Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

CICLO REGULAR

MÓDULO III

CLASE 03

INTERPRETACIÓN DE LA NORMA ISO 27001:2022

Ing. Johnattan Sifuentes Rojas

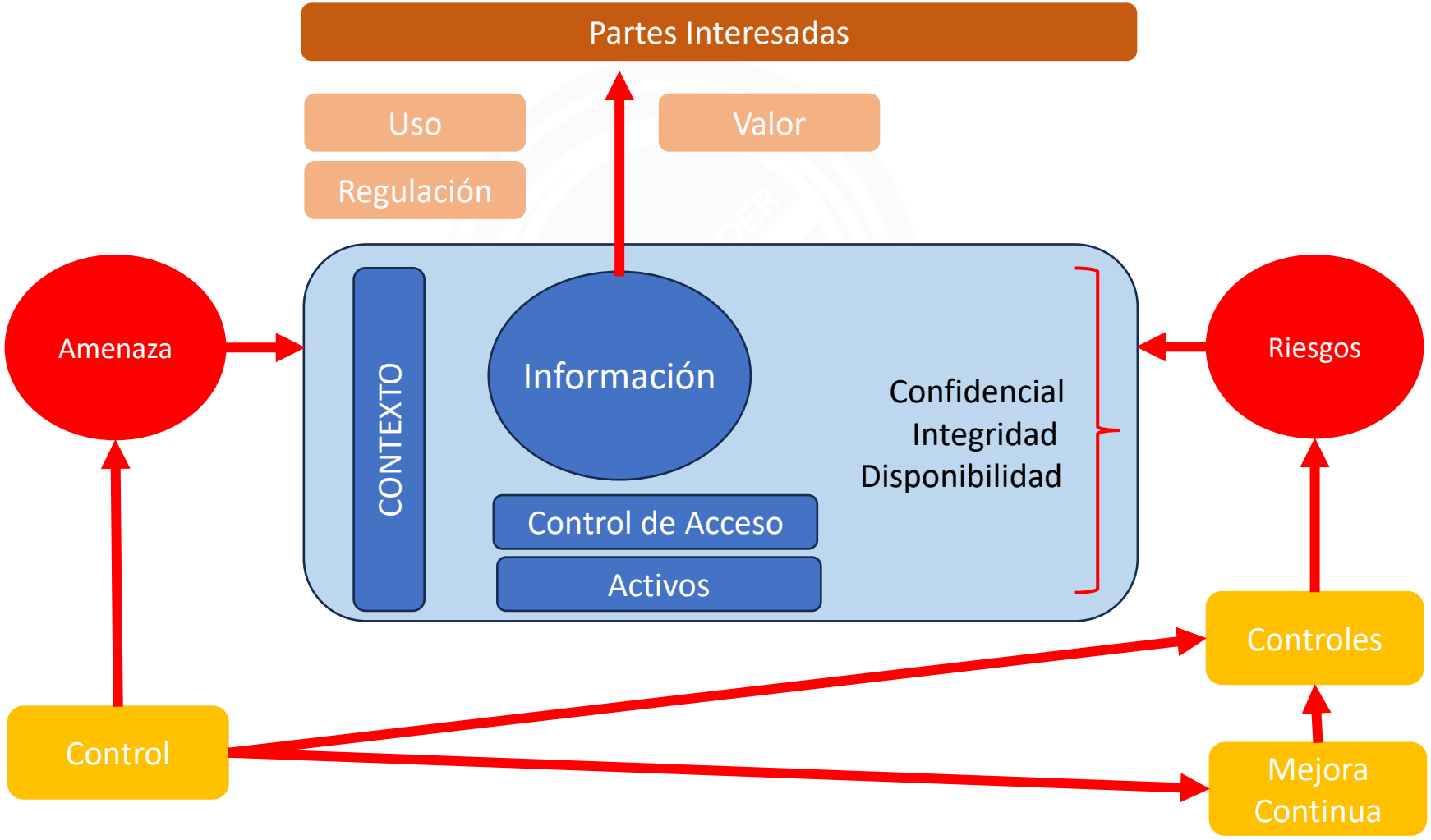
MODULO III – INTERPRETACIÓN DE LA NORMA ISO 27001 : 2022

CONTENIDO MODULO III – SESION 3

1. Alcance del SGSI
2. Evaluación del desempeño
3. Mejora
4. Referencia de los controles de Seguridad de la Información

ALCANDE DEL SGSI

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



EVALUACION DE DESEPEÑO

9
Evaluación del Desempeño

9.1. Seguimiento, medición, análisis y evaluación

- Seguimiento, medición, análisis y evaluación de los procesos y controles de S.I. para ser considerados validos.
- Establecer cuando debe ser realizado el seguimiento y medición.
- Quien y cuando deben hacer el seguimiento, medición, análisis y evaluación los resultados.
- Información documentada
- Evaluar el desempeño y eficacia del SGSI

