



Centro de
Especializaciones
Noeder



Florida
Global
University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE SEGURIDAD DE LA INFORMACION ISO 27001

CICLO INTENSIVO

MÓDULO IV

**IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN
DE SEGURIDAD DE LA INFORMACION (SGSI)**

Ing. Johnattan Sifuentes Rojas



MODULO IV – IMPLEMENTACIÓN DE LA NORMA ISO 27001 - 2022

CONTENIDO MODULO IV

1. Gestión del contexto organizacional
2. Liderazgo y compromiso en el SGSI
3. Planificación del SGSI
4. Gestión de objetivos y planificación de cambios
5. Gestión de recursos
6. Gestión de la comunicación y documentación
7. Gestión de operaciones
8. Gestión del riesgo operacional
9. Evaluación de desempeño
10. Mejora continua



ALCANDE DEL SGSI

ISO 27001

Sistema de Gestión de la Seguridad de la Información SGSI





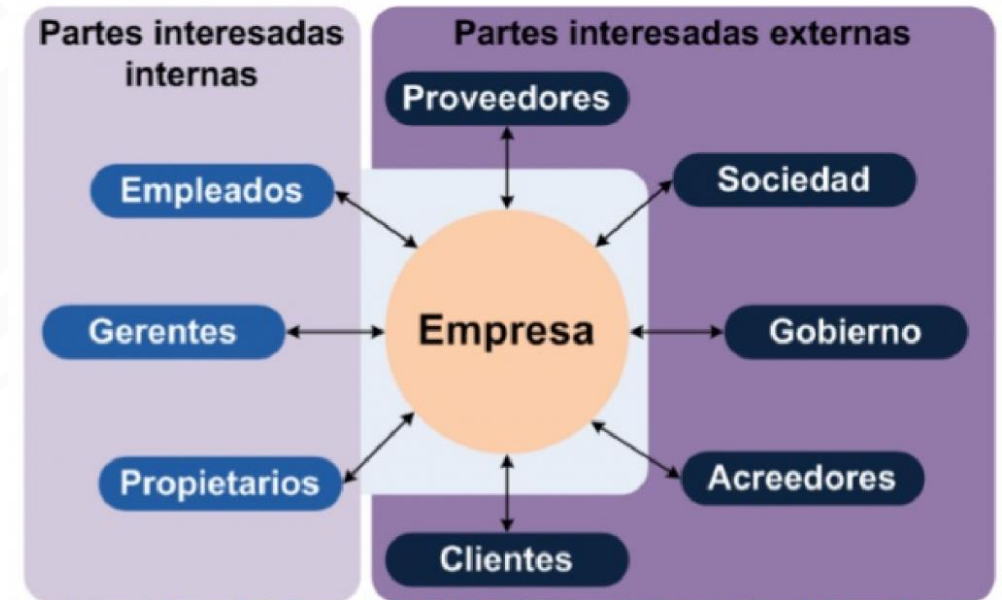
GESTION DEL CONTEXTO DE LA ORGANIZACION

1 Establecer el contexto de la organización

Análisis Interno y externo



Partes Interesadas



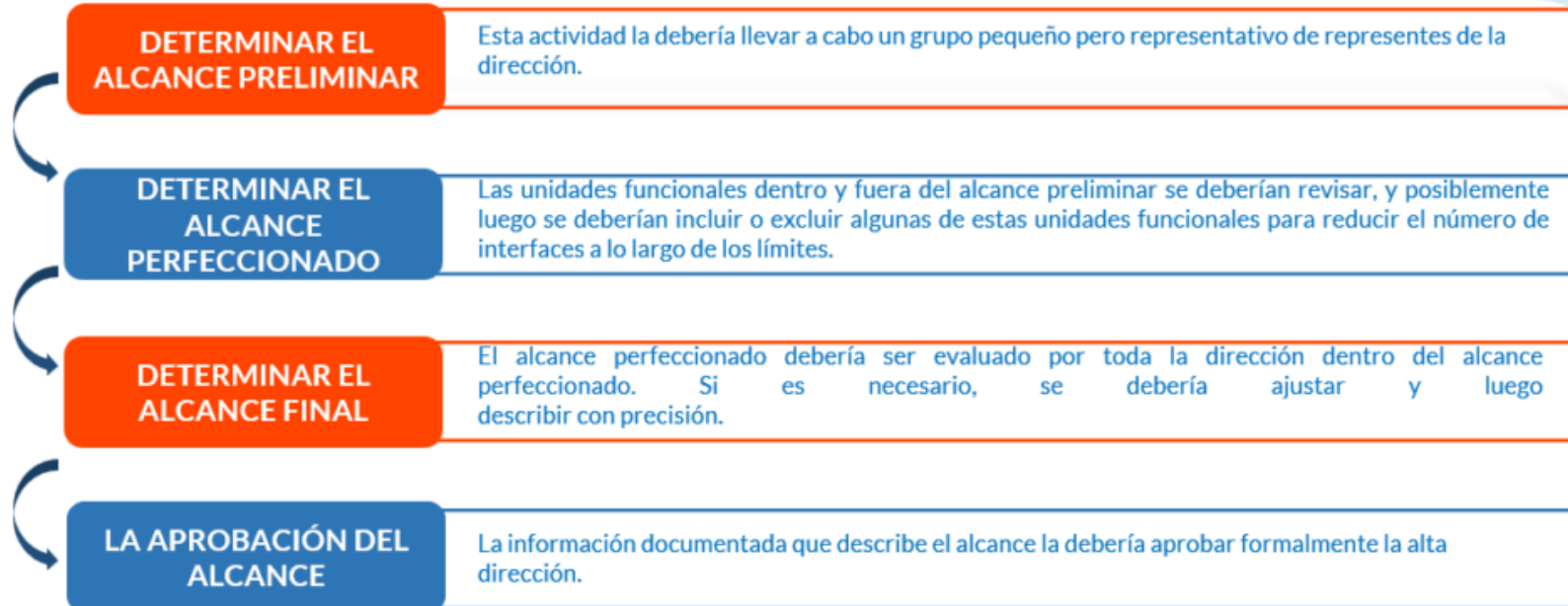
Necesidades y expectativas



PLANIFICACION SGI

2 Definir el alcance SGSI

Para establecer el alcance de un SGSI se puede seguir un enfoque multietapas:





PLANIFICACION SGI

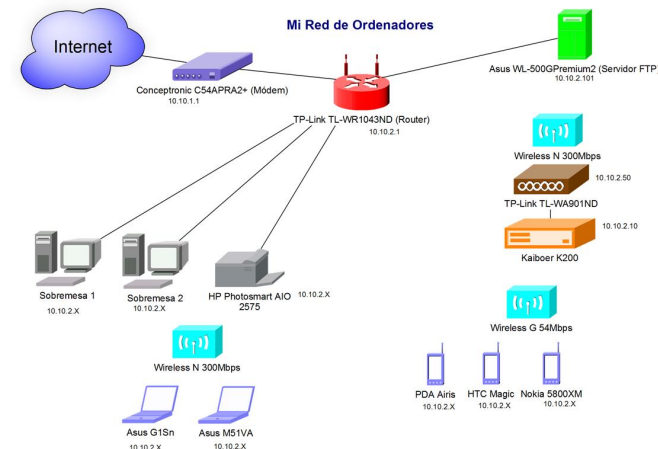
2 Definir el alcance SGI

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los sistemas de información que dan soporte a los procesos del negocio:

Comercialización y configuración de software contable xxx.

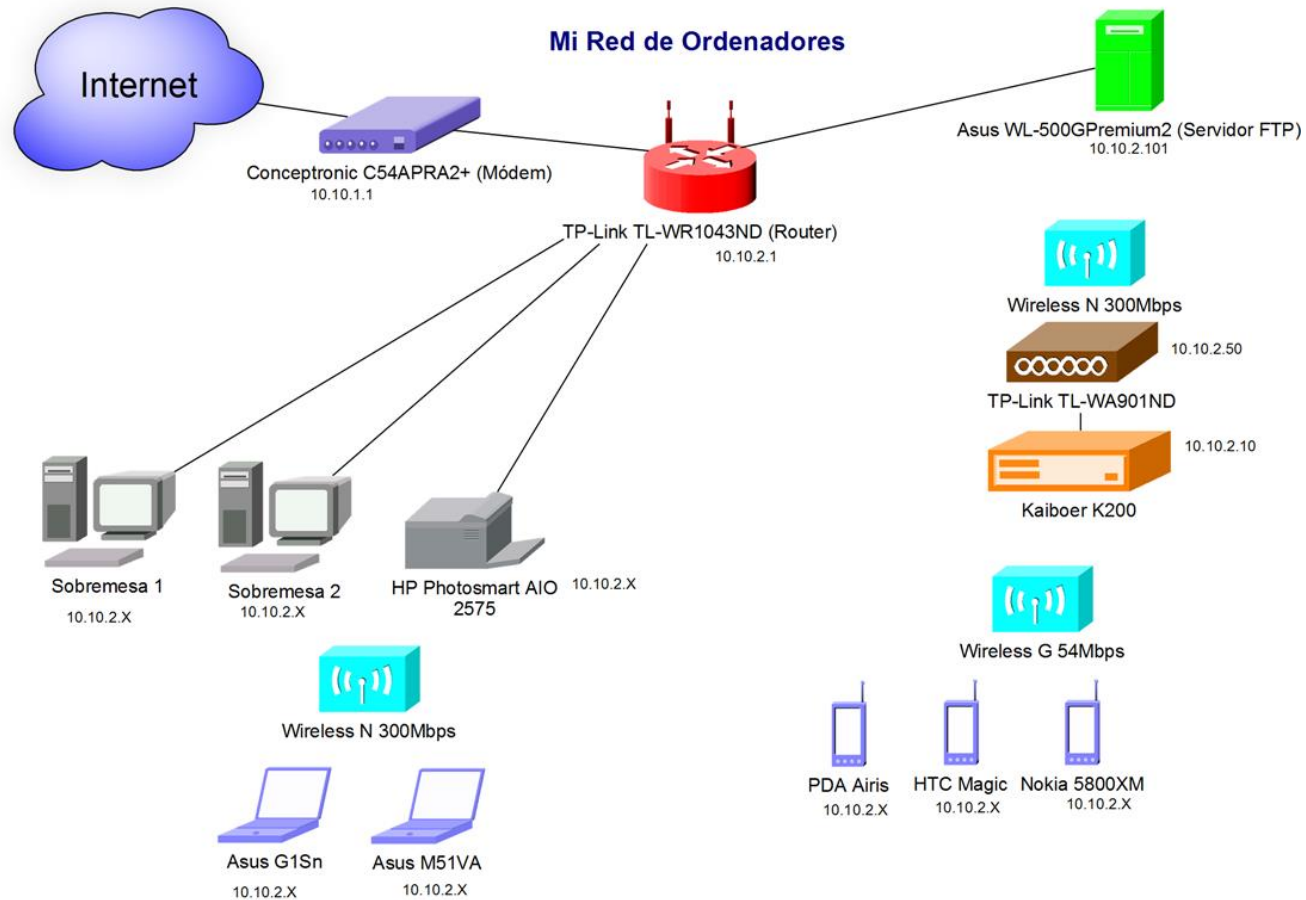
De acuerdo con el documento de aplicabilidad vigente a la fecha de emisión del certificado.





PLANIFICACION SGI

2 Definir el alcance SGI





GESTION DE OBJETIVOS Y PLANIFICACIÓN DE CAMBIOS

3 Establecer Política y Objetivos SGSI

Nube SAC es una empresa especializada en la comercialización de software as a service, nos comprometemos a mantener un Sistema de gestión de seguridad bajo los siguientes pilares:

Compromiso de la dirección: La dirección de la empresa se compromete a proporcionar los recursos necesarios para implementar y mantener esta política.

Responsabilidad: Cada empleado es responsable de proteger la información de la empresa.

Cumplimiento de requisitos aplicables: La empresa cumplirá con todas las leyes, regulaciones y requisitos del cliente en materia de seguridad de la información.

Mejora continua: El SGSI se evaluará y mejorará continuamente.

Objetivos de la ISO 27001





GESTION DE LA COMUNICACIÓN Y DOCUMENTACION

PLAN DE COMUNICACIÓN ISO 27001

La norma **ISO 27001** incluye requisitos en relación a la comunicación de la política de seguridad en una empresa. Se nos pide dar una respuesta a:

- 👉 Quien debe comunicar los aspectos de seguridad
- 👉 A quienes debe llegar la comunicación
- 👉Cuál es el contenido
- 👉 En qué momento ha de realizarse la comunicación
- 👉 Que medios utilizaremos

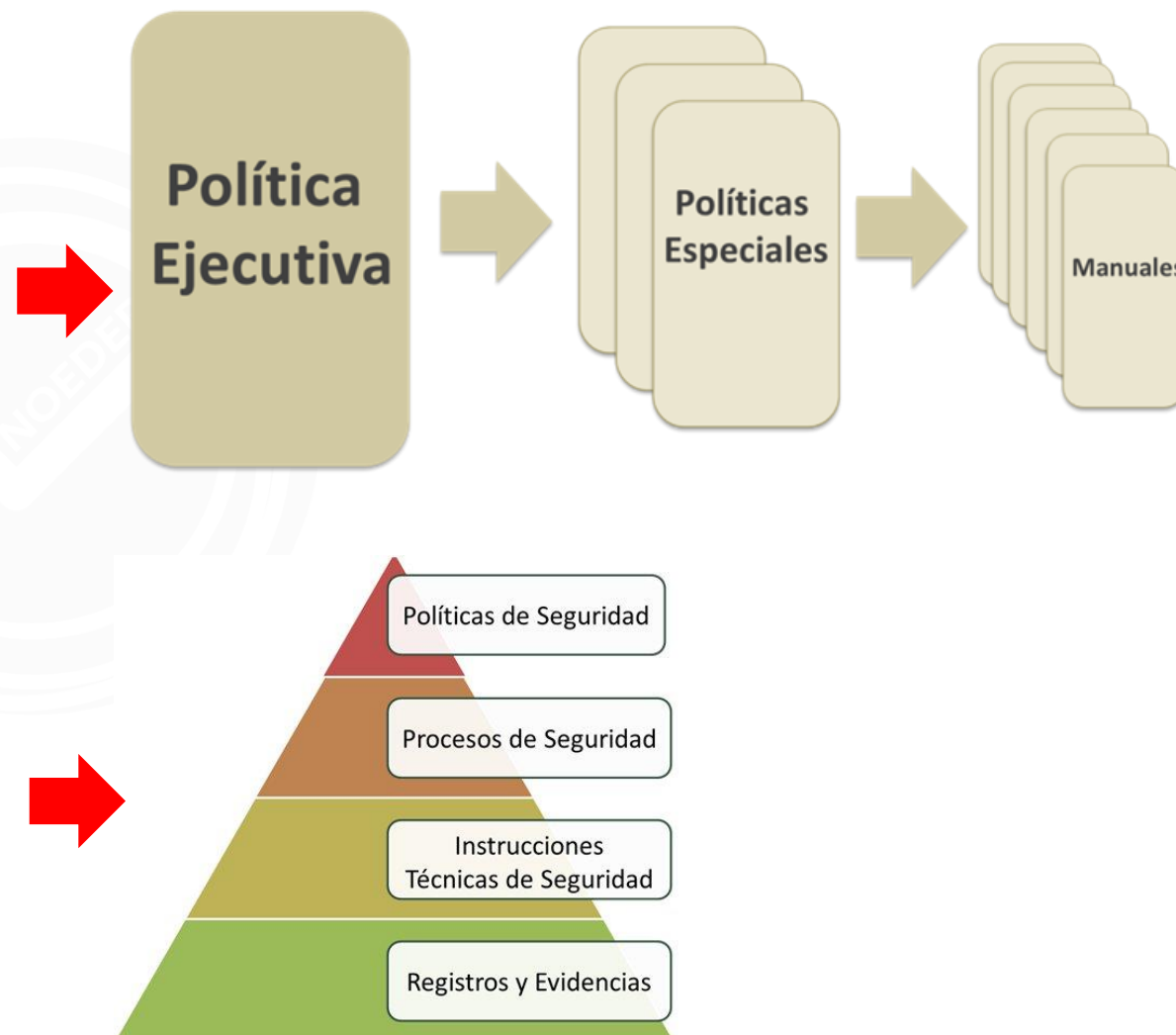
¿QUÉ INFORMACIÓN DEBE PUBLICARSE?

La información oficial del sistema SGI debería estar disponible para el personal que tenga derecho a su consulta.

En cuanto al medio de publicación no tenemos ningún requisito específico en la norma sin embargo, resulta conveniente que se publique en soportes electrónicos y que faciliten su difusión tales como intranet o en entornos de red compartidos

Los requisitos de la norma ISO 27001 en este caso nos piden que la documentación:

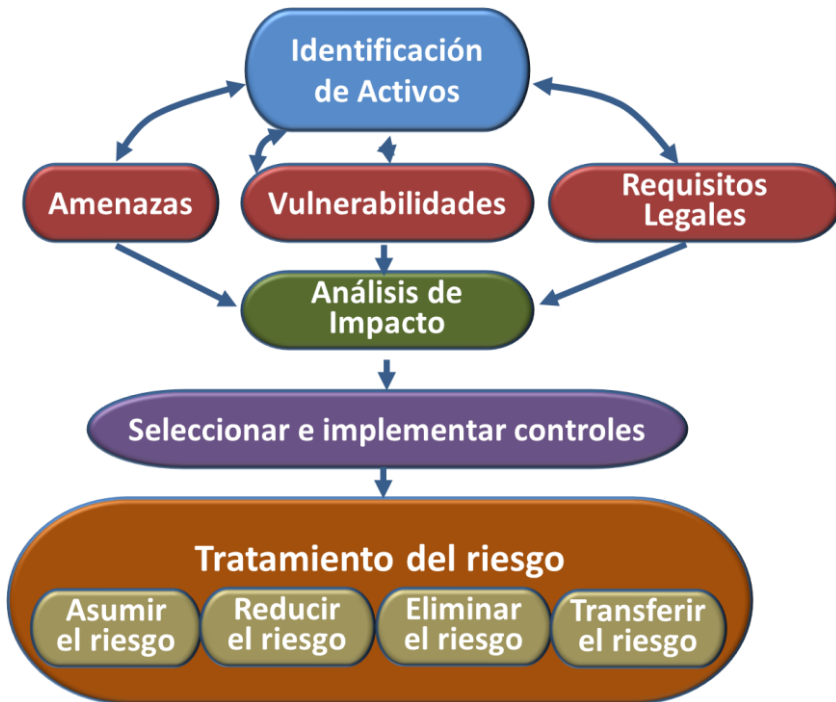
- 👉 Este completa
- 👉 Se encuentre actualizada
- 👉 Se realice un control de la documentación. Para ello lo más conveniente es tener un control mediante codificación que nos informe de la versión actualizada del documento y de las últimas modificaciones





GESTION DE OPERACIONES

6 Control Operacional



SOA

Identifica el control

Define Area responsable

Implementa el control

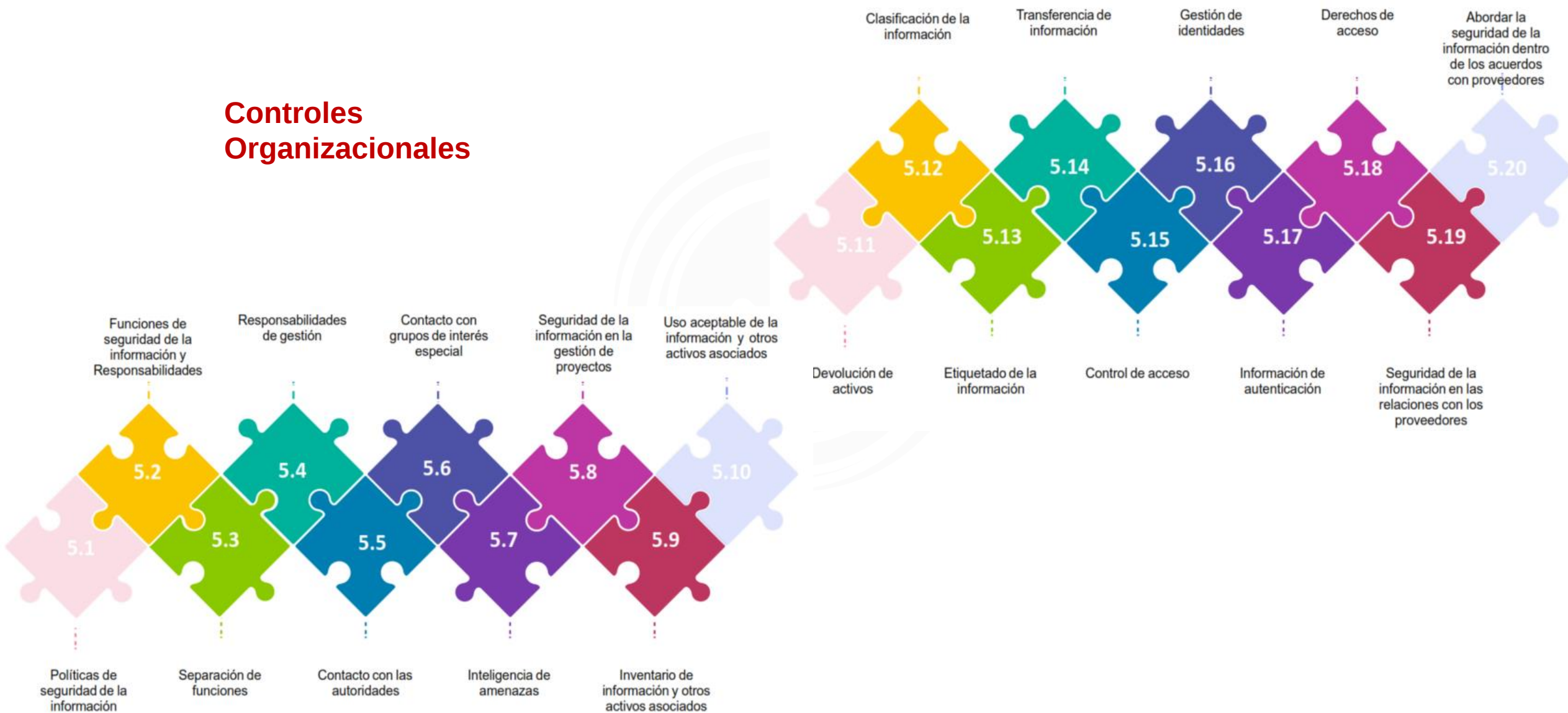
Define Política, Proceso y registros

Establece KPI



GESTION DE OPERACIONES

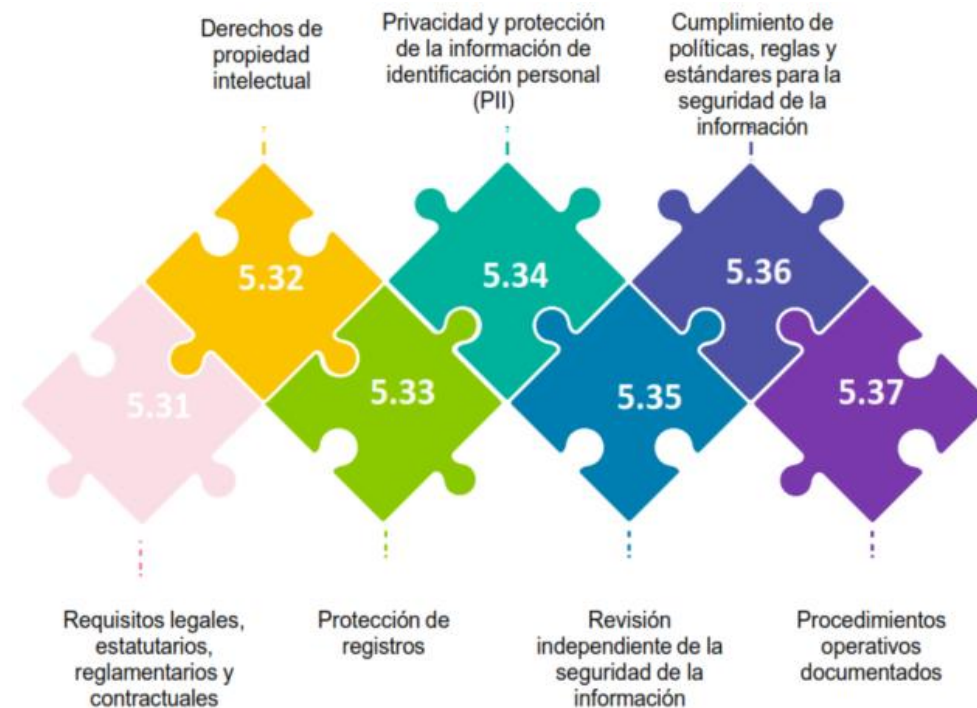
Controles Organizacionales





GESTION DE OPERACIONES

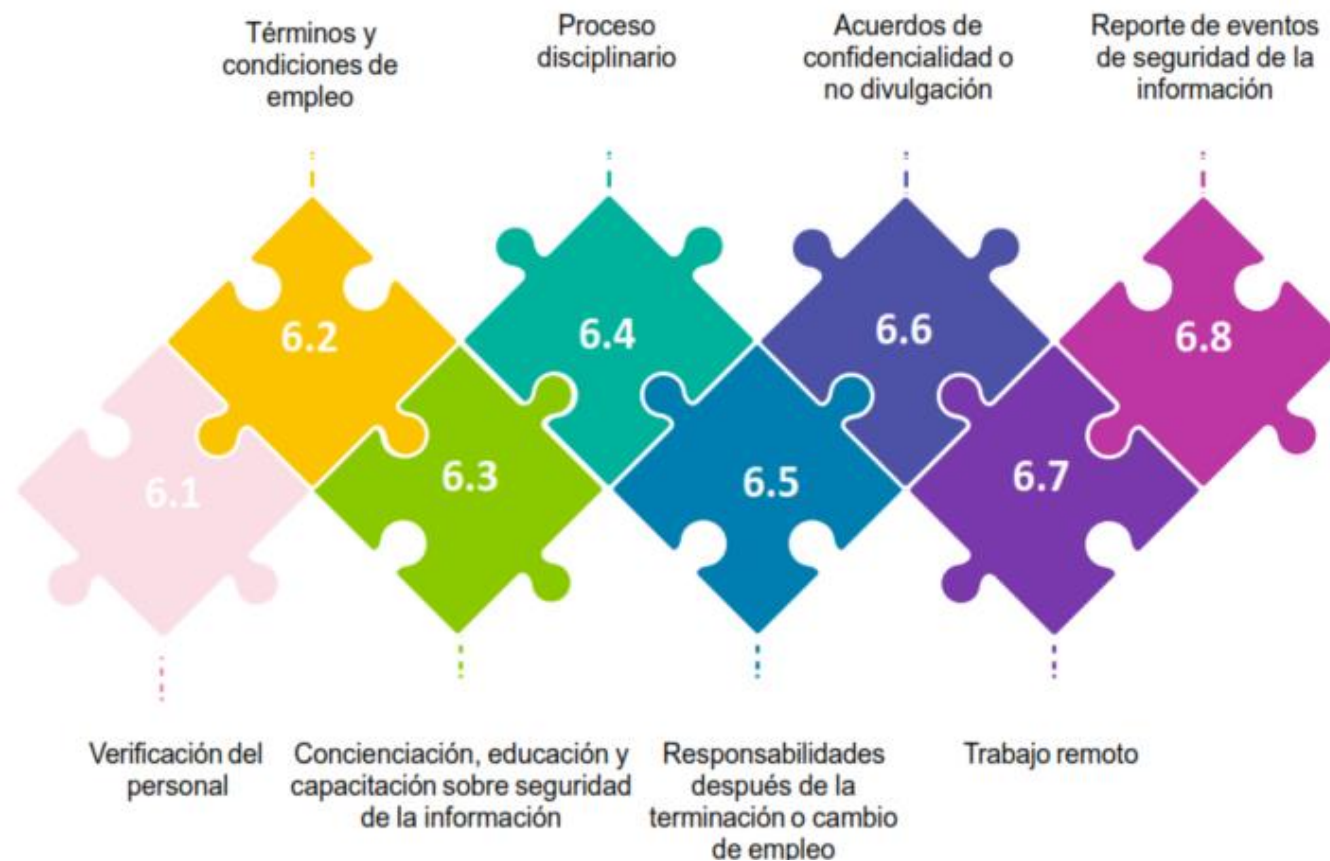
Controles Organizacionales





GESTION DE OPERACIONES

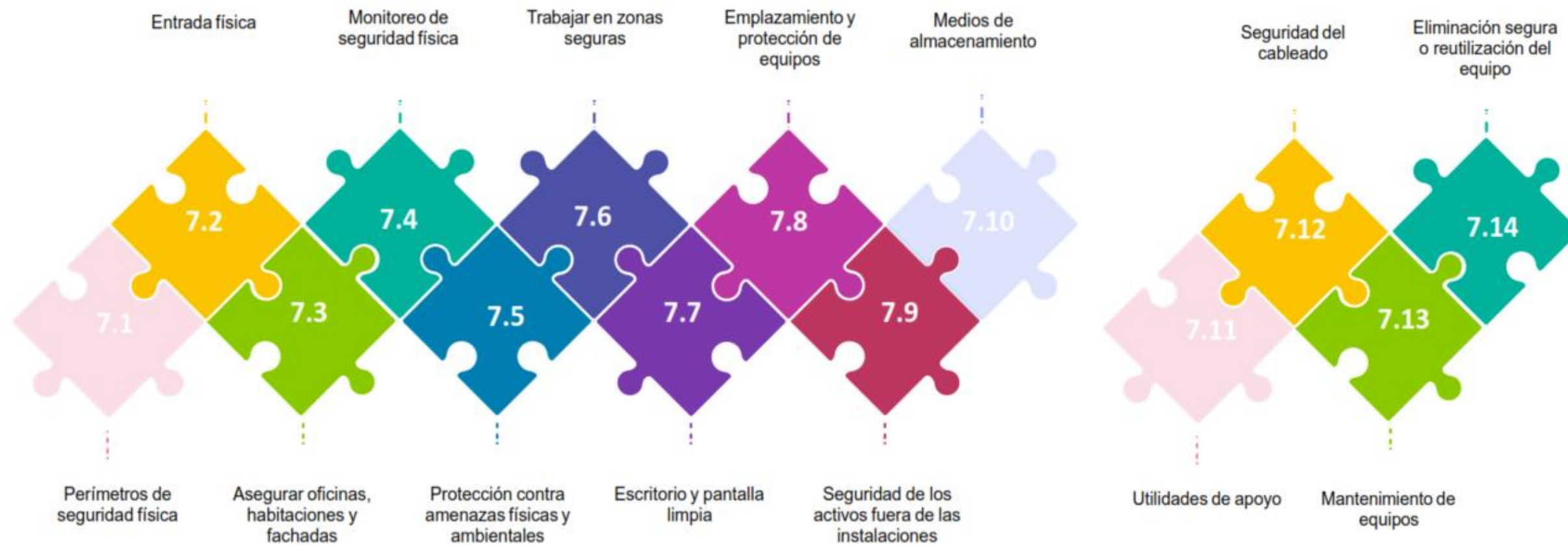
Controles de Personas





GESTION DE OPERACIONES

Controles Físicos





GESTION DE OPERACIONES

Controles Tecnológicos





GESTION DE OPERACIONES

Controles Tecnológicos

Segregación de
redes

Uso de criptografía

Requisitos de
seguridad de las
aplicaciones

Codificación segura

Desarrollo
externalizado

Gestión del cambio

Protección de los
