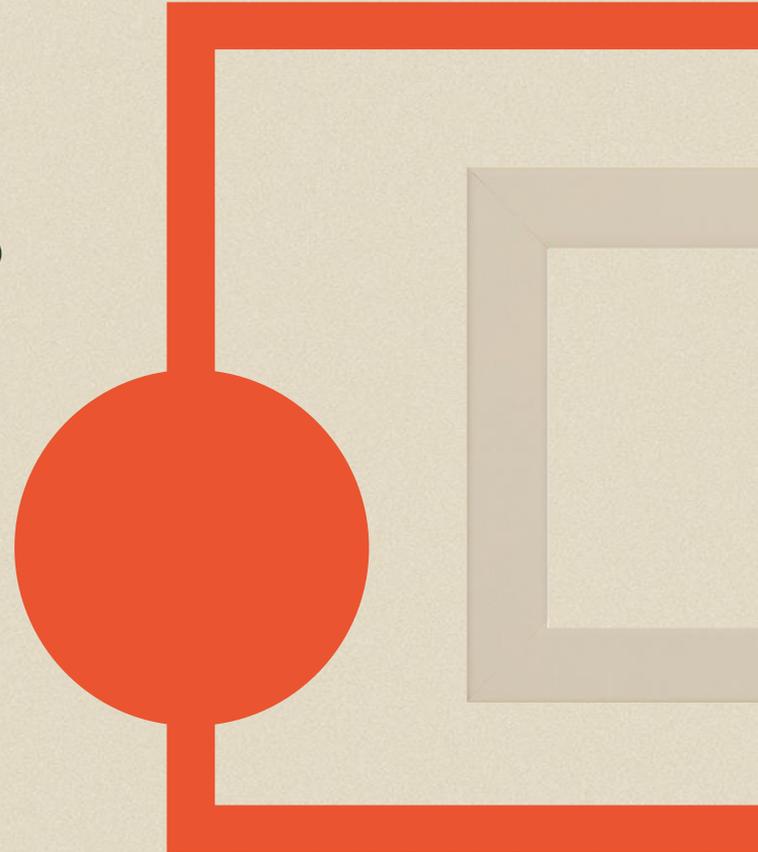


IMPLANTACIÓN DEL EGSÍ DE LA VERSION 2 DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE.

Patricio Narváez
Dangely Rosero



01

Contextualización

02

Objetivos

03

Metodología

04

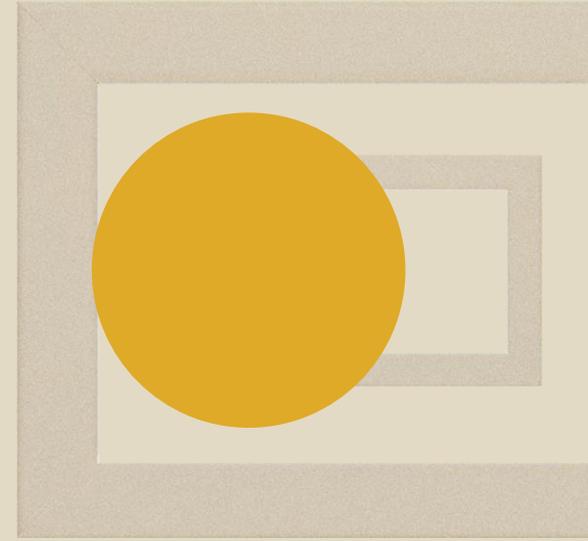
Resultados

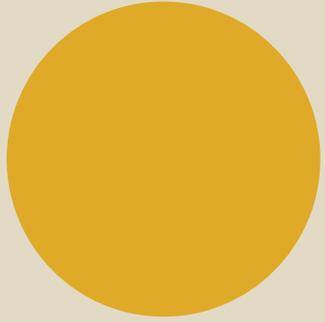
05

Beneficios

06

Conclusiones





01

Contextualización



Justificación e importancia



Situación actual

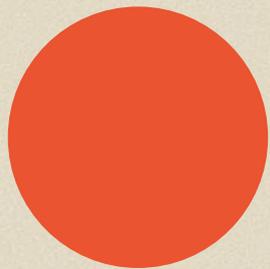
La seguridad de la información es un aspecto crítico para cualquier organización



Leyes Ecuatorianas

Acuerdo Ministerial 2019-025 del MINTEL





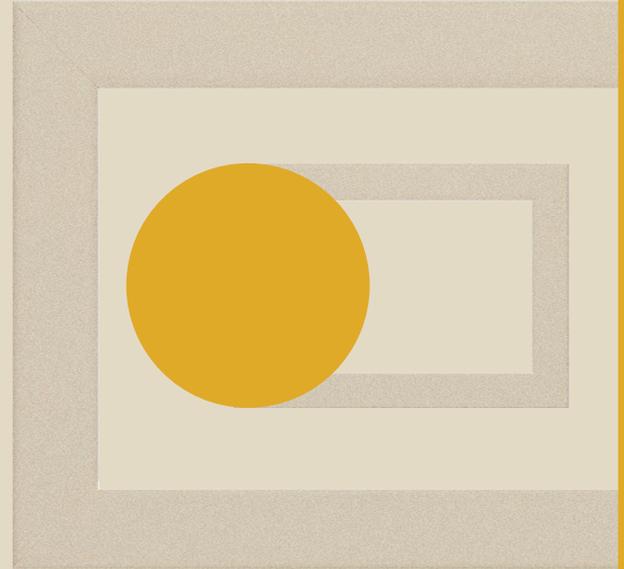
02

OBJETIVOS



Objetivo general

Realizar la Implantación de controles de la Versión 2 del EGSI de la Universidad de las Fuerzas Armadas ESPE, en base de las normas ISO 27001, ISO 27002, ISO 27003.



Objetivos específicos

ESTADO DEL ARTE

Establecer el estado de arte

IMPLANTACIÓN DE CONTROLES

Implementar los controles y salvaguardas del SGSI-ESPE Versión 2, en base del plan de Implementación.

01

02

03

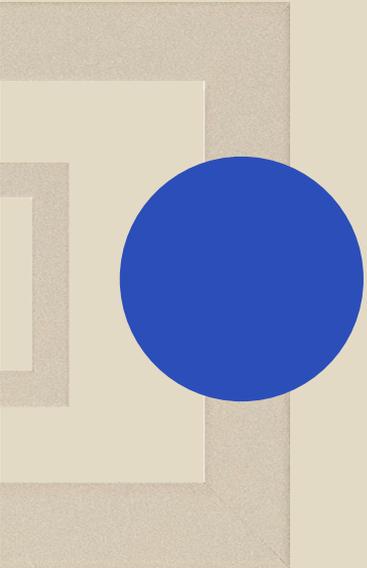
04

PLAN DE IMPLANTACIÓN

Elaborar el Plan detallado de implementación de controles y salvaguardas de la Versión 2 del EGSI de la ESPE

EVALUACIÓN

Evaluar la Implantación de controles y salvaguardas.



03

Metodología

METODOLOGÍA



Preparación y planificación

Se define el alcance del SGSI y se establecen objetivos.



Validación

Realizar revisiones y ajustes según las necesidades de la Universidad de las Fuerzas Armadas.



Selección de controles

Selección de controles adecuados, siguiendo los requerimientos de la Universidad de las Fuerzas Armadas.



Monitorización y evaluación

Realizar revisiones técnicas para evaluar el cumplimiento de los controles.



Diseño e Implementación

Generar los procedimientos y políticas necesarias para cada control seleccionado



Mejora continua

Realizar revisiones para considerar cambios necesarios dentro del sistema de la seguridad de la información.

Marco Legal



Constitución de la República del Ecuador (2008):

- Eliminación de activos
- Reporte de eventos
- Reporte de puntos débiles
- Recolección de evidencias



Ley Orgánica de Telecomunicaciones (2019):

- Asegurar los servicios de aplicaciones en redes públicas



Ley Orgánica de Comunicación

- Reporte de eventos
- Reporte de puntos débiles



Ley Orgánica de Datos Personales (2018):

- Eliminación de activos
- Reporte de eventos
- Recolección de evidencias
- Reporte de puntos débiles
- Evaluación y decisión sobre eventos de seguridad