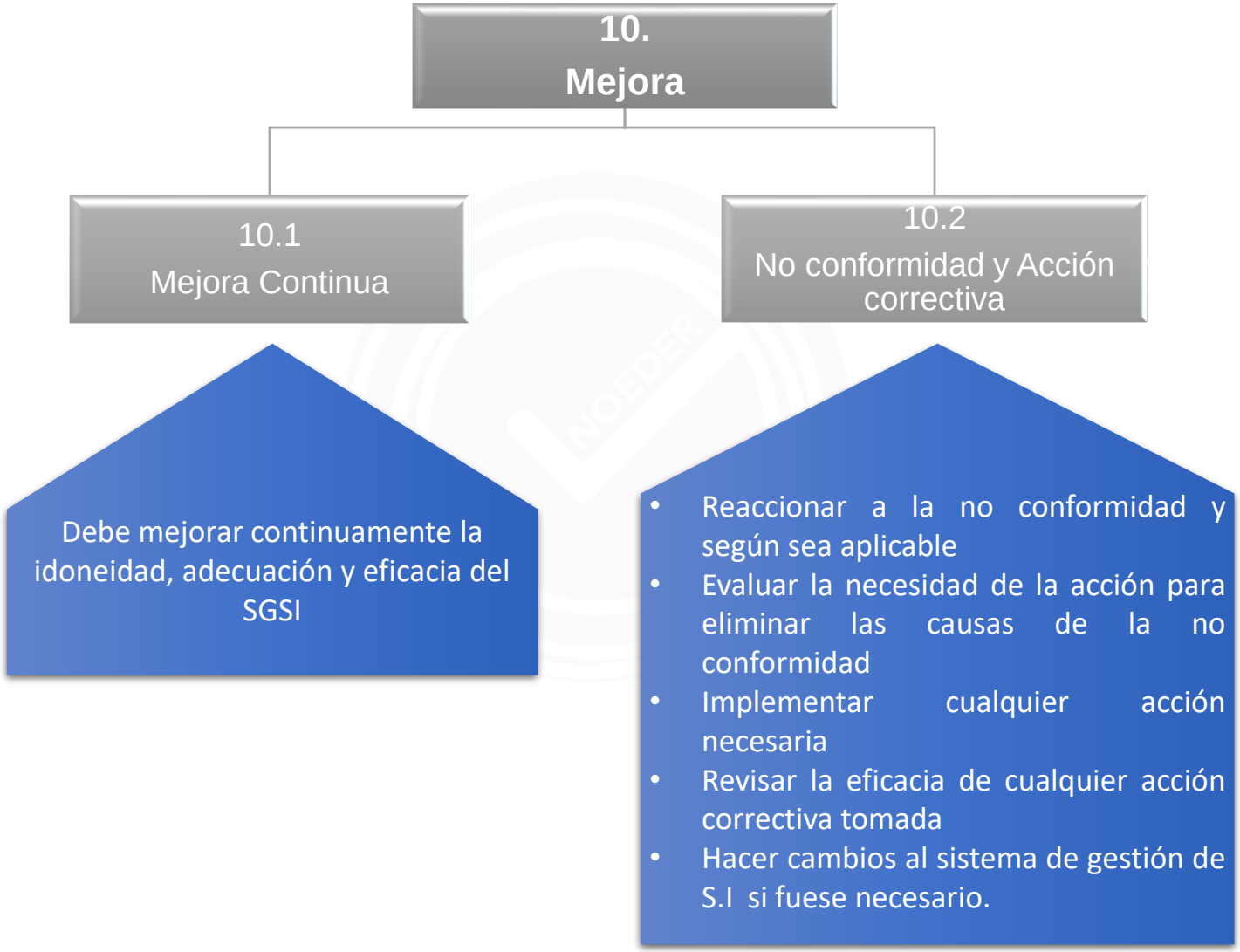
9.2. Auditoria Interna

- Debe planificar y programar auditorias internas para proporcionar información sobre el SGSI.
- Estar en conformidad con la NTP
- Estar eficazmente implementado y mantenido.
- Programar Auditoria interna periódicamente.

9.3. Revisión por la dirección

La alta dirección debe revisar el SGSI en intervalos planificados para asegurar su idoneidad, adecuación y eficacia continúa considerando los requisitos solicitados en las entradas para la revisión por la dirección (Req. 9.3.2.) y Resultados de la revisión por la dirección.

MEJORA CONTINUA



REFERENCIA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Tabla A.1 – Controles de seguridad de la información

5	**Controles organizacionales**	
5.1	Políticas para la seguridad de la información	**Control** La política de seguridad de la información y políticas específicas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y conocidas tanto por el personal como por las partes interesadas pertinentes, además revisadas en intervalos planificados y cuando ocurran cambios significativos.
5.2	Roles y responsabilidades en seguridad de la información	**Control** Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.
5.3	Segregación de funciones	**Control** Funciones en conflicto y áreas de responsabilidad en conflicto deben ser segregadas.
5.4	Responsabilidades de la dirección	**Control** La dirección debe requerir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y procedimientos específicos de la organización.
5.5	Contacto con autoridades	**Control** La organización debe establecer y mantener contacto con las autoridades pertinentes.

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad