado del sistema, servicio o red que indique una posible violencia de la política de seguridad de información o un fallo de los controles , o una situación previamente desconocida que pueda ser relevante para la seguridad.

4. Contexto de la organización

4.1 Comprensión de la organización y su contexto

La organización debe determinar :

4. Contexto de la organización

4.2 Comprensión de las necesidades y expectativas de partes interesadas

La organización debe determinar :

Partes interesadas que son pertinentes al SGSI.

- Los requisitos relevantes de estas partes interesadas para el SGSI.
- Cuáles de estos requisitos se abordarán a través del SGCSI.

4.2.1 Generalidades

4. Contexto de la organización

4.3 Determinar el alcance del SGSI.

La organización debe determinar :

- Límite
- Aplicabilidad

ISO 27001

Información documentada

Disponible.

La organización debe determinar :

Cuestiones internas.

Cuestiones externas.

Requisitos de partes interesadas pertinentes.

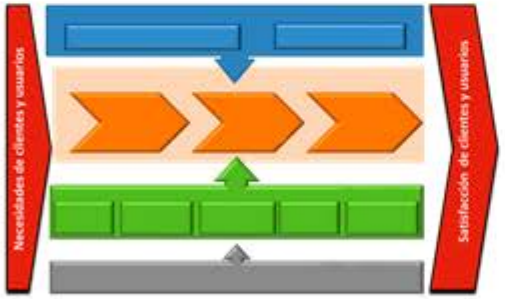
Productos y servicios

Interfases y dependencias entre las actividades realizadas por la empresa y las que se lleva a cabo por otras empresas.

4. Contexto de la organización

4.4 Sistema de gestión de seguridad de la información

La organización de debe establecer, implementar, mantener y mejorar el SGSI



La organización debe determinar los procesos necesarios para el SGSI y su aplicación en la empresa

5. 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.

5. 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.

5. 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:

5. 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.

6. 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.

6. Planificación

6.1 Acciones para abordar riesgos y oportunidades

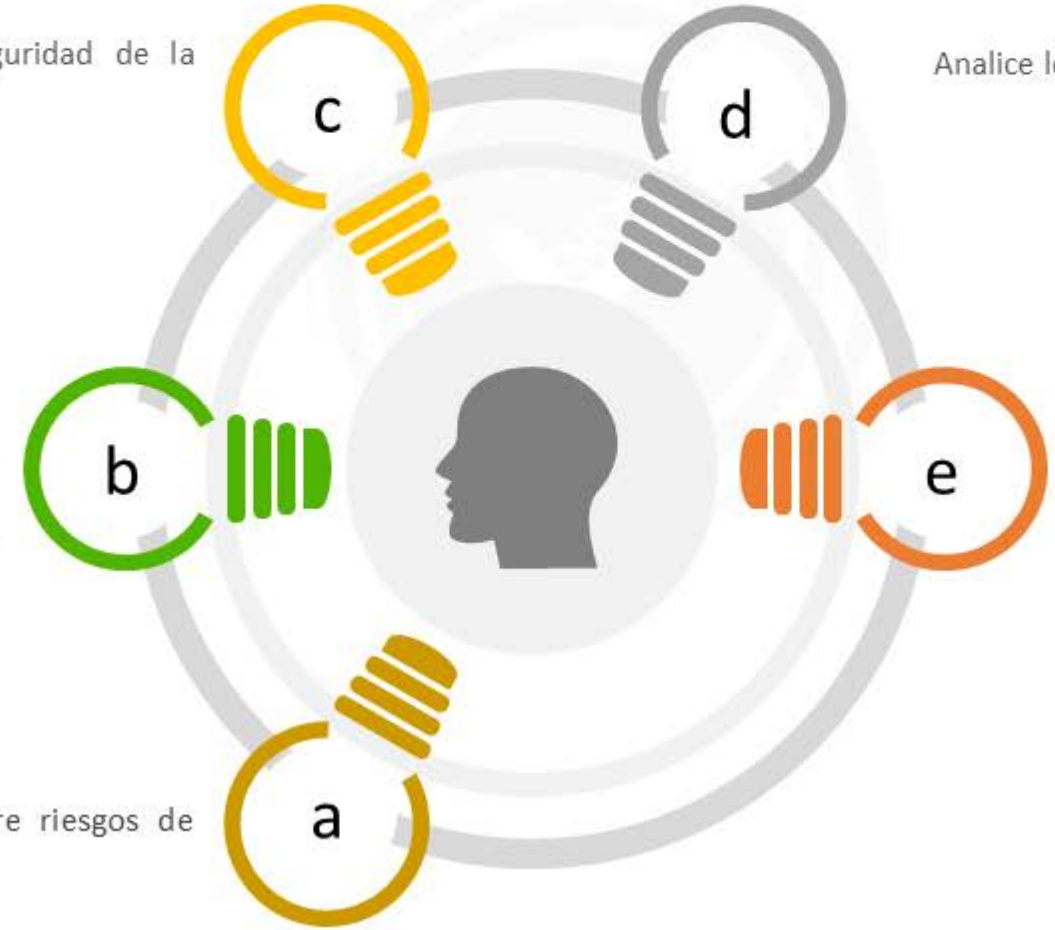
6.1.2 Evaluación de los riesgos de seguridad de la información

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

c) Identifique los riesgos de seguridad de la información.

d) Analice los riesgos de seguridad de la información.