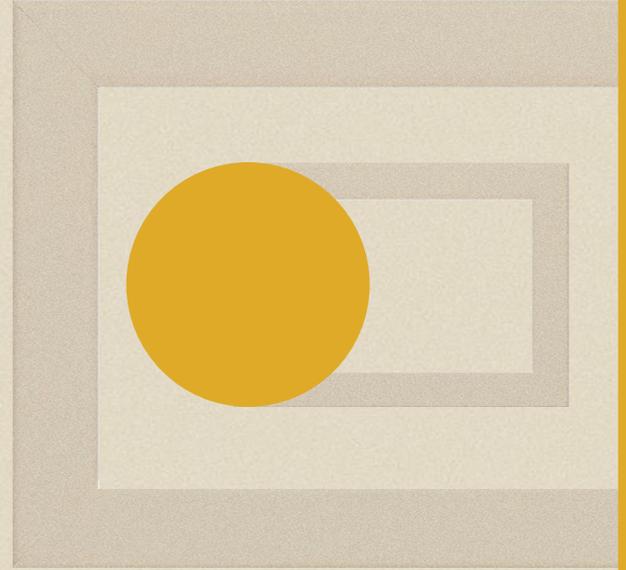


Ley Orgánica de Transparencia y Acceso a la Información Pública

- Eliminación de activos

04

Resultados



Entregables

EGSI

Controles

Formato de controles



Bitácoras

Formato de bitácoras



Reportes técnicos

Observaciones y consejos



Ejemplo de procedimiento

Actividad	Tarea/Descripción	Responsable	Información documentada
Identificación de activo a eliminar	El Propietario del Activo identificará los activos que han alcanzado el final de su ciclo de vida útil	Solicitante/ Propietario	Matriz de inventario
Evaluación y clasificación de activo	Se realizará una evaluación de los activos identificados para determinar su clasificación y la necesidad de implementar medidas especiales de eliminación	Comité de cambios	Resultados de evaluación



Estructura de bitácora

FECHA	Momento de registro de actividad
RESPONSABLE	Encargado de la eliminación
ACTIVO A ELIMINAR	Activo a ser eliminado
NÚMERO DE ACTIVO	Identificación única del activo.
MOTIVO DE ELIMINACIÓN	Razón para la eliminación del activo
DESCRIPCIÓN DE LA EVIDENCIA	Detalle de respaldo para la eliminación



Reporte técnico



Observación

Comentario o nota relevante.



Criterio

Estándar o requisito específico.



Condición

Estado o situación actual.



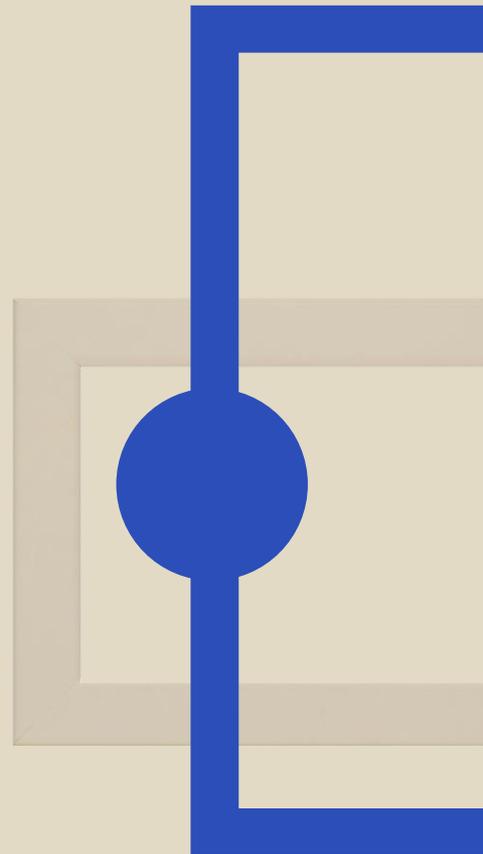
Efecto

Resultados o consecuencias posibles.



Recomendación

Sugerencia o consejo a seguir.



Análisis de impacto



Mejora en la Seguridad de la Información

Fortaleciendo la confianza en la protección de los activos de información.



Eficiencia Operativa Reforzada

Coordinación mejor en la gestión de la seguridad de la información.



Mayor cumplimiento Legal y Normativo

La implementación de controles específicos otorga las bases para un mayor cumplimiento legal y normativo en el futuro.



Protección de Datos Personales Mejorada

Con los controles implantados se ha reforzado la capacidad de proteger los datos personales de estudiantes y el personal.