sistemas de información
durante las pruebas de
auditoría

8.22

8.24

8.26

8.28

8.30

8.21

8.23

8.25

8.27

8.29

8.31

8.32

8.34

8.33

Seguridad de los
servicios de red

Filtrado web

Ciclo de vida de
desarrollo seguro

Arquitectura segura
del sistema y
principios de
ingeniería

Pruebas de
seguridad en
desarrollo y
aceptación

Separación de
entornos de
desarrollo, prueba y
producción

Información de
pruebas



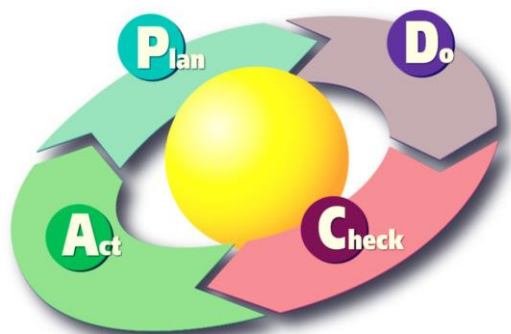
EVALUAR EL DESEMPEÑO

7 Evaluar el desempeño





MEJORA CONTINUA



8 Mejora Continua

- Definir **política de seguridad**
- Establecer **alcance del SGSI**
- Realizar **análisis de riesgos**
- Seleccionar los controles



- Implantar plan de **gestión de riesgos**
- Implantar el SGSI
- Implantar los **controles**
- **Formación y Concienciación**

ISO/IEC 27002 / Anexo A. ISO/IEC 27001



- A5** Política de Seguridad de Información
- A6** Organización de la Seguridad de la Información
- A7** Seguridad en los RRHH
- A8** Gestión de Activos
- A9** Control de Accesos
- A10** Criptografía
- A11** Seguridad física y ambiental
- A12** Seguridad en las operaciones

- A.13** Seguridad en las comunicaciones
- A.14** Adquisición, desarrollo y mantenimiento de sistemas
- A15** Relación con proveedores
- A16** Gestión de incidentes de seguridad
- A17** Aspectos de Seguridad de la información dentro de continuidad de negocio
- A18** Conformidad



- Adoptar las **acciones correctivas**
- Adoptar las acciones preventivas



- Revisar internamente el SGSI
- Realizar **auditorías internas** del SGSI
- Indicadores y Métricas
- Revisión por Dirección

¡Gracias!



Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad

