Escuela Superior de Guerra ‘General Rafael Reyes Prieto’

Gestión de riesgos en ciberseguridad

My. Chavarro Gutiérrez Luis Alberto

My. Esmeral Madrid Diego Alejandro

My. Guerrero Cortes Alex Danny

My. Robles Ocampo Edna Giannine

Gestión de la Ciberseguridad

Dr. Jaider Ospina Navas

Curso de estado Mayor

17 de Marzo de 2025

**Gestión de riesgos en ciberseguridad**

## Definiciones

## Gestión de Riesgos

La gestión de riesgos en ciberseguridad es un proceso sistemático que identifica, evalúa y mitiga amenazas que pueden comprometer la información y los sistemas de una organización. Su objetivo es minimizar posibles pérdidas a través de controles de seguridad y medidas preventivas (Instituto Nacional de Ciberseguridad (INCIBE), 2021, p. 12).

## Riesgos en ciberseguridad

### Malware.

El malware es un software malicioso diseñado para infiltrarse o dañar sistemas informáticos sin el consentimiento del usuario. Este tipo de amenaza incluye virus, gusanos, troyanos y ransomware, entre otros (INCIBE, 2021, p. 35).

### Phishing.

El phishing es una técnica de ingeniería social en la que los atacantes intentan obtener información confidencial haciéndose pasar por entidades legítimas. Se transmite a través de correos electrónicos falsificados o páginas web fraudulentas (IBM, s.f.).

### Ransomware

El ransomware es un software malicioso que cifra los archivos de la víctima y exige un pago para restaurar el acceso. Puede causar interrupciones operacionales y pérdidas económicas significativas (Fortinet, s.f.).

### Ataques de denegación de servicio (DDoS)

Un ataque DDoS sobrecarga un servidor o red con tráfico excesivo, provocando la interrupción de servicios y afectando la disponibilidad de los recursos (Fortinet, s.f.).

### Amenazas internas

Las amenazas internas provienen de empleados, contratistas o socios comerciales con acceso a los sistemas de la organización que, por negligencia o intención maliciosa, pueden comprometer la seguridad (INCIBE, 2021, p. 42).

### Ingeniería social

La ingeniería social es una técnica utilizada por ciberdelincuentes para manipular a las personas y obtener acceso a información sensible. Puede presentarse en forma de llamadas fraudulentas, mensajes engañosos o sitios web falsificados (Vectra AI, s.f.).

### Vulnerabilidades de terceros

Estas vulnerabilidades ocurren cuando sistemas de proveedores externos presentan fallos de seguridad que pueden ser explotados por atacantes, afectando a las empresas que dependen de esos servicios (Hewlett Packard Enterprise (HPE), s.f.).

### Filtraciones de datos

Una filtración de datos ocurre cuando información confidencial es expuesta o robada, ya sea por ataques cibernéticos o errores humanos. Estas filtraciones pueden generar sanciones legales y daños a la reputación de la organización (INCIBE, 2021, p. 48).

### Accesos no autorizados

Los accesos no autorizados ocurren cuando individuos sin permisos adecuados ingresan a sistemas o bases de datos confidenciales, lo que puede llevar al robo de información y alteración de datos (INCIBE, 2021, p. 51).

### Inyección de código

La inyección de código es una vulnerabilidad en la que los atacantes insertan código malicioso en una aplicación para ejecutar comandos no autorizados o acceder a datos sensibles (INCIBE, 2021, p. 55).

# Referencias

Fortinet. (s.f.). Tipos de ciberataques: ataque DDoS, ransomware y más. <https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks>

Hewlett Packard Enterprise (HPE). (s.f.). ¿Qué es una amenaza de ciberseguridad?. <https://www.hpe.com/lamerica/es/what-is/cybersecurity-threats.html>

IBM. (s.f.). ¿Qué es un ataque cibernético?. <https://www.ibm.com/mx-es/topics/cyber-attack>

Instituto Nacional de Ciberseguridad (INCIBE). (2021). Glosario de términos de ciberseguridad: una guía de aproximación para el empresario. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>

Vectra AI. (s.f.). ¿Qué son las técnicas de ataque?. <https://es.vectra.ai/topics/cyberattack-techniques>