

MALWARE Y VIRUS INFORMATICOS EN LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

¿Qué es el malware?

Un software malicioso que afecta la seguridad de los sistemas informáticos, comprometiendo la Confidencialidad, Integridad y Disponibilidad (CID) de la información.



CONFIDENCIALIDAD: RIESGO PARA LA PRIVACIDAD

- Robo de credenciales y datos sensibles.
 - Filtración de información confidencial.
 - Uso de spyware y keyloggers para monitorear actividad.
- ◆ Solución: Uso de antivirus, autenticación multifactor y monitoreo de accesos.



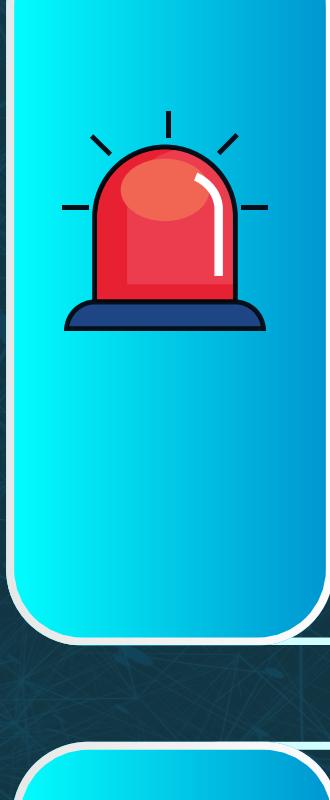
INTEGRIDAD: ALTERACION DE DATOS

- Corrupción de archivos y bases de datos.
 - Manipulación de información financiera o administrativa.
 - Ataques de ransomware que cifran datos.
- ◆ Solución: Copias de seguridad regulares, control de versiones y detección de intrusos.



DISPONIBILIDAD: INTERRUPCION DEL SISTEMA

- Ralentización o bloqueo de equipos.
 - Pérdida de acceso a datos y servicios.
 - Saturación de redes por malware propagado.
- ◆ Solución: Firewalls, segmentación de red y mantenimiento preventivo.



ESTRATEGIAS DE PROTECCION Y MITIGACION

- **Capacitación:** Concienciación sobre ciberseguridad.
- **Software de Seguridad:** Uso de antivirus y firewalls.
- **Actualizaciones Frecuentes:** Parches y correcciones de vulnerabilidades.
- **Copias de Seguridad:** Respaldo en la nube o almacenamiento externo.
- **Monitoreo y Respuesta Rápida:** Implementación de sistemas de detección de amenazas.



RECUPERACION DE SISTEMAS INFECTADOS

- Aislar dispositivos afectados.
- Usar herramientas de eliminación de malware.
- Restaurar información desde copias de seguridad.
- Reforzar las políticas de seguridad para prevenir futuros ataques.

CONCLUSION

En la actualidad, el malware sigue siendo una de las amenazas más significativas para la seguridad informática, afectando la confidencialidad, integridad y disponibilidad de los sistemas. La implementación de estrategias preventivas y de mitigación es esencial para reducir los riesgos asociados a estos ataques. La educación de los usuarios, el uso de herramientas de seguridad avanzadas y una respuesta eficaz ante incidentes son clave para garantizar la protección de la información y la continuidad de las operaciones en un entorno digital cada vez más expuesto a ciberamenazas.