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



e) Evalúe los riesgos de seguridad de la información.

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

Conservar

Información documentada

6. 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

6. 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:

C

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

1

2

Identificando os dueños del riesgo

Conservar

Información documentada

6. 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:

d

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

6. 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

6. 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

6. Planificación

6.1 Acciones para abordar riesgos y oportunidades

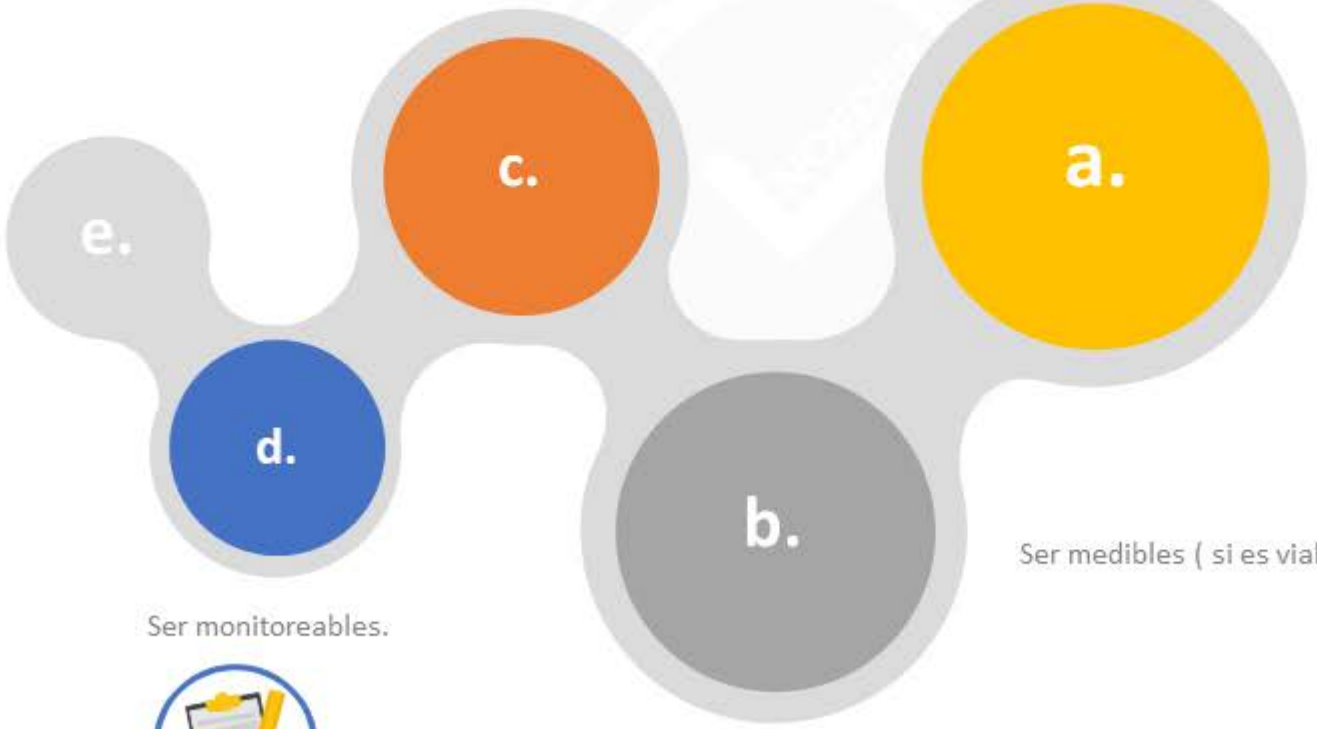
6.1.3 Tratamiento de los riesgos de seguridad de la información

DECLARACIÓN DE APLICABILIDAD
(contenido)

6. Planificación

6.2 Objetivos de seguridad de la información y planeación para su consecución

La organización debe establecer los objetivos del SGSI en las funciones y niveles pertinentes.



Ser coherentes con la política del SGSI.

Tener en cuenta los requisitos de SI y de la apreciación del riesgo.

Deben comunicarse.

Actualizarse según convenga.

Ser medibles (si es viable).

Ser monitoreables.

Conservar

Información documentada

6. Planificación

6.2 Objetivos de seguridad de la información y planeación para su consecución

La organización, al planificar el cómo logrará el cumplimiento de los objetivos , debe determinar: :

Qué se va a hacer

Qué recursos se necesitan

Quién será responsable

Cuándo se finalizará

Cómo se evaluará los resultados.

6. Planificación

6.3 Planificación de cambios

Cuando la organización determine la necesidad de cambios en el SGSI, estos cambios se deben llevar a cabo de manera planificada.

Debe considerar (recomendación de acuerdo a la norma ISO 9001:2015) :

01
El propósito del cambio y las consuencias potenciales.

02
La integridad del SGSI.

03
La disponibilidad de recursos.

04
La asignación o reasignación de responsabilidades y autoridad.

7. Recursos

7.1 Recursos

7. Recursos

7.2 Competencia

La organización debe :

Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño del SGSI.

Asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas.

Conservar la información documentada apropiada como evidencia de la competencia

Cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas

Conservar

Información documentada

7. Recursos

7.3 Concienciación

Las personas que realizan el trabajo bajo el control de la organización deben ser conscientes de :

a.La política del SGSI.

Las implicaciones del incumplimiento de los requisitos del SGSI.

b. Su contribución a la eficacia del SGSI, incluidos los beneficios de una mejora del desempeño de la SI.

7. Recursos

La organización debe determinar las necesidades de comunicaciones internas y externas pertinentes al SGSI, que incluyan :

7.4 Comunicación

7. Recursos

7.5 Información documentada

La información documentada requerida por esta Norma Internacional.

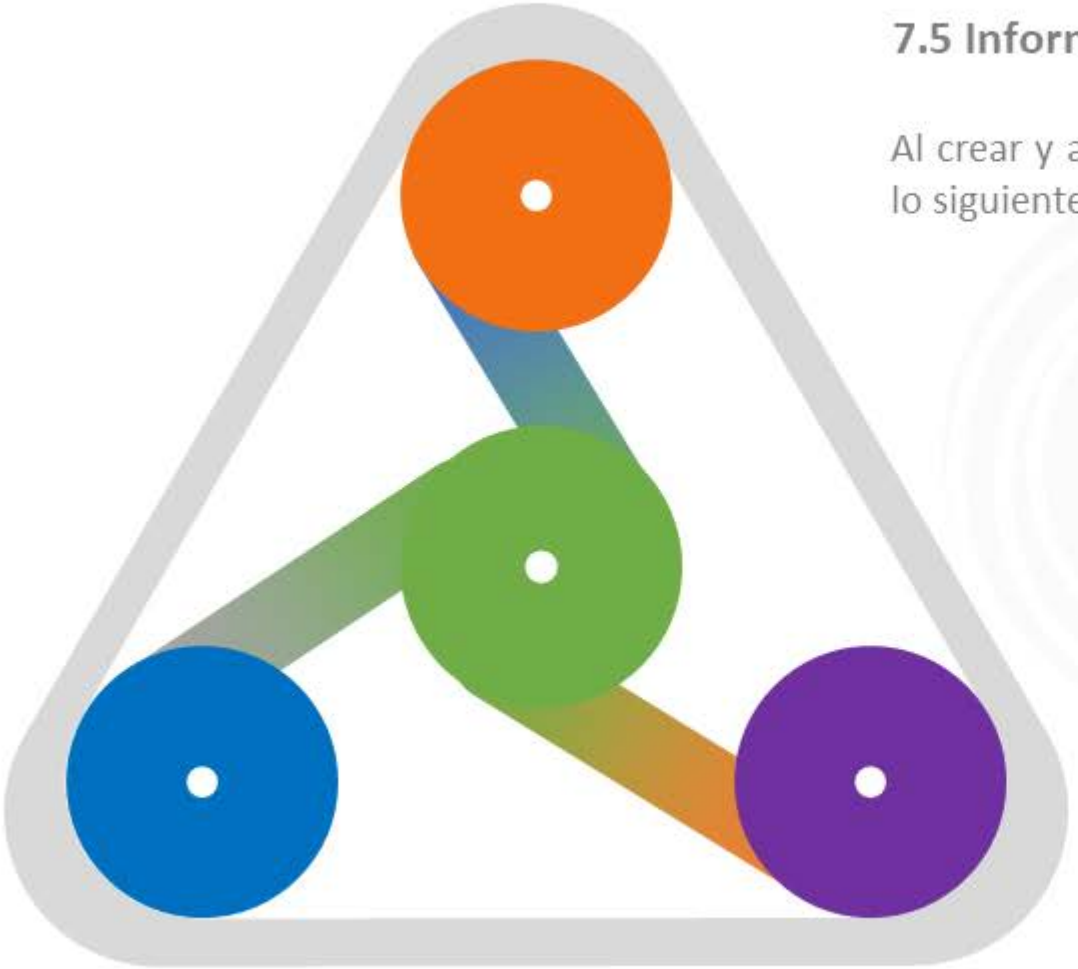
El SGSI debe incluir:

La información documentada que la organización determina como necesaria para la eficacia del SGSI.

Información documentada

7.5.1 Condiciones generales

7. Recursos



7.5 Información documentada

Al crear y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea apropiado :

