

CIBERSEGURIDAD

APLICADA A PYMES Y AUTÓNOMOS



Buenas prácticas en Seguridad de la información para pymes y emprendedores

Ana Bejarano Quintas, Consultora en Seguridad de la información de Ariadnex Tecnología Flexible

**BUENAS PRÁCTICAS
EN SEGURIDAD DE
LA INFORMACIÓN
PARA PYMES Y
EMPRENEDORES**

Índice

- 1. Noticias recientes**
- 2. Conceptos de ciberseguridad**
- 3. Riesgos**
- 4. Medidas preventivas**
- 5. Beneficios**
- 6. Preguntas**

**BUENAS PRÁCTICAS
EN SEGURIDAD DE
LA INFORMACIÓN
PARA PYMES Y
EMPRENEDORES**

Noticias recientes

¿Os suena...?

Detienen a 22 personas por estafar a 61 acceso a miles de víctimas en toda España "phishing" Las ciberestafas se disparan en Extremadura

Se trata de 10 hombres y 12 mujeres de entre 20 y 40 años. Se les detuvo en Palma de Mallorca (8), Barcelona (6), San Sebastián (1), Sevilla (1) y Pamplona (1).

Fuente: U

Los ciberdel

La última campaña de delincuencia por Internet se ceba con los clientes de Unicaja, aprovechando la fusión con Liberbank

TECNOLOGÍA

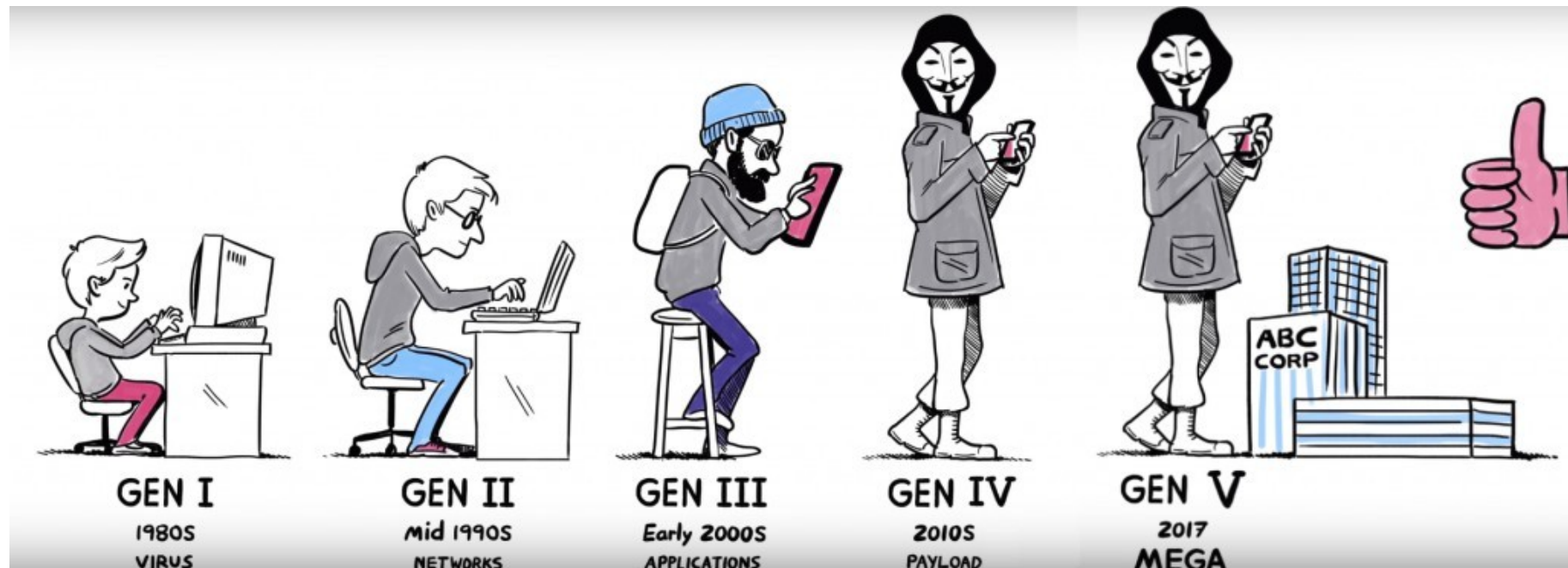
Deepfakes: FBI investiga el robo de identidades para conseguir trabajos remotos

- Los impostores utilizan rostros y voces falsos para ser contratados. La técnica se utiliza principalmente para postular en el sector tecnológico

nientos
unidos por
T

tes

Evolución amenazas ciberseguridad



**BUENAS PRÁCTICAS
EN SEGURIDAD DE
LA INFORMACIÓN
PARA PYMES Y
EMPREENDEDORES**

Conceptos de ciberseguridad

¿Qué es la ciberseguridad?

“Protección de **activos de información**, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los **sistemas de información** que se encuentran interconectados.”



¿Qué es la ciberseguridad?

“Protección de **activos de información**, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los **sistemas de información** que se encuentran interconectados.”



“Conocimientos o datos que tienen valor para una organización.”



“Aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma.”

**BUENAS PRÁCTICAS
EN SEGURIDAD DE
LA INFORMACIÓN
PARA PYMES Y
EMPRENDEDORES**

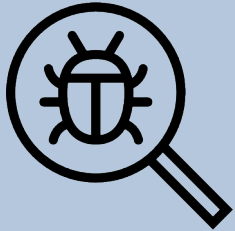
Riesgos

Malware

- Software malicioso.
- Proporciona acceso no autorizado para robar información y/o causar daños en el dispositivo.
- Diseñados para evadir herramientas de antivirus que escanean archivos adjuntos maliciosos.
- Señales → dispositivo ralentizado o bloqueado asiduamente, aparición de anuncios emergentes, disminución espacio del disco repentina, aumento de actividad de Internet en tu red.

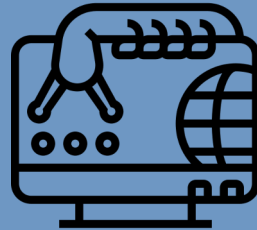


VIRUS



Código ejecutable

GUSANOS



Se propagan entre equipos

TROYANOS



Introducen malware

SPYWARE



Roba datos

TIPOS DE MALWARE

RANSOMWARE



Chantajes

ADWARE



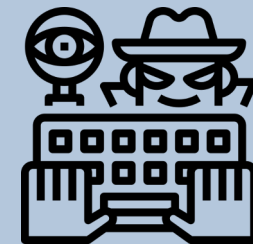
Publicidad sin parar

ROOTKIT



Permisos de administrador

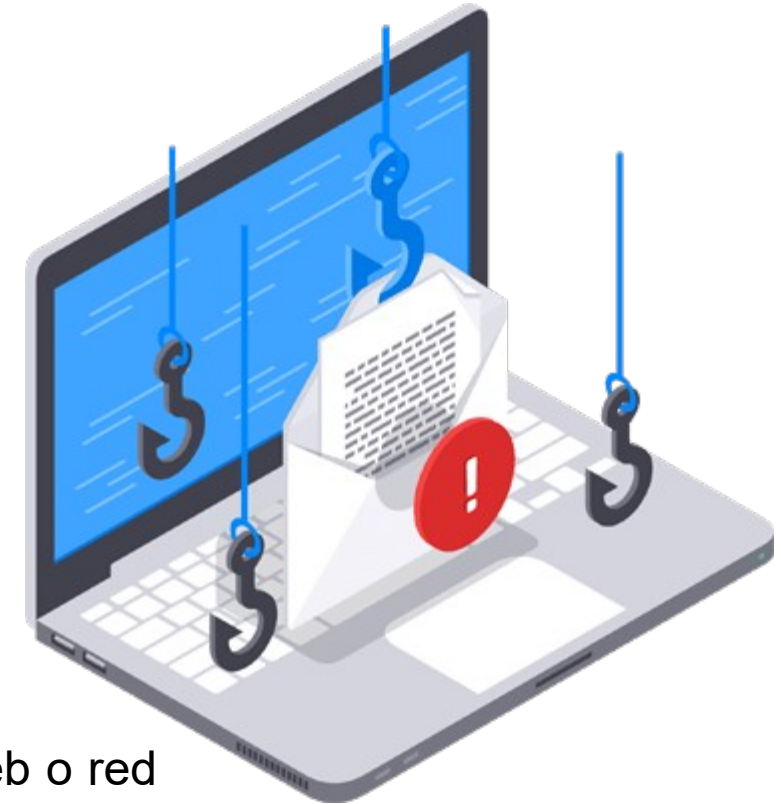
KEYLOGGER



Usan el teclado

Phishing

El estafador emplea técnicas de ingeniería social, haciéndose pasar por una persona o entidad de confianza a través de un medio electrónico como SMS, email, redes sociales, etc. para estafar y/u obtener información confidencial.



Denegación de servicios

Este tipo de ataques intenta bloquear un servidor, sitio web o red sobrecargándolo con tráfico generalmente usando el protocolo simple de administración de red (SNMP) empleado para routers, impresoras, switches, etc.

Amenazas internas

Los empleados que forman o hayan formado parte de la empresa, socios comerciales o cualquier persona que haya tenido acceso a sistemas internos pueden considerarse amenazas internas.

Ataques de intermediario

Ataques de espionaje en los que el ciberdelincuente intercepta y transmite mensajes entre dos partes para robar datos.



