Centro de Especializaciones Noeder

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR ISO 27001 E ISO 22301

CICLO INTENSIVO

MÓDULO I

INTERPRETACIÓN DE LA NORMA ISO 27001-2022

Ing. Johnattan Sifuentes Rojas

MODULO I – INTERPRETACIÓN DE LA NORMA ISO 27001 - 2022

CONTENIDO MODULO I

1. Alcance del Sistema de Gestión de Seguridad de la Información (SGSI)
2. Gestión del contexto organizacional
3. Liderazgo y compromiso en el SGSI
4. Planificación del SGSI
5. Gestión de objetivos y planificación de cambios
6. Gestión de recursos
7. Toma de conciencia y comunicación organizacional
8. Gestión de operaciones
9. Gestión del riesgo operacional
10. Evaluación de desempeño
11. Mejora continua
12. Anexo A – Controles de Seguridad de la Información (SoA)

ALCANDE DEL SGSI

ISO 27001
Sistema de Gestión de la Seguridad de la Información SGSI

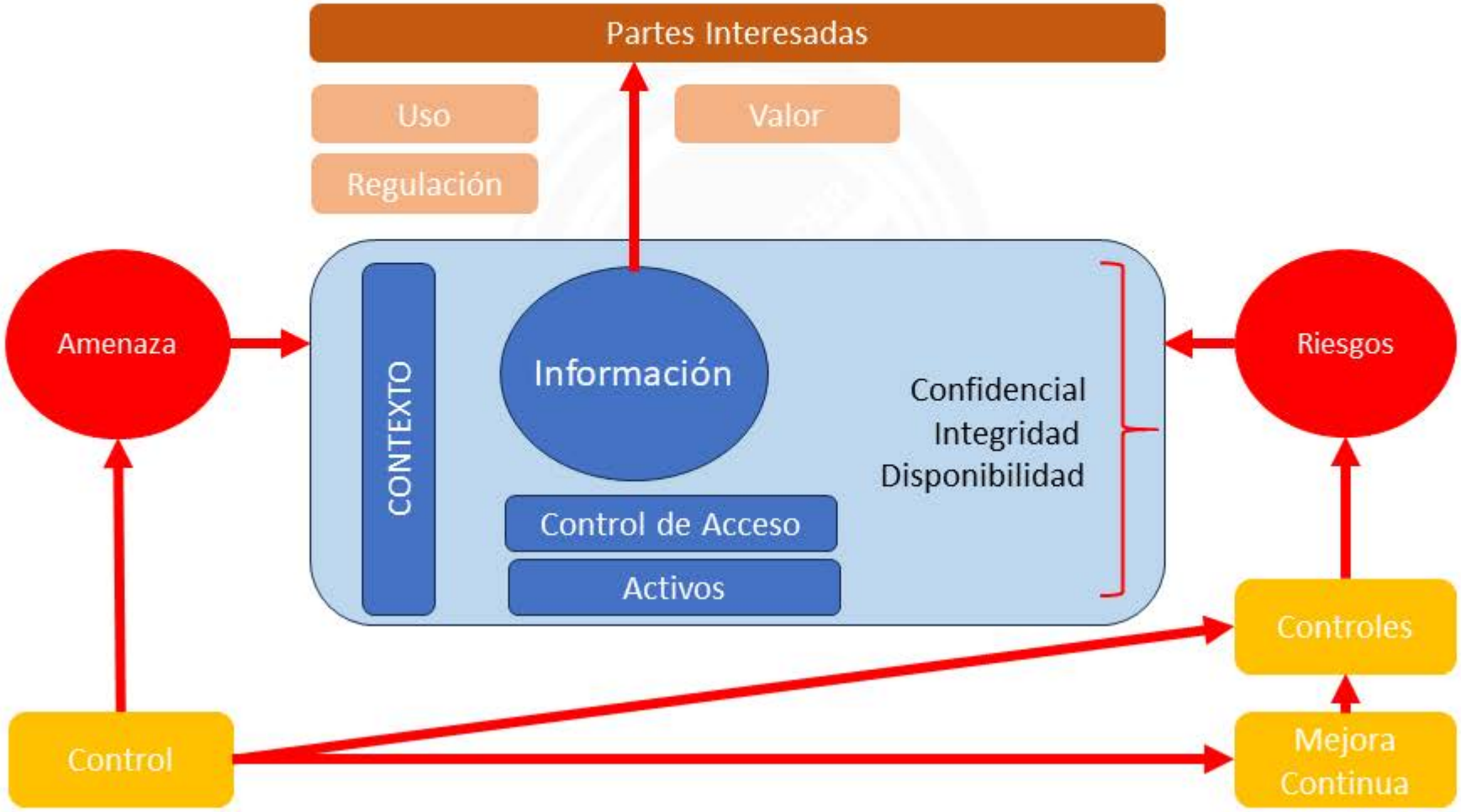
Objetivos:

- Proporcionar las mejoras practicas de seguridad de la información
- Permitir a las organizaciones desarrollar, implementar y medir las practicas eficaz de gestión de la seguridad
- Proporcionar seguridad y confianza entre las organizaciones.
- Aplicable a una amplia gama de organizaciones – grandes, mediana y pequeñas empresas

INTEGRIDAD	CONFIDENCIALIDAD	DISPONIBILIDAD
La información no puede manipularse sin autorización expresa	Solo pueden acceder a la información las personas autorizadas	El acceso a la información debe garantizarse en todo momento

ALCANDE DEL SGSI

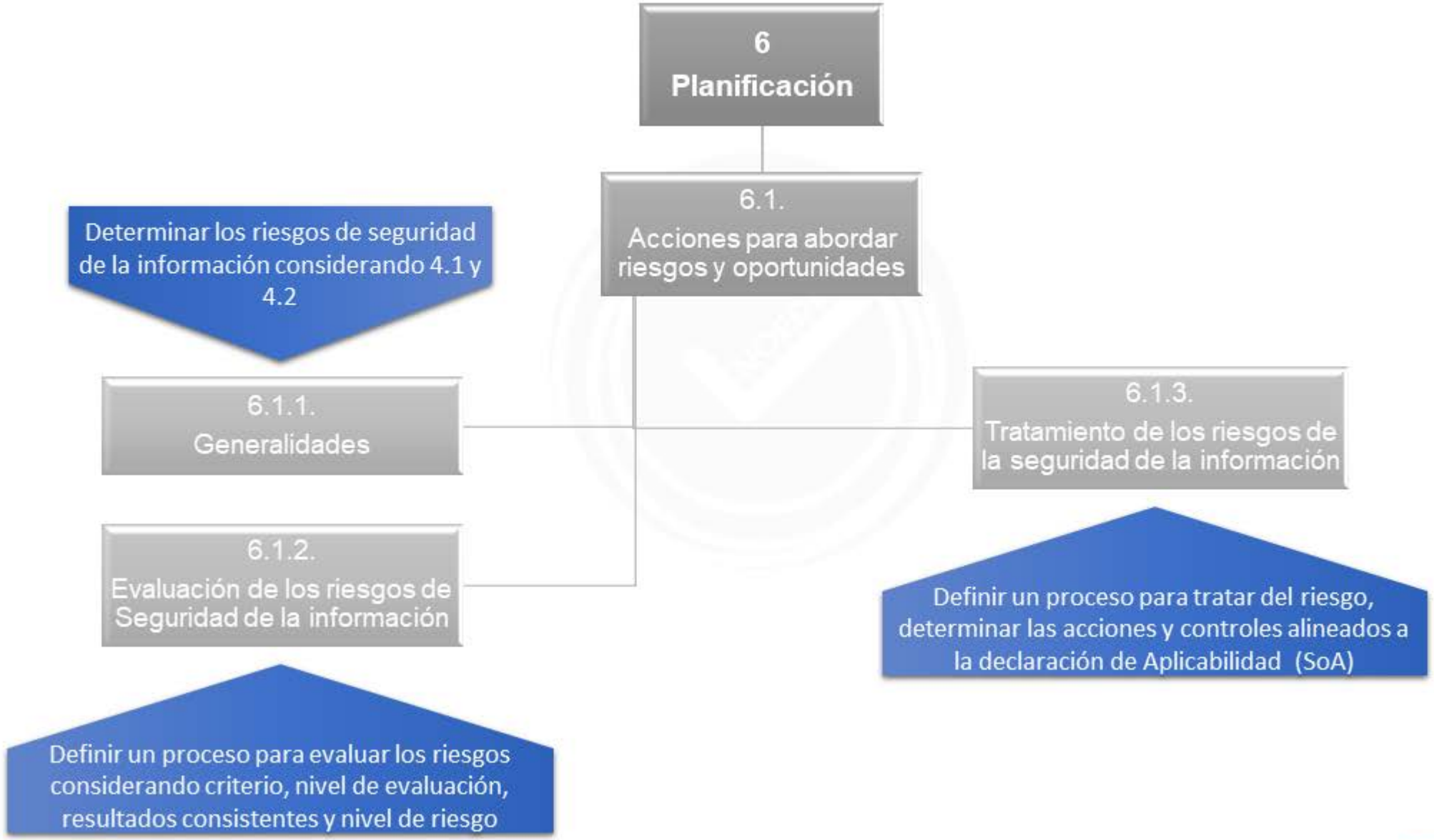
Seguridad de la información, ciberseguridad y protección de la privacidad.



GESTIÓN DEL CONTEXTO ORGANIZACIONAL

LIDERAZGO Y COMPROMISO DEL SGSI

PLANIFICACIÓN DEL SGSI



GESTION DE OBJETIVOS Y PLANIFICACIÓN DE CAMBIOS

6
Planificación

6.2.
Objetivos del SGSI y planificación para lograrlos

Determinar los objetivos y niveles considerando que se hará, qué recursos, responsable, cuando y como se evaluará

6.3.
Planificación de Cambios

Determinar las necesidades de cambios en el SGSI

Proceso de Gestión de Cambios

GESTION DE RECURSOS

7
Soporte

7.1.
Recursos

La organización debe determinar y proporcionar los recursos para establecer, implementar, mantener y mejorar el SGSI

7.2.
Competencia

Determinar la competencia de la(s) persona(s), asegurar las competencias en la educación, formación y experiencia.

CISO = Desarrolla estrategia
ISO = Ejecuta la política y controles
ISM = implementación de controles, el análisis de riesgos y la mejora continua

TOMA DE CONCIENCIA Y COMUNICACIÓN ORGANIZACIONAL

7
Soporte

7.3. Toma de Conciencia	7.4. Comunicación	7.5. Información documentada
La organización debe de tomar conciencia en la política, contribuir en la eficacia y mejora del desempeño	Determinar las necesidades de comunicación interna y externas incluyendo: qué comunicar, cuando comunicar, con quién comunicarse y cómo comunicarse	Información documentada determinada por la organización para asegurar la efectividad del SGSI considerando procesos, procedimientos y demás documentos

GESTIÓN DE OPERACIONES

8
Operación

8.1.
Planificación y control operacional

Debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos en base a los criterios establecidos en el capitulo 6.

8.2
Evaluación de los riesgos de seguridad de la información

Debe realizar evaluaciones de riesgos en intervalos planificados o cuando se tenga cambios significativos considerandos 6.1.2, conservar información documentada

8.3.
Tratamiento de los riesgos de la Seguridad de la Información

Debe de implementar el plan de tratamiento mantenimiento la información documentada.

GESTIÓN DEL RIESGO OPERACIONAL

8
Operación

8.2
Evaluación de los riesgos de seguridad de la información

Debe realizar evaluaciones de riesgos en intervalos planificados o cuando se tenga cambios significativos considerandos 6.1.2, conservar información documentada

8.3.
Tratamiento de los riesgos de la Seguridad de la Información

Debe de implementar el plan de tratamiento mantenimiento la información documentada.

EVALUACION DE DESEPEÑO

9
Evaluación del Desempeño

9.1.
Seguimiento, medición, análisis y evaluación

Debe hacer seguimiento y medición de los procesos y controles de SI considerando resultados comparables, periodicidad, responsable, evaluado y análisis de resultados.