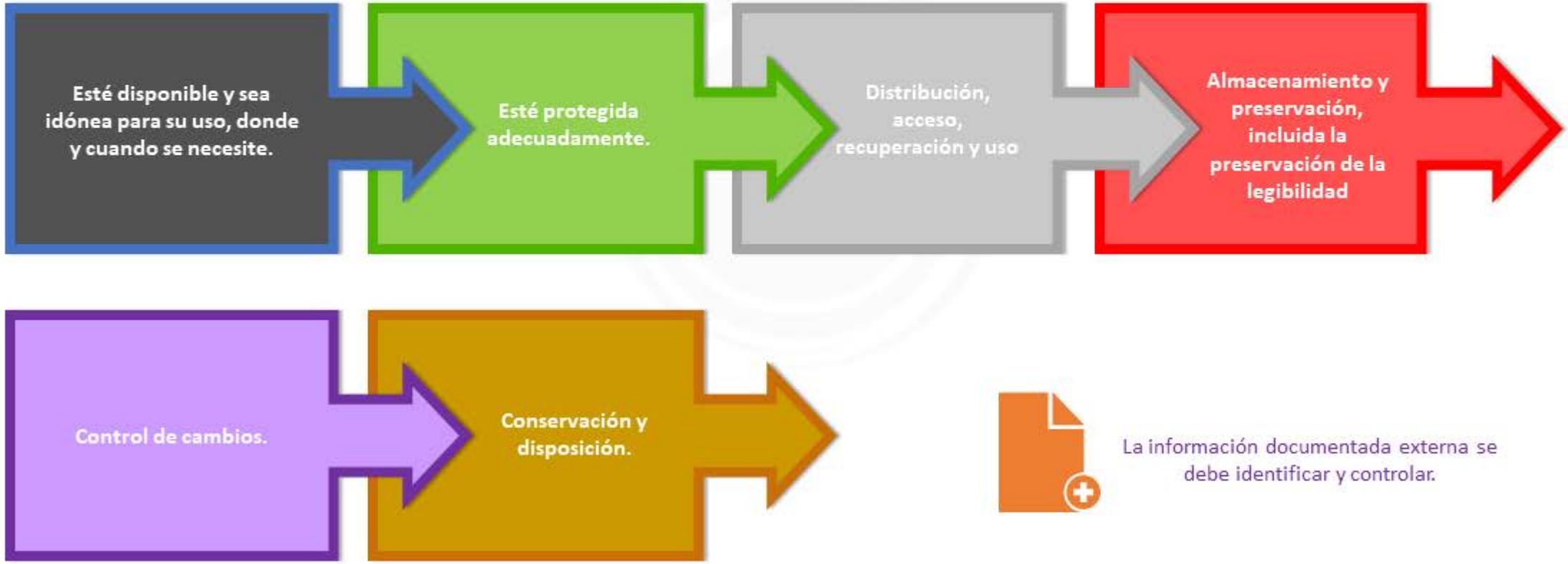
- La identificación y descripción (por ejemplo, título, fecha, autor o número de referencia)
- El formato (por ejemplo, idioma, versión del software, gráficos) y los medios de soporte (por ejemplo, papel, electrónico)
- La revisión y aprobación con respecto a la idoneidad y adecuación.

7.5.2 Creación y actualización

7. Recursos

7.5 Información documentada

La información documentada requerida por el SGCN y por esta Norma Internacional se debe controlar para asegurarse de que:



La información documentada externa se debe identificar y controlar.

7.5.3 Control de la información documentada

8. Operaciones

8. Operación

8.1 Planificación y control operacional

8.2 Evaluación de los riesgos de seguridad de la información

8.3 Tratamiento de los riesgos de seguridad de la información.

8. Operaciones

8. Operación

8.1 Planificación y control operacional

La organización debe :

Implementar

Planificar

Controlar

Para cumplir los requisitos del SGSI.

Para implementar acciones de la planificación (capítulo 6)

8. Operaciones

8. Operación

8.1 Planificación y control operacional

- Estableciendo criterios para los procesos.
- Implementando controles de los procesos acorde a los criterios.
- Determinación, mantenimiento y conservación de información documentada necesaria (a fin de cumplir lo planificado)
- Controlar los cambios planificados y revisar la consecuencia de los cambios no previstos (tomando acciones)
- Asegurarse que los procesos externos se controlen.

8. Operaciones

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

1. Asignación de responsabilidades en SI.
2. Segregación de tareas
3. Contacto con autoridades
4. Contacto con autoridades
5. Seguridad de la información en los proyectos

I. RESPONSABILIDADES EN EL SGSI

8. Operaciones

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

1. Teletrabajo.

2. Política de seguridad en dispositivos móviles

8. Operaciones

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

8. Operaciones

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

1.Establecer criterios para afrontar la seguridad de la información asociada al cese o cambio de puestos de trabajo.

IV. CESE O CAMBIO DE PUESTOS

8. Operaciones

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

01

- Clasificación de la información.

02

- Etiquetado y manipulación de la información.

03

- Manipulación de activos.

