SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

1.4.2. Capítulo 4 - Parte 2

Plan de implantación de seguridad

JOSÉ PABLO HERNÁNDEZ

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA

Criterios de selección de:

- **MAGERIT**
- **ISO27002**
- **Otras referencias**

3.1. SELECCIÓN DE CONTROLES EN MAGERIT

En MAGERIT, la aplicación de contramedidas es un proceso ordenado, que resumidamente consiste en:

1. **Determinar responsables**
2. **Establecer objetivos para saber que la amenaza ha sido tratada**
3. **Dar procedimientos paso a paso de cómo ejecutar la contramedida**
4. **Ejecutar la contramedida.**
5. **Evaluar si todo está funcionando según lo previsto.**

MAGERIT define un criterio general, y un criterio basado en pérdidas y ganancias.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO GENERAL DE SELECCIÓN.

Prioritariamente, deben elegirse controles preventivos (que buscan impedir incidentes o ataques).

Pero en la práctica, no todo es previsible, ni resultará económicamente razonable…

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO GENERAL DE SELECCIÓN.

…por lo que:

Es necesario disponer de elementos que detecten el inicio del incidente lo antes posible: estos son los controles de:

- **Detección (que buscan reaccionar con presteza para dar la alarma).**
- **Seguidamente, intervendrían las medidas de emergencia (que buscan parar y limitar el incidente).**
- **Y por último, las medidas de recuperación (que buscan regresar a donde se debe estar).**

Y …

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO GENERAL DE SELECCIÓN.

…Buscando un equilibrio entre las contramedidas:

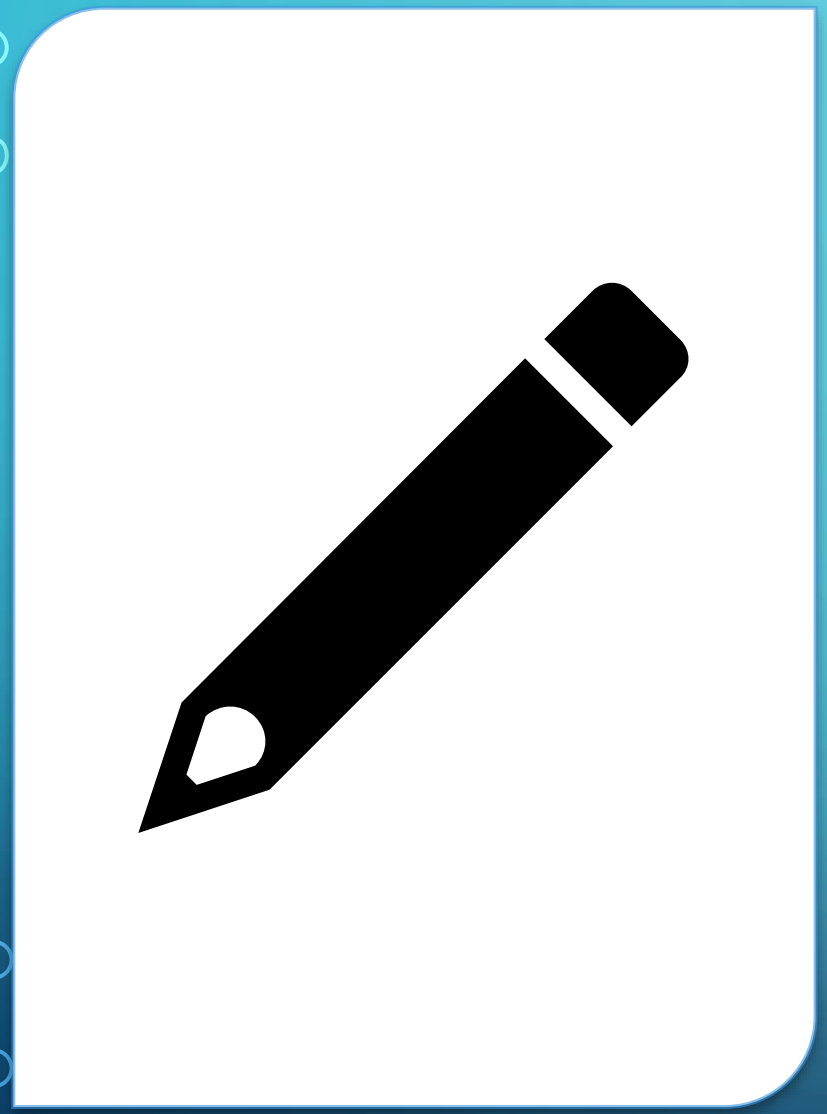
- **Técnicas (usadas en aplicaciones, equipos, y comunicaciones**
- **Físicas (protección del entorno, de las personas, y de los equipos**
- **Organizativas (de prevención y gestión de incidencias**
- **Política de personal (que es el eslabón más delicado: política de contratación, formación permanente, reporte de incidencias, plan de reacción, y medidas disciplinarias).**

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO GENERAL DE SELECCIÓN.

Es importante elegir las contramedidas más fáciles de usar.

El caso ideal lo constituyen las contramedidas "transparentes", en las que el usuario no debe hacer nada, o en su defecto, cuanto menos tenga que hacer mejor.

Esto se debe a que una contramedida compleja añade la amenaza de su uso indebido.

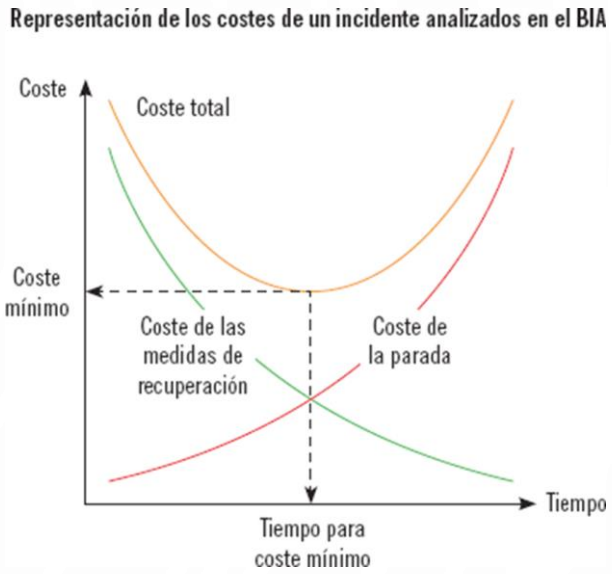


Actividades

CLASIFIQUE, SEGÚN LOS CRITERIOS GENERALES VISTOS, LAS MEDIDAS QUE PODRÍAN REDUCIR EL RIESGO DE EVASIÓN DE INFORMACIÓN POR ROBO DE UN DISCO DURO EXTERNO CONVENCIONAL.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

No aplicar contramedidas que sean más valiosas que aquello que se protege.



Buscar equilibrio entre el coste de las pérdidas por un incidente, y el coste de la ganancia en seguridad que lo evite.

El equilibrio se alcanza cuando ambos costes sean mínimos.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Ganancias: se deben realizar valoraciones del coste de la seguridad o contramedidas, frente al nivel de protección que logran (lo que resulta difícil de cuantificar, como se vio en el capítulo anterior). Existen en general tendencias crecientes y exponenciales (que reflejan que inicialmente se logra mucha seguridad con poca inversión, y que posteriormente, incluso pequeños incrementos de la seguridad son cada vez más caros).

Pérdidas: el coste de la inseguridad o riesgo, decrece exponencialmente (reflejando que el riesgo desciende inicialmente muy rápido con pequeñas medidas, para posteriormente precisar muchas medidas para reducirlo un poco).

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

En la práctica, se estudia el coste frente al tiempo (por ejemplo, para 5 años), y para diversos escenarios (E0, E1,... En), en los que se aplican un conjunto de contramedidas de las que se evalúa su coste anual:

- **E0: situación en la que no se aplica ninguna contramedida.**
- **E1: situación en la que se aplica un conjunto de contramedidas C1.**
- **...**
- **En: situación para un conjunto de contramedidas Cn.**

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Para calcular el coste anual de las contramedidas, se contempla en:

- **positivo** la mejora de productividad de carácter recurrente (que puede ser negativo si la organización pierde productividad, por ejemplo, si se introduce un proceso de clasificación de la información) y la mejora de capacidad de la organización para prestar nuevos servicios, o tener mejores condiciones con los proveedores también de carácter recurrente.

- **Negativo** el riesgo residual, que permanece en el sistema de carácter recurrente, el coste de las contramedidas de carácter puntual, y el coste anual de mantenimiento de carácter recurrente.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Ejemplo: dado el riesgo de un sistema de información **(E0 = 10)**, se estudian **3 posibles conjuntos de contramedidas** y se obtienen los siguientes costes para los primeros **5 años:**

E1 = {-30, -40, -50, -60, -70},

E2 = {-45, -40, -35, -30, -25},

E3 = {-55, -40, -25, -10, 5}.