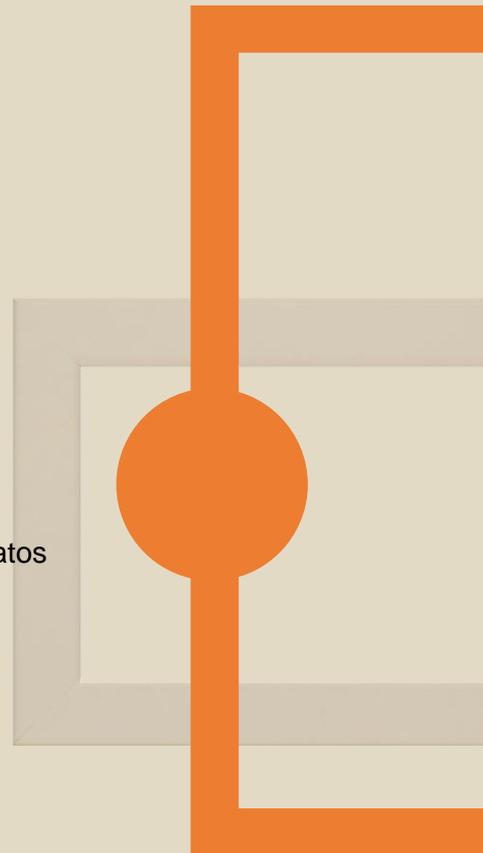
Mayor conciencia de Seguridad

Mayor compromiso con la seguridad de la información.



Imagen institucional reforzada

Demuestra un entorno más seguro y confiable.

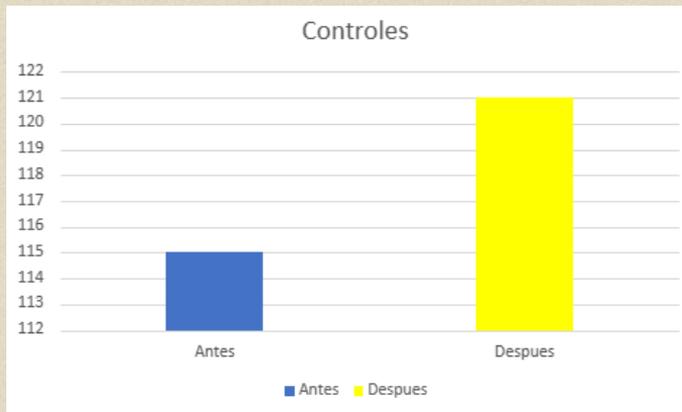


COMPARACIÓN

	VERSION INICIAL	ESTADO ACTUAL
Controles	115 Controles	121 Controles
Bitácoras	Sin formato de bitácoras de registro	Template de bitácoras
Revisión técnica	No contaba con una revisión periódica de controles	Se encuentra un informe detallado con las mejoras y la situación actual.