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

01 Gestión de soportes extraíbles

02 Eliminación de soportes

03 Soportes físicos en tránsito.

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

8. Operación

8.1 Planificación y control operacional

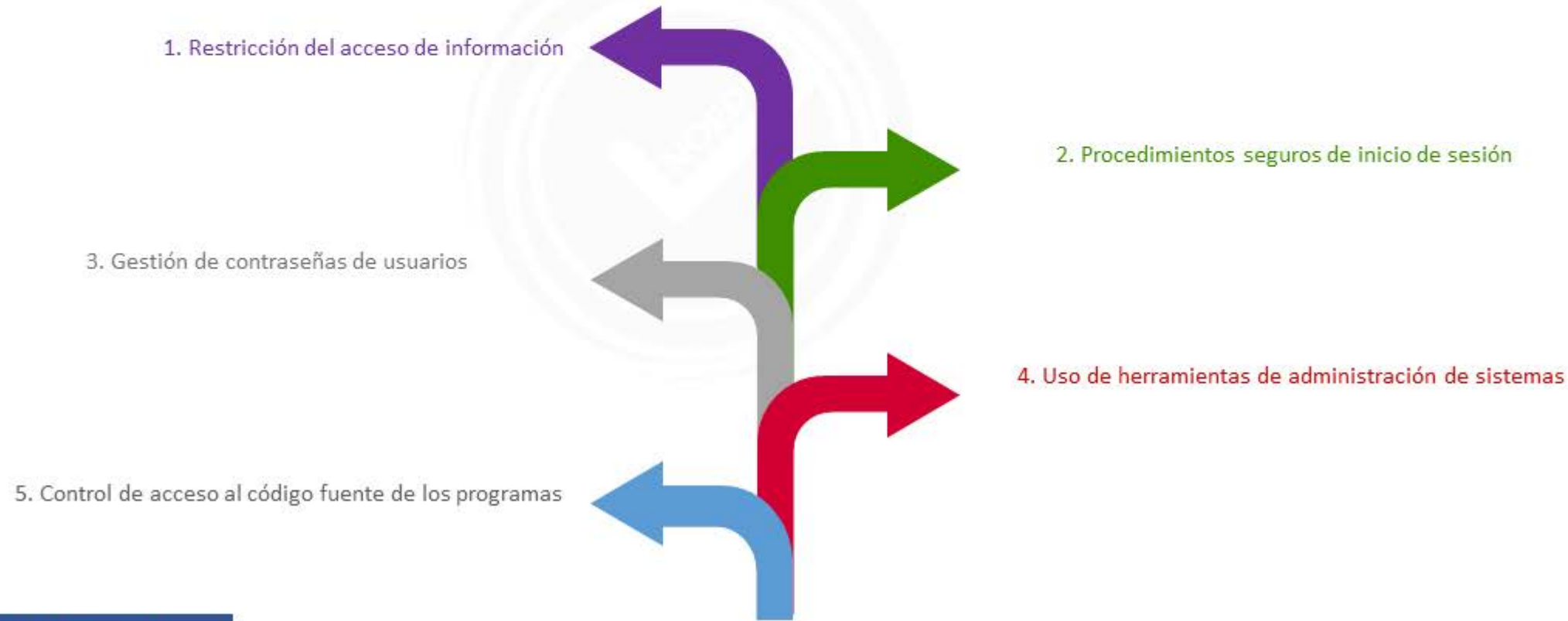
Se recomienda que la organización documente su **planificación y aplicación de controles** para :

Uso de información confidencial para la autenticación

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

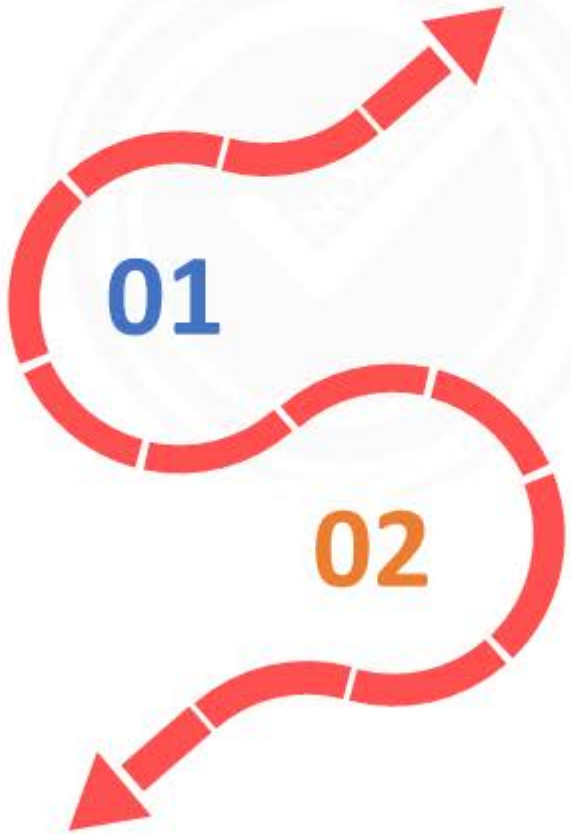


8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

Gestión de áreas seguras



Seguridad de los equipos

- Protección de equipos.
- Instalaciones de suministros.
- Seguridad del cableado.
- Mantenimiento de equipos.
- Sala de activos fuera de la empresa.
- Reutilización y retirada de dispositivos.
- Equipo informático de usuario desantendido.
- Política de puesto de trabajo despejado y bloqueo de pantalla.