La representación de estos costes ayuda a interpretar su significado, siendo el caso **óptimo el E3**.

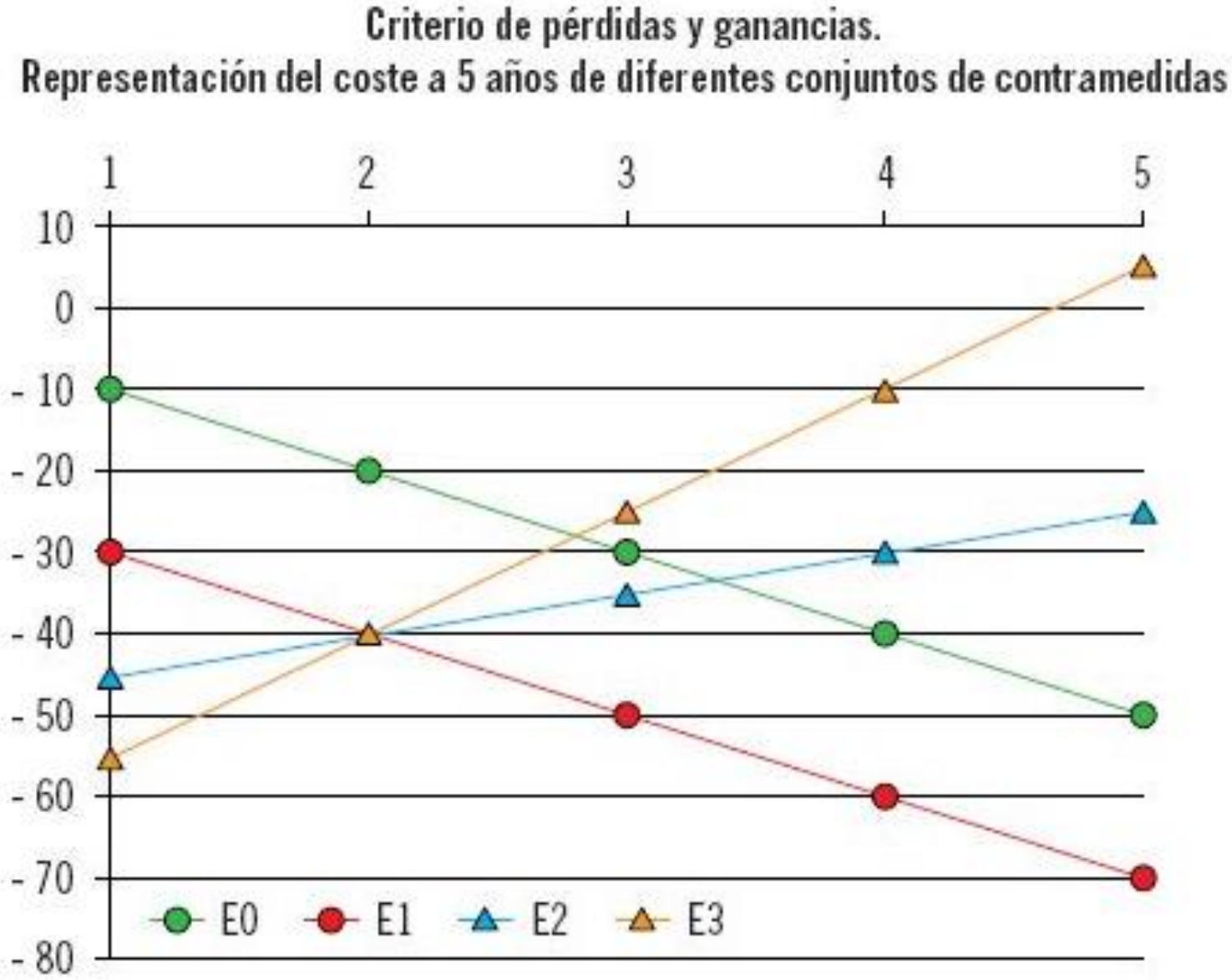
En el escenario E0 (sin contramedidas) el gasto se acumula año tras año en una cantidad igual al riesgo estimado.

