Características de impacto y análisis de riesgos

¿Qué es el riesgo?

Es la posibilidad de **sufrir una afectación** por causa de factores externos o internos

Un peligro latente que puede o no materializarse

Riesgos que contemplan:

Vulnerabilidades y amenazas

Controlados, tratados, mitigados, prevenidos y, en algunos casos, eliminados, es momento de profundizar en ellos y conocer su impacto, probabilidad, su análisis y tratamiento.

Riesgo total = **probabilidad x impacto promedio**

A partir de esta fórmula, se determina el tratamiento y después de la aplicación de los controles se obtendrá:

- El riesgo residual
- La determinación de los activos
- Los requisitos legales y de negocio
- La valuación de los activos identificados

Así mismo, se obtendrá:

- La identificación de las amenazas y vulnerabilidades
- La evaluación del riesgo
- El cálculo del riesgo
- Escala de riesgo preestablecidos

Efectuado el análisis, se determinan las acciones respecto a los riesgos residuales:

Controlar el riesgo. Reforzar los controles existentes y/o agregar nuevos controles.

Aceptar el riesgo. Se selecciona que el nivel de exposición es ajustado y por lo tanto se acepta.

Compartir el riesgo. Con acuerdos contractuales parte del riesgo se traspasa a un tercero.

Eliminar el riesgo. Excluir el activo relacionado por ende se elimina el riesgo.

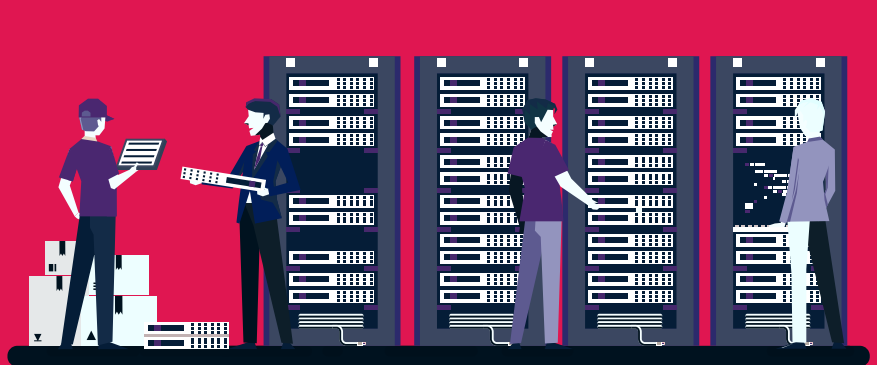
Análisis del riesgo

Realizar la evaluación de los **activos de información**, a partir de unos criterios de evaluación de características que afectan la seguridad de la información.

Es todo aquello que tiene valor para la organización y que pueden ser activos tangibles e intangibles

Ejemplos de tipos de activos son:

- Servidores: servidor *web*, servidor de base de datos.
- Registros: registros, bases de datos, fotografías, videos.
- *Software:* aplicaciones y sistemas basados en *software*.
- *Hardware*: infraestructura tecnológica.
- Servicios: servicios de aplicación. Datos/información pura.



Dimensiones

Son atributos o características que dan valor a un activo de información.

Se pueden utilizar para medir el grado de materialización de una amenaza sobre un activo.

Ejemplos:

- Disponibilidad
- Integridad
- Confidencialidad
- Autenticidad
- Trazabilidad

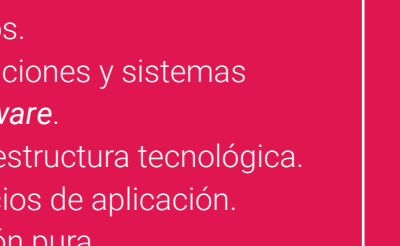
Criterios de valoración

Se sugiere el establecimiento de escalas que permiten comparar y medir riesgos que pueden afectar un activo.

Amenazas

"Cosas que les pueden pasar a los activos causando un perjuicio a la organización" se pueden identificar los siguientes tipos sugeridos.

- Desastres naturales.
- De origen industrial.
- Errores y fallas no intencionados.
- Ataques intencionados.



Salvaguardas

Son los procedimientos o mecanismos que se aplican para reducir el riesgo a un activo de información.

Probabilidad

Es la posibilidad de que suceda una amenaza sobre un activo de información.

Beneficios de examinar los riesgos

- ☑ Favorece la toma de medidas que evitan que se produzcan y/o mitigarlos.
- ☑ Prepara a las organizaciones sobre este tipo de situaciones negativas y recolecta una serie de factores fundamentales para su consecución.
- ☑ Visualización y detección de las debilidades existentes en los sistemas.
- ☑ Ayuda en la toma de las mejores decisiones en materia de seguridad de la información.

Objetivos del análisis de riesgos, se encuentran:

Identificar los riesgos informáticos que pueden afectar los activos de información en una organización.

Facilitar la identificación de estrategias de control para mitigar los riesgos identificados.

Siempre será posible establecer acciones para realizar el tratamiento de los riesgos:

- Eliminar el riesgo.
- Mitigar el riesgo.
- Compartir el riesgo.
- Aceptar y financiar el riesgo.

Fuentes: Freepik. Recursos Educativos Digitales SENA (2021).