8. Operación

8.1 Planificación y control operacional

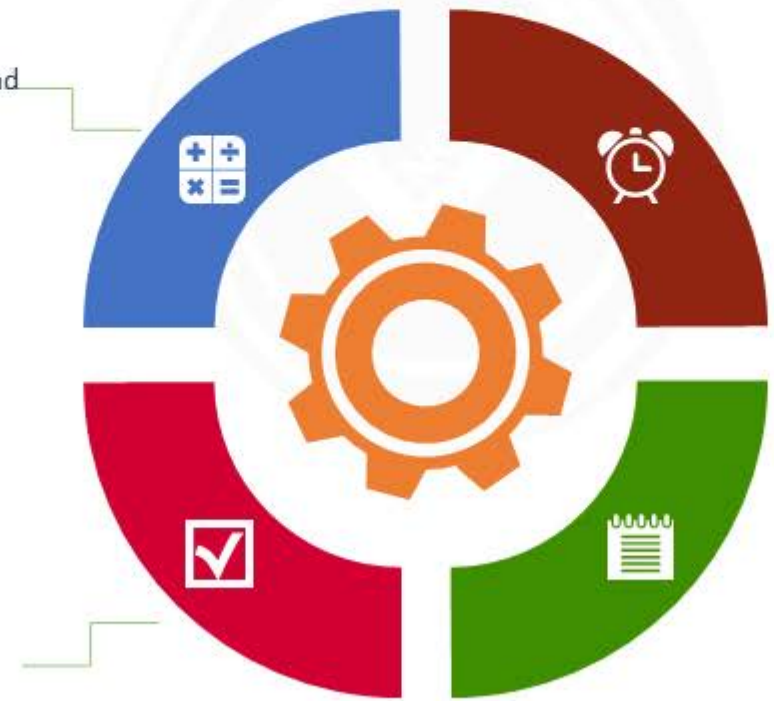
Se recomienda que la organización documente su **planificación y aplicación de controles** para :

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

1.Gestión de compras de seguridad



3.Registro y control de eventos

2.Registro de actividad y supervisión.

4.Protección de los registros de información.

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

2.Si la empresa cambia algún requisito del servicio, lo debe comunicar al cliente (comunicaciones formales)

3.Sincronización de relojes

1.Registros de actividad del administrador y operador del sistema

4.Instalación del software en las áreas de producción.

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

1.Gestión de vulnerabilidades técnicas

2.Restricciones en las instalaciones de software.

3. Controles de auditoría en los sistemas de información

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

1. Controles de redes

2. Mecanismos de seguridad asociadas a la red

3. Política y procedimientos de intercambio de información

3. Acuerdos de intercambio de información.

8. Operación

8.1 Planificación y control operacional

Se recomienda que la organización documente su **planificación y aplicación de controles** para :

1. Mensajería electrónica

2. Acuerdos de confidencialidad y acuerdos.

8. Operación

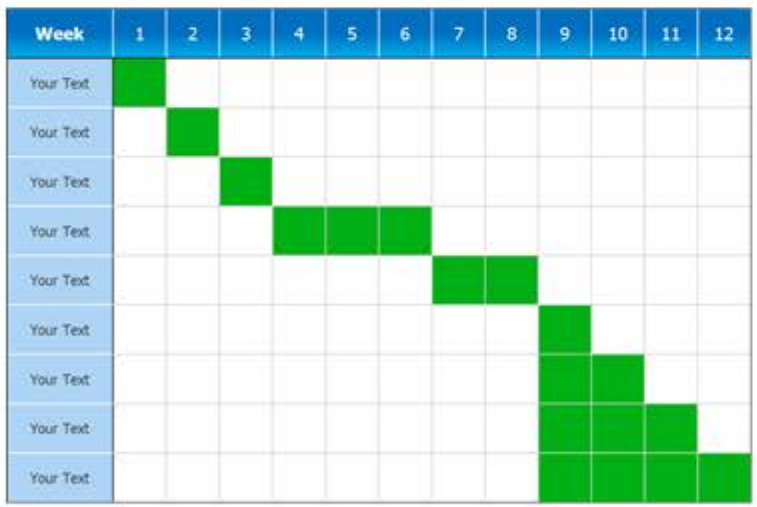
8.2 Evaluación de los riesgos de seguridad de la información

La organización debe:

8. Operación

8.3 Tratamiento de los riesgos de seguridad de la información.

La organización debe:



Implementar el Plan de Tratamiento de los Riesgos de Seguridad de la Información.

Información documentada

Conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de la información.

9. Evaluación de Desempeño

9.1 Monitoreo, medición, análisis y evaluación

La organización debe determinar:

a.

A qué es necesario monitorizar y medir, incluyendo procesos y controles de SI.

b.

Métodos de monitorización, medición, análisis y evaluación para asegurar resultados válidos.

Los métodos seleccionados deben producir resultados comparables y reproducibles.

c. , d.

Cuándo y quién dará el seguimiento, y medición.

e.

Cuándo y quién realizará la evaluación y análisis de los resultados del seguimiento y medición.

Evaluar el desempeño y eficacia del SGSI.

Información documentada

9. Evaluación de Desempeño

9. Evaluación de desempeño

9.2 Auditoría Interna / 9.2.1 Consideraciones generales

- Es conforme con la norma ISO 27001
- Es conforme con los requisitos establecidos por la empresa.

Si el SGSI se implementa y es eficaz.

La organización debe realizar auditorias internas a intervalos planificados del SGSI.