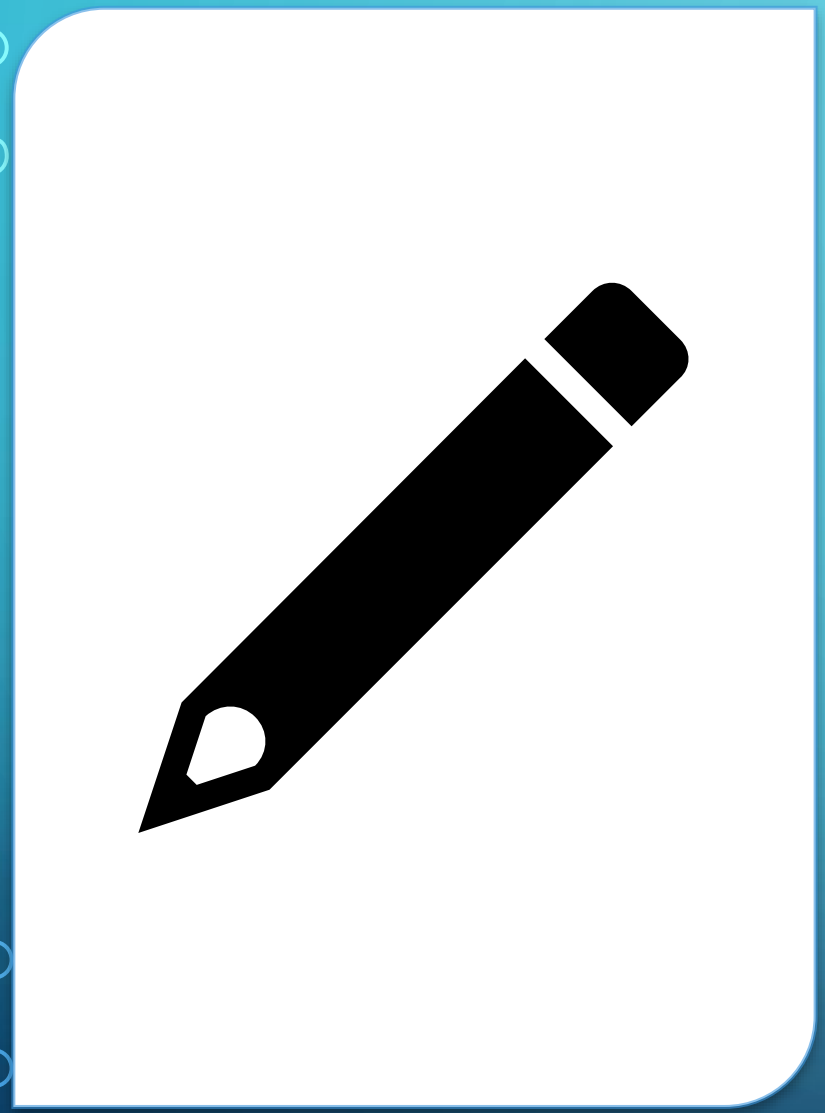
En el escenario E1 hay un desembolso inicial, que no se recupera en los siguientes años.

En el escenario E2, de mayor desembolso inicial, se obtiene rentabilidad (se supera la curva E0) en el año 4.

Por último, en el caso E3, que es el de mayor inversión inicial, se obtiene rentabilidad en el año 3, e incluso se obtienen beneficios operativos en el año 5.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.





Actividades

PARA PROTEGER UN ACTIVO FRENTE A UN RIESGO DE PÉRDIDA ANUAL DE VALOR 50, DETERMINAR SI SE ELEGIRÍA:

UNA MEDIDA A, CUYO COSTE INICIAL ES 100, Y CON UN COSTE DE MANTENIMIENTO ANUAL DE 25,

UNA MEDIDA B, CUYO COSTE INICIAL ES 200, Y QUE, LIBRE DE MANTENIMIENTO, APORTA UN BENEFICIO ANUAL DE 25.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Catálogo de salvaguardas de MAGERIT:

De entre los controles de referencia incluidos en “MAGERIT v2. II-Catálogo de Elementos”, podríamos destacar los de las siguientes diapositivas.

NOTA: En algunas salvaguardas, se indica entre paréntesis la dimensión de la seguridad afectada (C: confidencialidad, I: integridad, D: disponibilidad, A-S: autenticidad en el uso del servicio, A-D: autenticidad en el uso de los datos, T-S: trazabilidad en el uso del servicio, T-D: trazabilidad en el uso de los datos).