Controles implantados

Total de controles



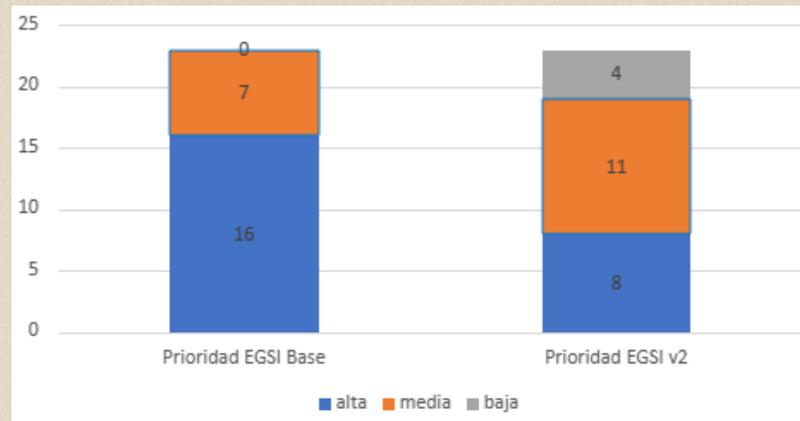
115

Version original

121

Version actual

Nivel de relevancia



50%

Altas

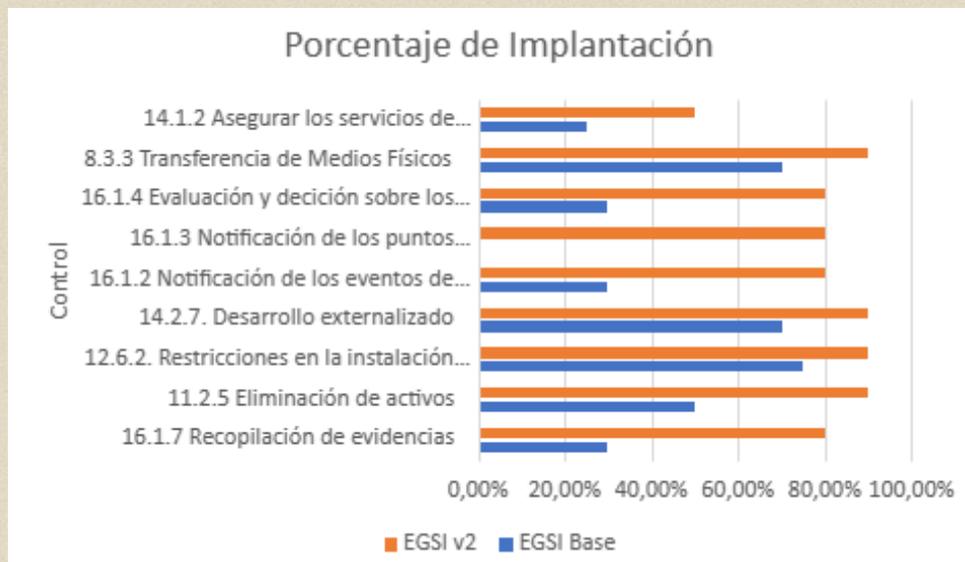
11

Medio

4

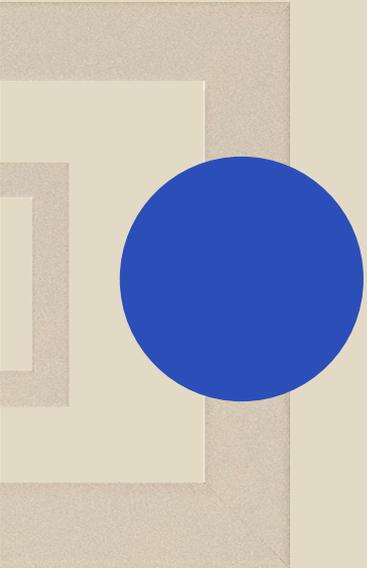
Bajo

Porcentaje de implantación



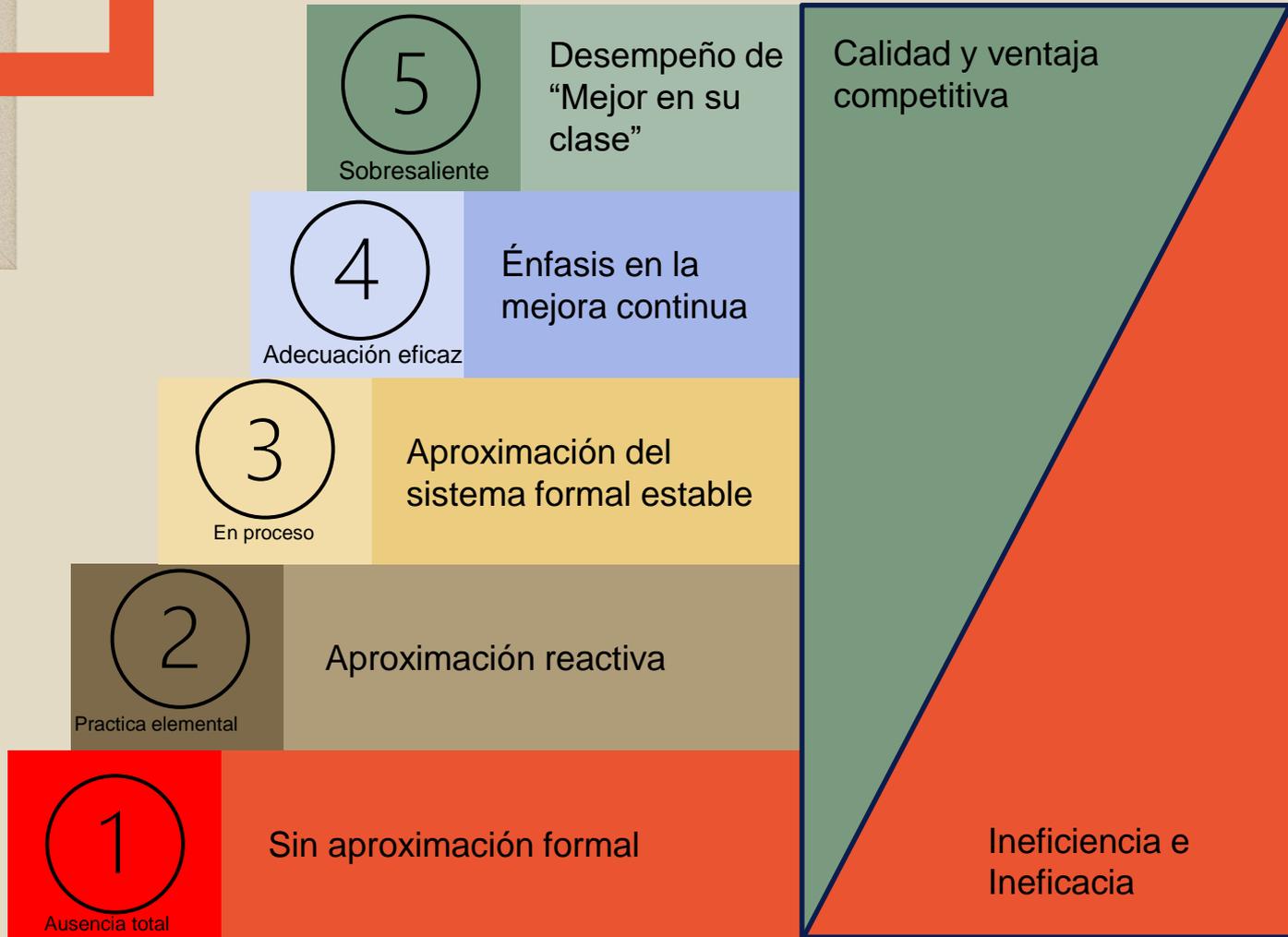
30% - 90%

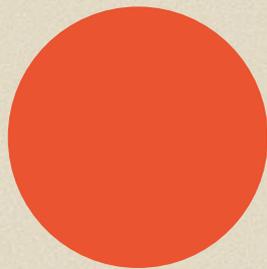
Aumento



05

Beneficios





06

**Conclusiones y
Recomendaciones**



Conclusiones

01

Elaboración del estado del arte

Permitió comprender precisamente el contexto y los retos que conlleva la implantación de controles.



02

Plan de implantación

En base al plan desarrollado se pudo definir tareas, responsables, tiempos y activos a tratar.



03

Implantación de controles

Mediante las tareas definidas previamente se logro implantar los controles satisfactoriamente.



04

Evaluación de controles

Gracias a la evaluación se determinó la línea base y el nivel de madurez que otorgo este proyecto a la institución



Recomendaciones



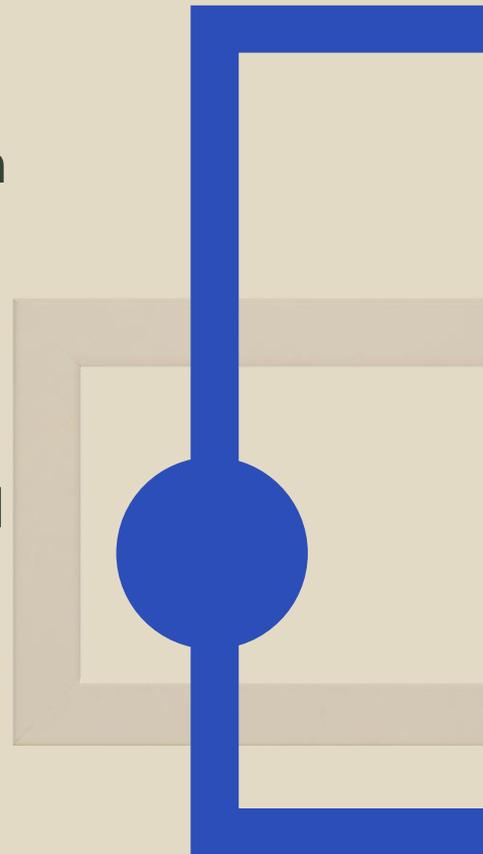
Políticas de revisión y actualización periódicas



Evaluación de eficiencia y eficacia



Fomentar la cultura de la seguridad de la información



Gracias

