Actividad 15. Aplicación de MAGERIT

Realizar un Análisis y gestión de riesgos en una organización dedicada a la elaboración de productos de bollería/panadería.
Se debe pasar por varias fases:

PASOS PREVIOS:

Fase 1. Selección de la metodología de análisis y gestión de riesgos.

En nuestro caso, seleccionamos la metodología:

MAGERIT es la metodología de análisis y gestión de riesgos de los sistemas de información.
Está compuesta de tres libros:

- Libro I: Método (habla de una estructura para la gestión del riesgo)
- Libro II: Catálogo de elementos (es una lista de activos que tiene la organización y hasta qué punto el riesgo que tenga un activo puede llegar a afectarle
- Libro III: Guía de técnicas. Muestra herramientas utilizadas en análisis y gestión de riesgos

Tiene 4 objetivos:

- Concienciar a los responsables de la organización de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar y gestionar los riesgos derivados del uso de tecnologías de la información y comunicaciones
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control
- Preparar la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Fase 2. Recopilación de la información de la organización.

Es necesario conocer la organización. Para ello se realizarán visitas, entrevistas, encuestas, revisión de documentos y listas de chequeo para tener una visión clara del entorno que se va a evaluar.

MAGERIT:

Fase 1. Identificación y valoración de los activos críticos de información

Se dividen los activos en diferentes tipos, agrupándolos, dependiendo de la función que realizan en el tratamiento de la información.

IDENTIFICACIÓN DE ACTIVOS:

- Fórmulas de los productos
- Base de datos administrativa
- Sistema administrativo
- Infraestructura de comunicaciones
- Servidor local
- Equipos informáticos

Fase 1. Identificación y valoración de los activos críticos de información

VALORACIÓN DE ACTIVOS:

Se procede a valorar los activos. Se hará la valoración de acuerdo con 3 dimensiones:

- Confidencialidad
- Integridad
- Disponibilidad

Se ha utilizado el siguiente criterio:

VALOR		CRITERIO
Alto (A)	3	Daño grave
Medio (M)	2	Daño importante
Bajo (B)	1	Daño menor

Los resultados han sido los siguientes:

ACTIVO	VALOR
Fórmulas de los productos	3
Base de datos administrativa	3
Sistema administrativo	2
Infraestructura de comunicaciones	2
Servidor local	2
Equipos informáticos	1

Fase 2. Determinación de las amenazas potenciales

Se identifican todas las amenazas posibles que puedan dañar en alguna de las dimensiones a nuestros activos de información.

La valoración de las amenazas se realiza de acuerdo con la frecuencia de ocurrencia y a la degradación del activo.

FRECUENCIA:

VALOR		CRITERIO
Frecuente (F)	10	Mensualmente
Normal (N)	1	Una vez al año
Poco frecuente (PF)	1/10	Cada varios años

La **degradación del activo** la valoramos en una escala del 1 al 100%

Las posibles amenazas se obtienen del catálogo de elementos de MAGERIT, que las divide en:

- Desastres naturales
- De origen industrial
- Errores y fallos no intencionados
- Ataques intencionados

Fase 2. Determinación de las amenazas potenciales

AMENAZAS:

Las amenazas detectadas fueron las siguientes:

AMENAZA	FRECUENCIA	C	I	D
De origen industrial	1/10			80%
Errores de usuarios	1/10	10%	80%	50%
Errores del administrador	1	10%	50%	70%
Escapes y fugas de información	10	90%		
Pérdida y robo de equipos	10	90%		80%
Abuso de privilegios	1	90%	50%	10%
Acceso no autorizado	1	90%	50%	
Modificación deliberada de la información	1		90%	

Fase 4. Estimación del impacto POTENCIAL

Para estimar el impacto se utiliza el valor de los activos y las amenazas a la que están expuestos, realizando un cálculo para cada activo y para cada amenaza de tal manera que el resultado del impacto sea alto (A), medio (M) o bajo (B):

ACTIVO	AMENAZA	Impacto TOTAL
Fórmulas	Escapes y fugas de información	A
Fórmulas	Acceso no autorizado	A

ACTIVO	AMENAZA	Impacto TOTAL
Base de datos administrativa	Errores de usuarios	A
Base de datos administrativa	Errores de administrador	A
Base de datos administrativa	Abuso de privilegios	M
Base de datos administrativa	Modificación deliberada de información	A

ACTIVO	AMENAZA	Impacto TOTAL
Sistema administrativo	Errores de administrador	M
Servidor local	De origen industrial	M
Infraestructura de comunicaciones	De origen industrial	M
Equipos informáticos	Pérdida y robo de equipos	B

Fase 5. Cálculo del riesgo POTENCIAL

Para realizar el cálculo del riesgo, se multiplica la frecuencia de la amenaza por el impacto resultado del paso anterior:

ACTIVO	AMENAZA	RIESGO
Fórmulas	Escapes y fugas de información	A
Fórmulas	Acceso no autorizado	A

ACTIVO	AMENAZA	RIESGO
Base de datos administrativa	Errores de usuarios	M
Base de datos administrativa	Errores de administrador	A
Base de datos administrativa	Abuso de privilegios	M
Base de datos administrativa	Modificación deliberada de información	A

ACTIVO	AMENAZA	RIESGO
Sistema administrativa	Errores de administrador	M
Servidor local	De origen industrial	B
Infraestructura de comunicaciones	De origen industrial	B
Equipos informáticos	Pérdida y robo de equipos	M

Fase 3. Identificación y determinación de salvaguardas

El catálogo de elementos de MAGERIT clasifica a las salvaguardas en 16 tipos.

Se identificaron algunas salvaguardas que nos permitirán reducir la probabilidad de que las amenazas detectadas se materialicen sobre los activos de la organización:

- Identificación y autenticación (6.1. Protecciones generales u horizontales. H.IA)
- Control de acceso lógico (6.1. Protecciones generales u horizontales. H.AC)
- Copias de seguridad (6.2. Protección de los datos/Información. D.A)
- Aplicación de perfiles de seguridad (6.7. Protección de las comunicaciones. COM.A)
- Aseguramiento de la disponibilidad (6.4. Protección de los servicios. SA)
- Control de accesos físicos (6.11. Seguridad física – Protección de las instalaciones. L.AC)
- Plan de recuperación de desastres (6.14. Continuidad de operaciones. DRP)

ACTIVO	AMENAZA	SALVAGUARDA
Fórmulas	Escapes y fugas de información	Identificación y autenticación
Fórmulas	Acceso no autorizado	Control de acceso lógico

ACTIVO	AMENAZA	SALVAGUARDA
Base de datos administrativa	Errores de usuarios	Copias de seguridad
Base de datos administrativa	Errores de administrador	Copias de seguridad
Base de datos administrativa	Abuso de privilegios	Aplicación de perfiles de seguridad
Base de datos administrativa	Modificación deliberada de información	Aplicación de perfiles de seguridad

+

Fase 3. Identificación y determinación de salvaguardas

ACTIVO	AMENAZA	SALVAGUARDA
Sistema administrativa	Errores de administrador	Copias de seguridad
Servidor local	De origen industrial	Aseguramiento de la disponibilidad
Infraestructura de comunicaciones	De origen industrial	Aseguramiento de la disponibilidad
Equipos informáticos	Pérdida y robo de equipos	Control de accesos físicos

Cálculo del riesgo RESIDUAL

Para realizar el cálculo del riesgo, se multiplica la frecuencia de la amenaza por el impacto resultado del paso anterior:

AMENAZA	FRECUENCIA	C	I	D
De origen industrial	1/10			80%
Errores de usuarios	1/10	10%	80%	50%
Errores del administrador	1	10%	50%	70%
Escapes y fugas de información	10	90%		
Pérdida y robo de equipos	10	90%		80%
Abuso de privilegios	1	90%	50%	10%
Acceso no autorizado	1	90%	50%	
Modificación deliberada de la información	1		90%	

ACTIVO	AMENAZA	Impacto TOTAL
Fórmulas	Escapes y fugas de información	**M**
Fórmulas	Acceso no autorizado	**B**

ACTIVO	AMENAZA	Impacto TOTAL
Base de datos administrativa	Errores de usuarios	**B**
Base de datos administrativa	Errores de administrador	**B**
Base de datos administrativa	Abuso de privilegios	**B**
Base de datos administrativa	Modificación deliberada de información	**M**

Cálculo del riesgo RESIDUAL

ACTIVO	AMENAZA	Impacto TOTAL
Sistema administrativo	Errores de administrador	**B**
Servidor local	De origen industrial	**B**
Infraestructura de comunicaciones	De origen industrial	**B**
Equipos informáticos	Pérdida y robo de equipos	**B**

ACTIVO	AMENAZA	RIESGO
Fórmulas	Escapes y fugas de información	**M**
Fórmulas	Acceso no autorizado	**B**

ACTIVO	AMENAZA	RIESGO
Base de datos administrativa	Errores de usuarios	**B**
Base de datos administrativa	Errores de administrador	**B**
Base de datos administrativa	Abuso de privilegios	**B**
Base de datos administrativa	Modificación deliberada de información	**M**

Cálculo del riesgo RESIDUAL

ACTIVO	AMENAZA	RIESGO
Sistema administrativa	Errores de administrador	**B**
Servidor local	De origen industrial	**B**
Infraestructura de comunicaciones	De origen industrial	**B**
Equipos informáticos	Pérdida y robo de equipos	**B**