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Catálogo de salvaguardas de MAGERIT:

Tipo salvaguarda: TODOS

- Organización de la seguridad: responsables y comités.
- Política corporativa de Seguridad de la Información.
- Gestión de privilegios: adjudicación, revisión y terminación.
- Procedimientos de escalado y gestión de incidencias.
- Procedimientos de continuidad de las operaciones: planes de emergencia y recuperación.
- Auditorías, registros, certificaciones y acreditaciones del sistema.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Catálogo de salvaguardas de MAGERIT:

Tipo salvaguarda: Servicios

- Control del ciclo de vida de los servicios: especificación, desarrollo, despliegue, operación y terminación del servicio.
- Control de los servicios externalizados u outsourcing, mediante cierre de la relación contractual, especificando:
  - acuerdo de nivel de servicio, y si la disponibilidad es un valor;
  - compromiso de secreto, y si la confidencialidad es un valor;
  - identificación y calificación del personal encargado, procedimientos de escalado y resolución de incidencias, procedimiento de terminación y duración en el tiempo de las responsabilidades asumidas, asunción de responsabilidades, y penalizaciones por incumplimiento.
- Controles de acceso (A-S) basados en contraseñas, certificados digitales, y dispositivos o características biométricas.
- Registros de actuaciones (T-S).
- Registros de incidencias (T-S).
- Plan de continuidad (A).

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Catálogo de salvaguardas de MAGERIT:

Tipo salvaguarda: Información

- Organización de la información: documento de seguridad en caso de datos de carácter personal, clasificación de la información, gestión de claves.
- Control de acceso (A-D).
- Firma electrónica (A-D).
- Registro de actuaciones (T-D).
- Registro de incidencias (T-D).
- Copias de respaldo (D).
- Cifrado (C), de carácter preventivo.
- Marcado (C), facilita la persecución.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Catálogo de salvaguardas de MAGERIT:

Tipo salvaguarda: Aplicaciones

- Control del ciclo de vida del SW (software): especificación funcional y no funcional, desarrollo seguro y protección del código fuente, aceptación y puesta en operación, explotación incluida gestión de cambios/ configuración/ incidencias, homologación/ certificación/ acreditación.
- Protección frente a código dañino (I) como virus, troyanos o puertas traseras.
- Control de acceso (A-S, A-D).
- Registro de actuaciones (T-S, T-D).

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Catálogo de salvaguardas de MAGERIT:

Tipo salvaguarda: Equipos

- Control de la seguridad física: inventario, control de entradas y salidas, destrucción, homologación/ certificación/ acreditación.
- Configuración de equipos internos y de equipos que salen de los locales.
- Mantenimiento (I) con protección frente a código dañino y detección de intrusión.
- Registro de intrusiones.
- Gestión de privilegios.
- Control de acceso.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Catálogo de salvaguardas de MAGERIT:

Tipo salvaguarda: Comunicaciones

- Control del ciclo de vida: planificación de la capacidad, adquisición, y mantenimiento, configuración de la segregación de redes de los router y de los cortafuegos, gestión de claves si se emplea cifrado, detección de intrusión con monitorización de uso.
- Plan de continuidad (D).
- Garantías de integridad (I).
- Cifrado (C).
- Control de acceso (A-S).
- Registro de actuaciones (T-S).

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Catálogo de salvaguardas de MAGERIT:

Tipo salvaguarda: Seguridad física

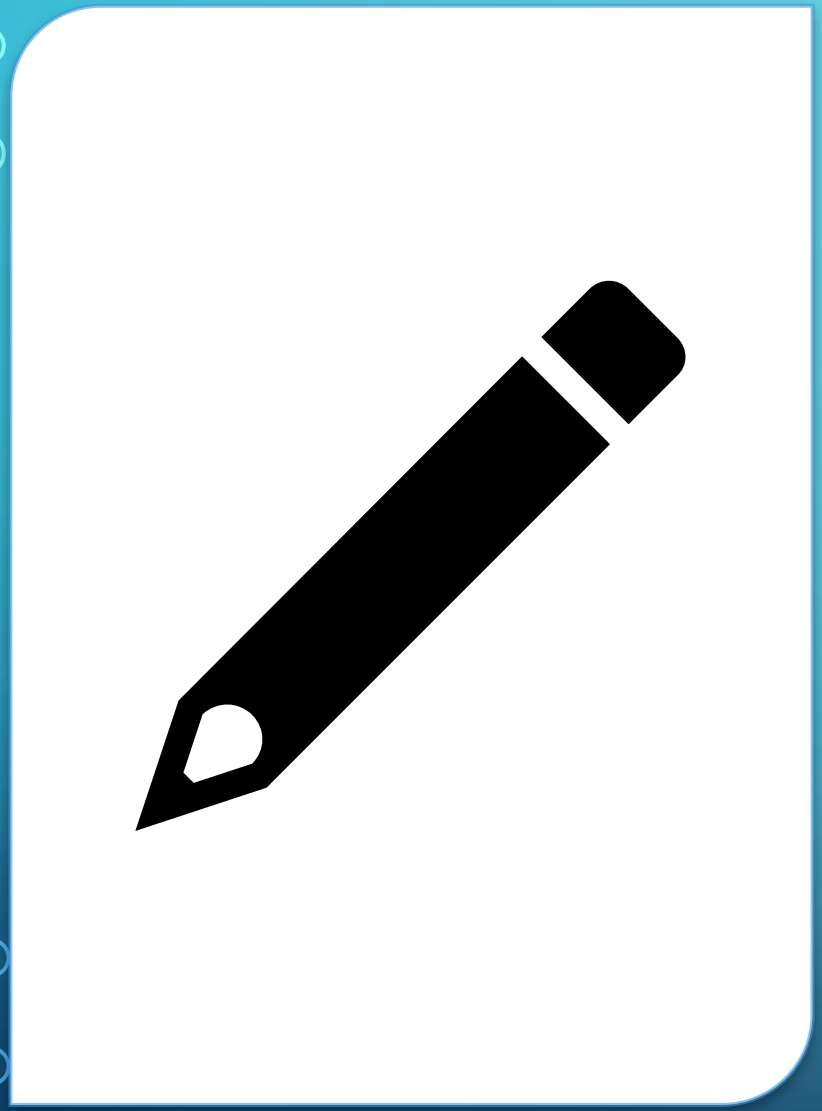
- Protección frente a accidentes naturales (terremotos, riadas, incendios, tormentas, etc.).
- Protección frente a accidentes industriales (incendio, inundación, contaminación mecánica como polvo o vibraciones, contaminación electromagnética).
- Protección frente a emanaciones electromagnéticas.
- Protección del recinto (edificios, locales, y áreas de trabajo) con un mínimo anuncio de la actividad que se realiza, mediante barreras físicas, y mediante protección del cableado.
- Control de acceso de las entradas/ salidas de personas/ equipos/ soportes de información.

3.1. SELECCIÓN DE CONTROLES EN MAGERIT. CRITERIO DE PÉRDIDAS Y GANANCIAS.

Catálogo de salvaguardas de MAGERIT:

Tipo salvaguarda: Personal

- Control del ciclo de vida del personal: especificación del puesto de trabajo, selección del personal, condiciones contractuales (como la responsabilidad en seguridad de la información), y formación continua.



Actividades

REVISE LAS SALVAGUARDAS DE MAGERIT, Y CLASIFIQUE, SEGÚN LOS CRITERIOS GENERALES VISTOS, LAS MEDIDAS QUE PODRÍAN REDUCIR EL RIESGO DE EVASIÓN DE INFORMACIÓN POR ROBO DE UN DISCO DURO EXTERNO CONVENCIONAL.

3.2. SELECCIÓN DE CONTROLES EN ISO17799: 2005, ISO 27002

El Apartado 4.2 de la norma ISO 17799 especifica que los controles deben asegurar que se reduzcan los riesgos a un nivel aceptable, según:

- **Los requerimientos y restricciones de la legislación y regulaciones nacionales e internacionales.**
- **Los objetivos organizacionales.**
- **Los requerimientos y restricciones operacionales.**
- **El coste de implementación y operación en relación a los riesgos que se están reduciendo manteniéndolo proporcional a los requisitos de la empresa.**
- **La necesidad de equilibrar la inversión en implementación y operación de las contramedidas, con el daño probable resultado de las amenazas.**

3.2. SELECCIÓN DE CONTROLES EN ISO17799: 2005, ISO 27002

Como en otras normas y metodologías, se emplea el concepto de "línea base de seguridad", que en ISO 17799 se denomina punto de inicio de la seguridad de la información.

Estos son unos principios guías, aplicables a la mayoría de las organizaciones, y a su implementación se le otorga la consideración de controles esenciales y de práctica común para la seguridad de la información.

