


ESCENARIO Y ELEMENTOS CLAVES



Es muy importante que una organización realice un examen consciente de su actual situación respecto a la seguridad.

Este análisis permitirá tomar acciones en caso que el resultado indique que se encuentra en una situación comprometida.



El examen implica los siguientes pasos:

Identificación de activos

Evaluación de vulnerabilidades

Identificación de amenazas

Estimación de los riesgos

Activos

La identificación de activos es el proceso mediante el cual una organización intenta valorar la información y sus sistemas.

La parte más difícil del proceso de identificación de activos es intentar asignarle un valor a la información.

En algunos casos, deberíamos determinar qué sucedería en el caso que la información se pierda o se vuelva no disponible.

Activos

Si la ausencia de esta información provoca que el negocio se detenga, se podrá valorar según el costo que le provoque a la empresa esta detención.

Podemos mencionar los siguientes activos asociados a los sistemas de información:

Recursos de información

Recursos de equipos

Recursos Humanos

Vulnerabilidades

Una vulnerabilidad es un fallo en un sistema **que puede ser explotada** por un atacante generando un riesgo para la organización o para el mismo sistema.

Existen dos tipos de vulnerabilidades que se mencionan a continuación:

Vulnerabilidades físicas

Vulnerabilidades lógicas

Vulnerabilidades físicas

Son las que van a afectar a la ***infraestructura*** de la organización de manera física y se pueden mencionar en este tipo de clasificación a los desastres naturales.

También los controles de acceso y las condiciones de los CPD o data center.

Vulnerabilidades lógicas

Son las que van a afectar directamente el ***desarrollo*** de la operación de los sistemas, y estas pueden ser de:

- Configuración (Sist Op, Firewalls, Server)
- Actualización (Sist, App)
- Desarrollo (SQL)

Amenazas

Una vez identificados los recursos que necesitan protección, se deberá identificar cuáles son las amenazas a estos recursos, y poder determinar qué potencial de daño o pérdida existe.

La implementación de una política de seguridad requiere que no solo se evalúen las amenazas, sino también el **origen**, por lo cual tendremos amenazas:

- **Externas**
- **Internas**
- **Activas**
- **Pasivas**

RIESGO

La evaluación de riesgos es una consideración **sistemática** de los siguientes puntos:

- **Impacto potencial** de una falla de seguridad en la organización, teniendo en cuenta las consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos.
- **Probabilidad de ocurrencia** de dicha falla tomando en cuenta las amenazas, vulnerabilidades y los **controles actualmente implementados**.

RIESGO

El análisis de riesgos implica determinar lo siguiente:

- ***Qué necesito proteger:*** Evaluación de los activos y su importancia.
- ***De quién debo protegerlo:*** Evaluación de amenazas y vulnerabilidades.
- ***Cómo protegerlo:*** Evaluación de contramedidas.

RIESGO

Los factores que debemos tener en cuenta para realizar una correcta evaluación del riesgo son:

- **El riesgo de pérdida del recurso,**
- **La importancia que representa el recurso para la empresa**
 - La **Disponibilidad**: es la medida cuán importante es tener el recurso disponible todo el tiempo.
 - La **Integridad**: es la medida de cuán importante es que el recurso o los datos del mismo sean consistentes.
 - La **Confidencialidad**: es la medida de la importancia de que los recursos sólo sean utilizados por las personas autorizadas.

RIESGO

Objetivos de la Gestión de Riesgo

Análisis de Riesgos: Comprende la Identificación de vulnerabilidades y amenazas y también el análisis de probabilidad de ocurrencia e impacto.

Tratamiento de Riesgos: Comprende las tareas de priorizar, presupuestar, implementar y mantener las medidas seleccionadas para mitigar los riesgos.

El principal objetivo de la Gestión del Riesgo es el de reducir los riesgos hasta niveles de tolerancia aceptables para la organización.