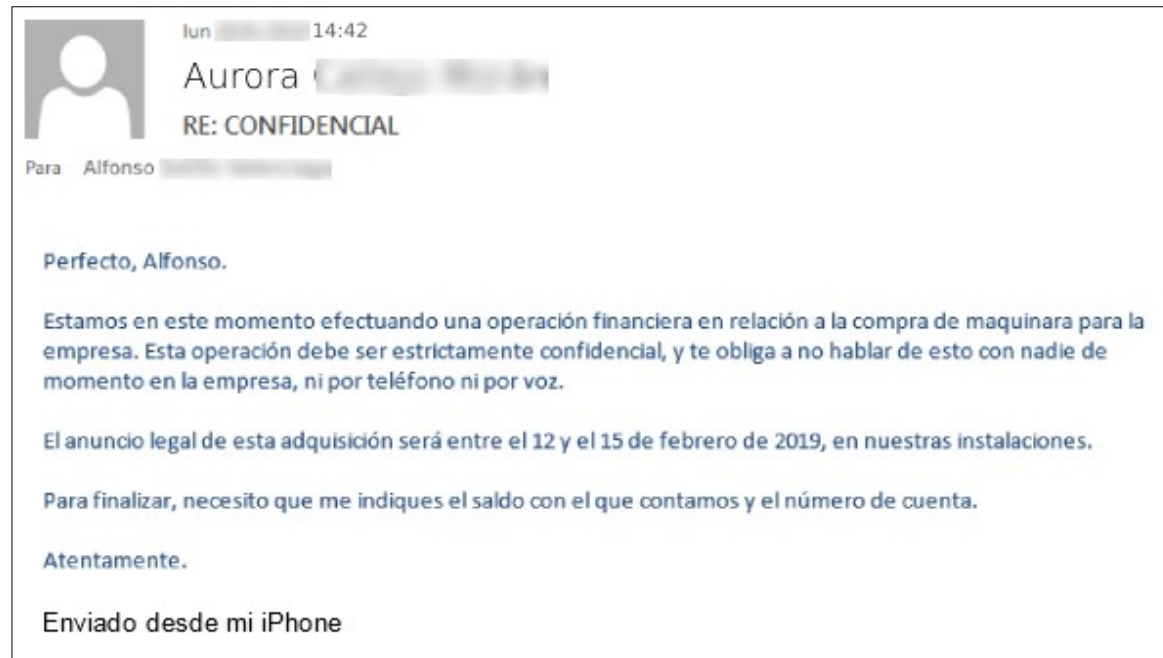
Estafa del CEO

Se trata de una estafa que tiene como objetivo engañar a empleados para que paguen una factura o realicen una transferencia desde la cuenta de la empresa a una cuenta del ciber criminal.



Estafa del CEO

Se trata de una estafa que tiene como objetivo engañar a empleados para que paguen una factura o realicen una transferencia desde la cuenta de la empresa a una cuenta del ciber criminal.



**BUENAS PRÁCTICAS
EN SEGURIDAD DE
LA INFORMACIÓN
PARA PYMES Y
EMPREENDEDORES**

Medidas preventivas

¿Qué podemos hacer nosotros?



**Cambio periódico de
contraseñas**

Contraseñas robustas

**No reutilizar
credenciales**



123456
Maria123
m@R!a1970#
Sl@!U^&l8rRu

MEDIDAS PREVENTIVAS

20

Cambio periódico de contraseñas

Contraseñas robustas

No reutilizar credenciales

Copias de seguridad

Evitar uso de dispositivos personales

Verificar remitente en correos sospechosos

Mantener equipos actualizados

Evitar programas piratas sin licencia

Limitar el uso de USB

Almacenar credenciales con software específico

Bloquear la pantalla al abandonar puesto de trabajo habitual

No hacer clic en links o archivos de correos SPAM o sospechosos

Evitar descargar software de páginas no oficiales

Ante cualquier duda contactar con el personal informático

No otorgar datos personales por correo

**BUENAS PRÁCTICAS
EN SEGURIDAD DE
LA INFORMACIÓN
PARA PYMES Y
EMPRENEDORES**

Beneficios

¿Se invierte lo suficiente en ciberseguridad?

¿Es costoso?

¿Es una pérdida de tiempo y dinero?

¿Sale rentable?

¿Cuánto de probable es sufrir un ciberataque?



yahoo!

IBERDROLA



MediaMarkt

¿Y las pymes?

Los ciberataques a empresas han aumentado un **80%** tras la pandemia. En concreto, **7 de cada 10** pymes en España han sufrido uno

España es el **tercer país** que más ciberataques sufre por detrás de Estados Unidos y Alemania

Ha incrementado un 125% el número de ataques en España con respecto al año pasado, **40.000/día** ciberataques de media

El coste medio de un ciberataque a una pequeña empresa en España es de **75.000€**

VENTAJAS

- 1) Reducir riesgos y ahorrar gastos imprevistos
- 2) Mantener confianza con clientes
- 3) Mejorar la reputación de la marca e imagen corporativa
- 4) Asegurar integridad de la información y datos internos
- 5) Monitorización continua
- 6) Aumento de la productividad
- 7) Capacidad de recuperación

DESVENTAJAS

- 1) No hay garantía del 100% de protección
- 2) Se trata de una inversión
- 3) Compleja
- 4) Constante seguimiento y supervisión

**BUENAS PRÁCTICAS
EN SEGURIDAD DE
LA INFORMACIÓN
PARA PYMES Y
EMPRENEDORES**

Preguntas

¿Tenéis alguna pregunta?



Ana Cristina Bejarano Quintas
ana@ariadnex.com
Ariadnex Tecnología Flexible S.L.
www.ariadnex.com

¡Muchas gracias!



UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

JUNTA DE EXTREMADURA