3.2. SELECCIÓN DE CONTROLES EN ISO17799: 2005, ISO 27002

Controles ESENCIALES, perspectiva legislativa	Protección de datos y privacidad de la información (15.1.4)
	Protección de los registros de la empresa (15.1.3)
	Derechos de propiedad intelectual (15.1.2)
Controles PRÁCTICA COMÚN	Documento de Política de Seguridad de la Información (5.1.1)
	Asignación de responsabilidades de la Seguridad de la Información (6.1.3)
	Conocimiento, educación y capacitación en Seguridad de la Información (8.2.2)
	Procesamiento correcto de las aplicaciones (12.2)
	Gestión de la vulnerabilidad técnica (12.6)
	Gestión de la continuidad comercial (14.1)
	Gestión de los incidentes y mejoras de la Seguridad de la Información (13.2)

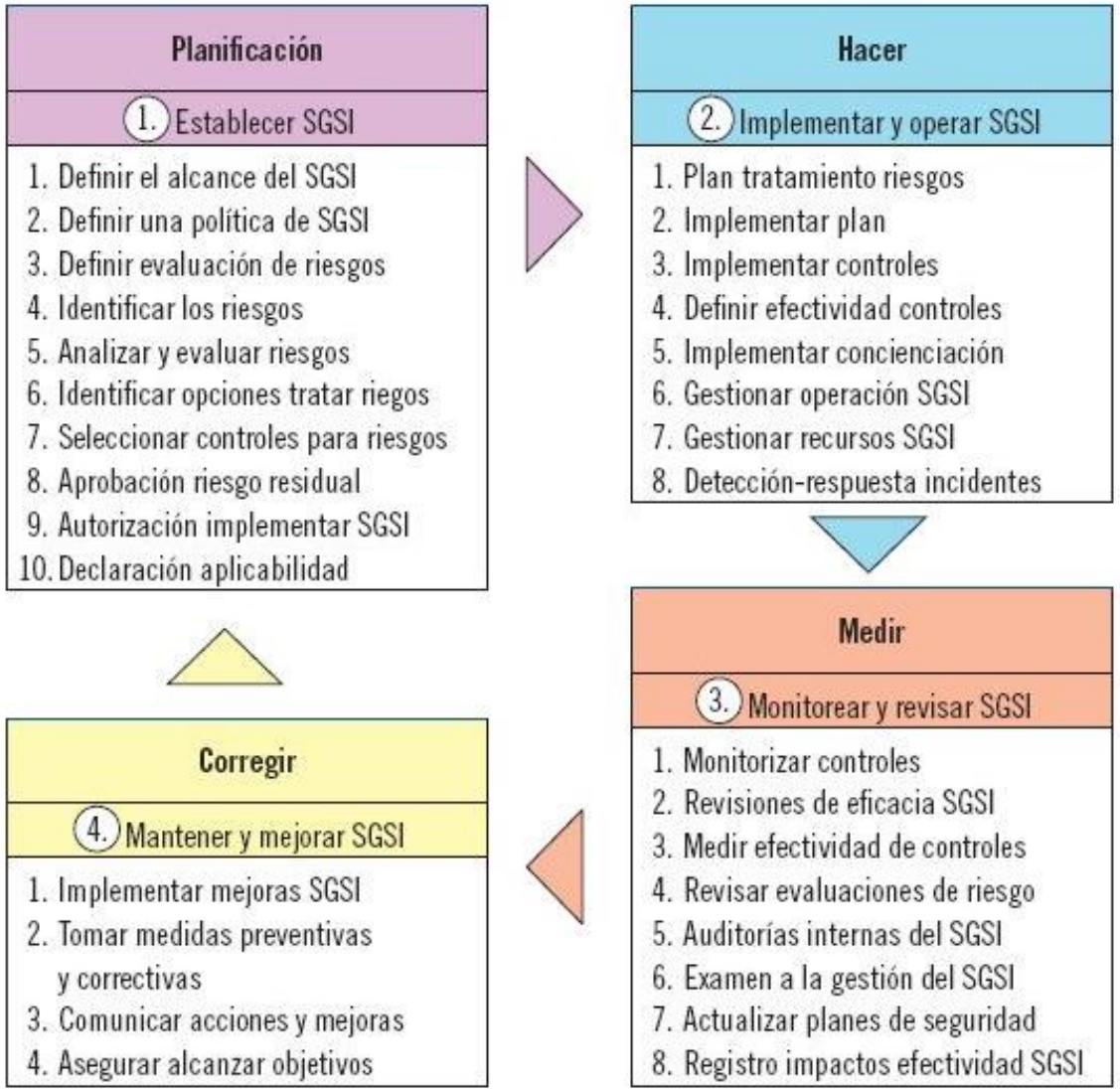
3.2. SELECCIÓN DE CONTROLES EN ISO17799: 2005, ISO 27002

La norma ISO 27001 marca que debe existir un documento que proporcione un resumen de las decisiones referentes a la selección de salvaguardas y tratamiento del riesgo. Este documento se denomina declaración de aplicabilidad, y debe incluir al menos lo siguiente:

- Controles seleccionados. Incluir los objetivos de control y los controles seleccionados, así como los motivos para seleccionarlos.
- Controles existentes. Incluir los objetivos de control y los controles actualmente implementados.
- Controles excluidos. Se deben enumerar expresamente los objetivos de control y los controles, excluidos de los propuestos en el anexo A de la norma ISO27001 (es decir, los recomendados por la norma ISO27002 e ISO17799: 2005), justificando por qué se excluyen.