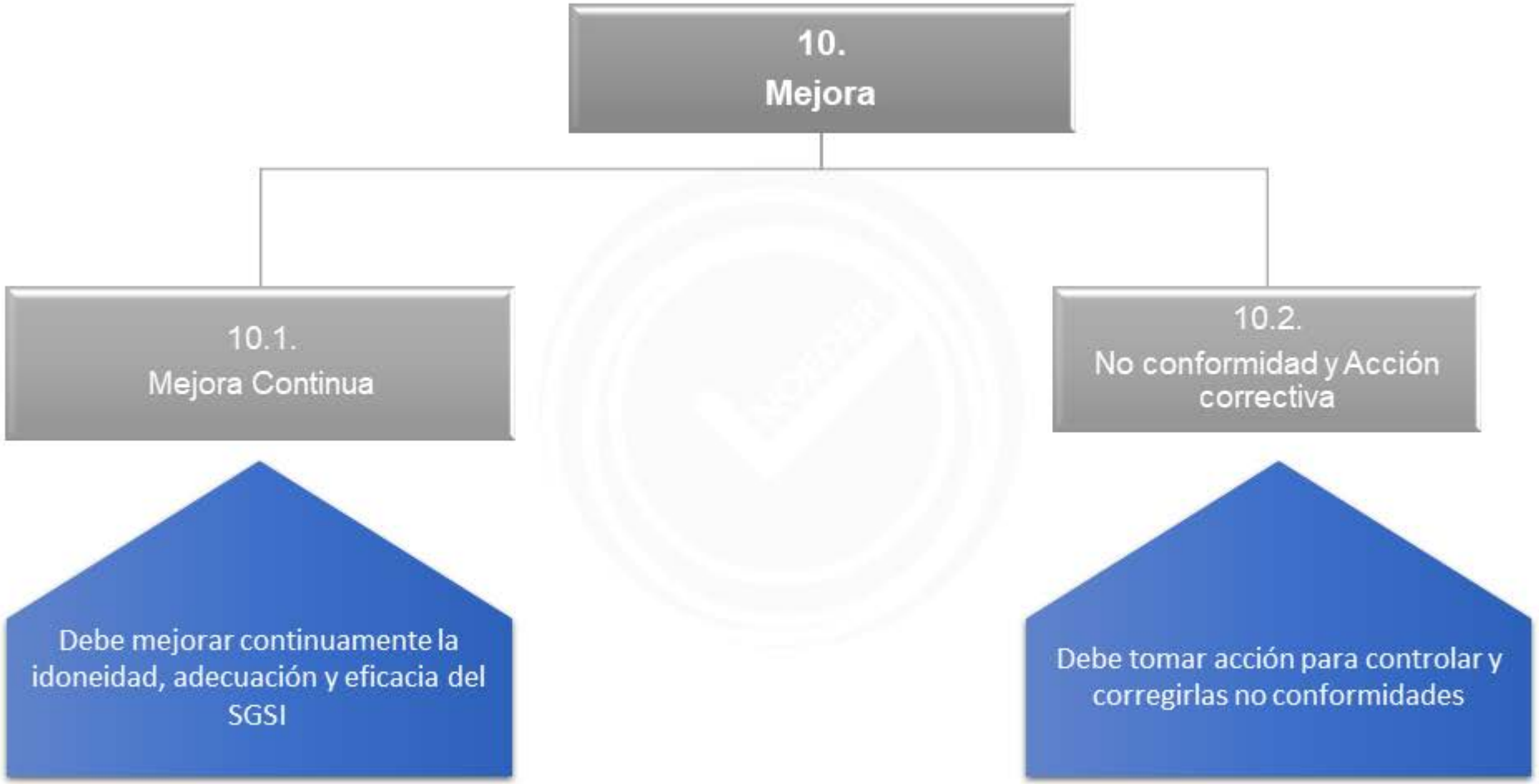
9.2.
Auditoria Interna

Debe planificar y programar auditorias internas para proporcionar información sobre el SGSI.

9.3.
Revisión por la dirección

La alta dirección debe revisar el SGSI en intervalos planificados para asegurar su idoneidad, adecuación y eficacia continua.

MEJORA CONTINUA



Anexo A – Controles de Seguridad de la Información (SoA)

93 controles que deben ser referenciados en la declaración de aplicabilidad

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón