# FORMACIÓN CIBERSEGURIDAD 2024

**Javier Castillo Osuna** 

### Introducción

La ciberseguridad es un pilar fundamental para garantizar la protección de los datos, sistemas y personas en nuestra organización.

El objetivo de este plan de formación es proporcionar las herramientas y conocimientos necesarios para fortalecer nuestra postura de seguridad y garantizar la continuidad operativa en un entorno digital seguro.



### **Amenazas Comunes**

**Phishing**: Correos o mensajes fraudulentos para robar información.

**Malware**: Programas maliciosos que comprometen dispositivos.

**Ingeniería social**: Manipulación para obtener información confidencial.

**Errores humanos**: Uso indebido de contraseñas, clics en enlaces inseguros, etc.

#### PRINCIPALES AMENAZAS A LA CIBERSEGURIDAD



#### Ransomware

Se considera la amenaza más preocupante en la actualidad. Los ciberdelincuentes utilizan técnicas de extorsión cada vez más complejas.



### Malware (software malicioso)

Se incluyen en esta categoría los troyanos, gusanos y programas espías. Su uso disminuyó durante la pandemia de Covid-19, pero ha vuelto a aumentar.



#### Amenazas de ingeniería social

Se aprovechan del comportamiento o error humano para obtener información. El ataque más común es el phishing (a través del correo electrónico) o el smishing (a través de mensajes de texto).

Fuente: Agencia de la Unión Europea para la Ciberseguridad (ENISA), 2022



## **Phishing**

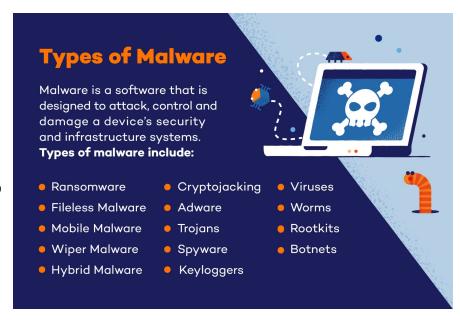
- Descripción: Técnica de ingeniería social que engaña a los usuarios para que revelen información sensible (contraseñas, tarjetas de crédito, etc.) mediante correos electrónicos o sitios web falsificados.
- Ejemplo: Correos que parecen ser de instituciones legítimas, como bancos o empresas tecnológicas, solicitando que el usuario ingrese datos personales.
- Prevención:
  - No hacer clic en enlaces desconocidos.
  - Verificar la autenticidad del remitente antes de proporcionar información.



#OSI**consejo** www.incibe.es/ciudadania

### **Malware**

- Descripción: Software malicioso diseñado para dañar, explotar o deshabilitar computadoras y sistemas. Incluye virus, troyanos, ransomware, entre otros.
- Ejemplo: Archivos adjuntos o enlaces en correos electrónicos que instalan software dañino cuando se abren.
- Prevención:
  - Usar software antivirus actualizado.
  - No abrir archivos adjuntos de fuentes no verificadas.



# Ingeniería Social

- Descripción: Manipulación psicológica de las personas para que realicen acciones o divulguen información confidencial.
- Ejemplo: Llamadas telefónicas o mensajes que pretenden ser de un compañero de trabajo o proveedor, pidiendo contraseñas o acceso a sistemas.
- Prevención:
  - Verificar siempre la identidad de la persona antes de proporcionar información.
  - No compartir contraseñas ni credenciales por canales no seguros.



### **Errores Humanos**

- Descripción: Errores involuntarios cometidos por los empleados que pueden comprometer la seguridad, como utilizar contraseñas débiles, hacer clic en enlaces maliciosos o compartir información sensible accidentalmente.
- Ejemplo: Escribir contraseñas fáciles de adivinar o enviar información confidencial por error a la persona equivocada.
- Prevención:
  - Implementar políticas de contraseñas seguras.
  - Entrenamiento continuo sobre buenas prácticas de seguridad y manejo de información.