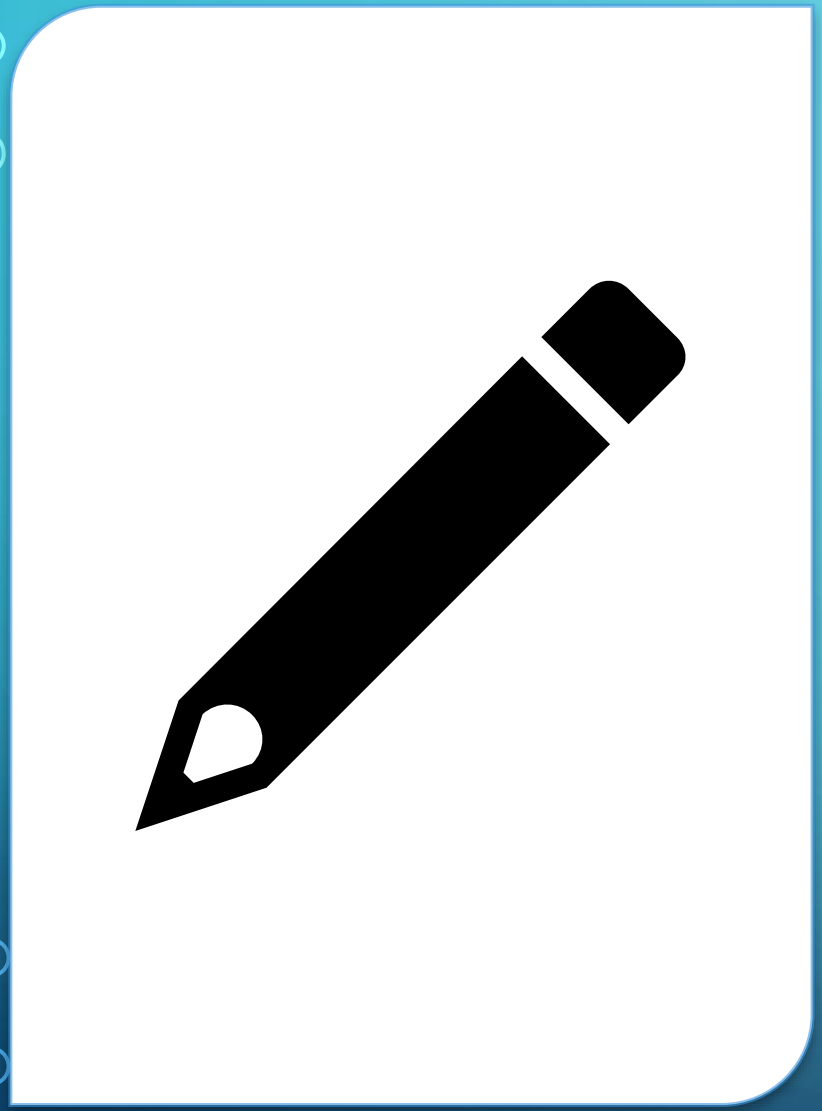
4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

Fases de un SGSI: (1) establecimiento, (2) implementación y operación, (3) monitoreo y revisión, y (4) mantenimiento y mejora



4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

La norma ISO27001 establece en su punto "4.2.1 Establecimiento del SGSI", apartado "j", que la empresa deberá preparar una declaración de aplicabilidad, que incluya los objetivos de control seleccionados y por qué, los objetivos de control existentes, y por último, los objetivos de control excluidos, y por qué.



Ejercicio

REVISE LAS SALVAGUARDAS DE MAGERIT, Y CLASIFIQUE, SEGÚN LOS CRITERIOS GENERALES VISTOS, LAS MEDIDAS QUE PODRÍAN REDUCIR EL RIESGO DE EVASIÓN DE INFORMACIÓN POR ROBO DE UN DISCO DURO EXTERNO CONVENCIONAL.