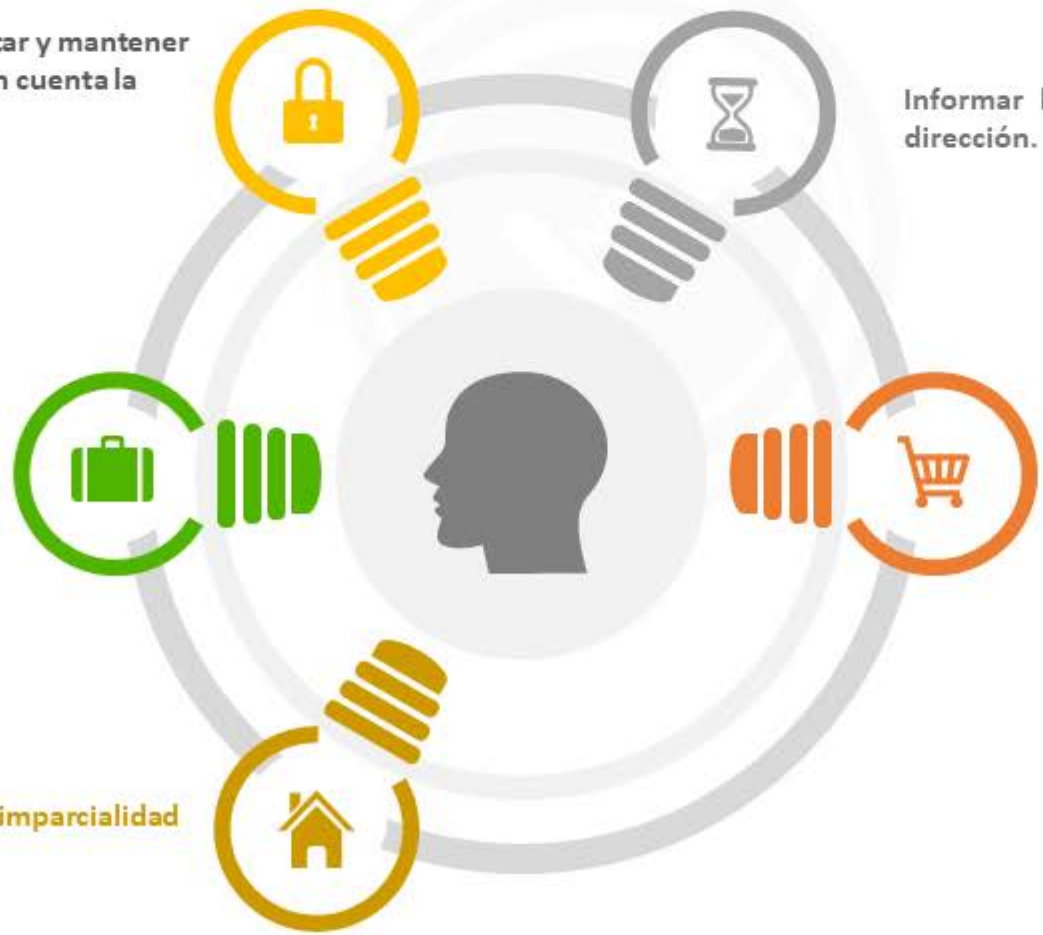
9. Evaluación de Desempeño

9.2.2 Auditoría Interna / 9.2.2 Programa de auditoría interna

La organización debe determinar:

Planificar, establecer, implementar y mantener programas de auditoría. Tener en cuenta la importancia de los procesos.

Informar los resultados de auditoría a la dirección.



Definir los criterios y alcance de auditoría.

Selección de auditores (imparcialidad y objetividad)

Información documentada

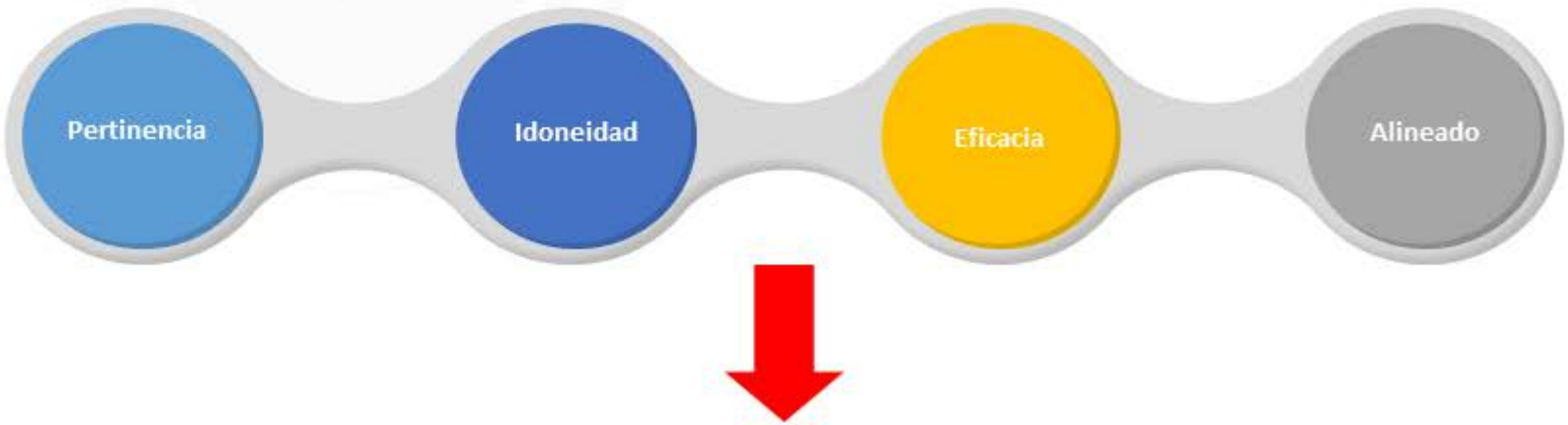
Evidencia de cumplimiento del programa y los resultados de auditoria.

9. Evaluación de Desempeño

9.3. Revisión por la dirección/ 9.3.1 Consideraciones generales

La Alta Dirección debe revisar a intervalos planificados el SGSI.

A fin de asegurar :



DIRECCIÓN ESTRATÉGICA

9. Evaluación de Desempeño

9.3 Revisión por la dirección/ 9.3.2_9.3.3 Entradas y resultados

Entradas

a. Estado de las Revisiones por la Dirección previas

b. Cambios en cuestiones internas y externas

c. Cambios en necesidades y expectativas de P.I.

d. Información sobre el comportamiento de la S.I.:

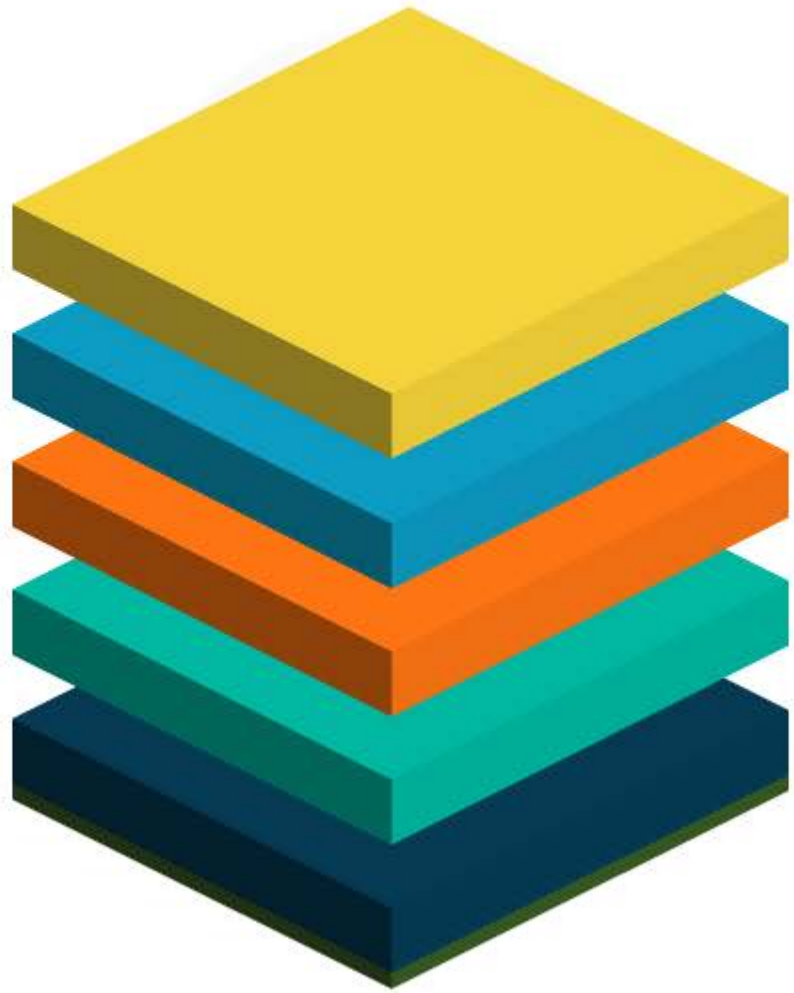
Tendencias:

- No conformidades y acciones correctivas.
- Seguimiento y resultados de la evaluación de la medición.
- Resultado de auditorías
- Cumplimiento de los objetivos de S.I.

e. Comentarios de las partes interesadas

f. Resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.

g. Oportunidades de mejora



Resultados

Oportunidades de mejoramiento continuo

Cualquier necesidad de cambio en el SGSI

Información documentada

- Disponible como evidencia de resultados de lña revisión por la dirección.

10 . Mejora

10.1 Mejora Continua

La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del SGSI.

10 . Mejora

Cuando ocurra una NC incluido por quejas se debe:

Información documentada

Naturaleza de la NC y cualquier acción tomada.
Resultado de acciones correctivas.

- **A**
  - Tomar acciones para controlar y corregir
  - Hacer frente a las consecuencias
- **B**
  - Revisión y análisis de la NC
  - Determinación de las causas de NC
  - Determinar NC similares
- **C**
  - Según el proceso y las circunstancias
- **D**
  - Verificar que no se han presentado eventos relacionados a la NC
- **E**
  - Según el proceso y sus riesgos
- **F**
  - Cambios en todo el SGSI.
- **G**
  - Proporcionales

10.2 No Conformidad y Acción Correctiva

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón