humalia
Solutions

# Consejos Prácticos de Ciberseguridad en la Nueva Normalidad

Oscar Jimenez
ojimenez@humalia.es
www.humalia.es

# Agenda

1. Situación Actual
2. Principales Riesgos
3. Consejos Prácticos

# Agenda

1. Situación Actual
2. Principales Riesgos
3. Consejos Prácticos


El cibercrimen ya es la actividad delictiva que mueve más dinero, por encima de la venta de armas y el narcotráfico


La crisis del coronavirus aumenta la ciberdelincuencia
https://www.interempresas.net/Ciberseguridad/Articulos/300317-La-crisis-del-coronavirus-aumenta-la-ciberdelincuencia.html
El coronavirus dispara las posibilidades de ciberataques
https://www.niusdiario.es/ciencia-y-tecnologia/tecnologia/ciberseguridad-tiempos-coronavirus-pedro-perez-pablo-telefonica-delitos-online-fake-news-ataque-informatico-teletrabajo_18_2921370108.html
Cuidado: proliferan los ciberataques durante la crisis de la COVID-19
https://nmas1.org/news/2020/03/28/ciberseguridad-coronavirus
Cybersecurity experts to fight coronavirus-related hacking
https://www.foxbusiness.com/technology/cybersecurity-experts-come-together-to-fight-coronavirus-related-hacking
WORLD ECONOMIC FORUM
Why cybersecurity matters more than ever during the coronavirus pandemic
https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/
Riesgo de 'hackeos' graves por la oleada de teletrabajo. ¿Qué hacer para evitarlos?
https://www.elconfidencial.com/tecnologia/2020-03-12/ciberseguridad-teletrabajo-covid-fallos_2491832/

# Incremento de Ciberataques

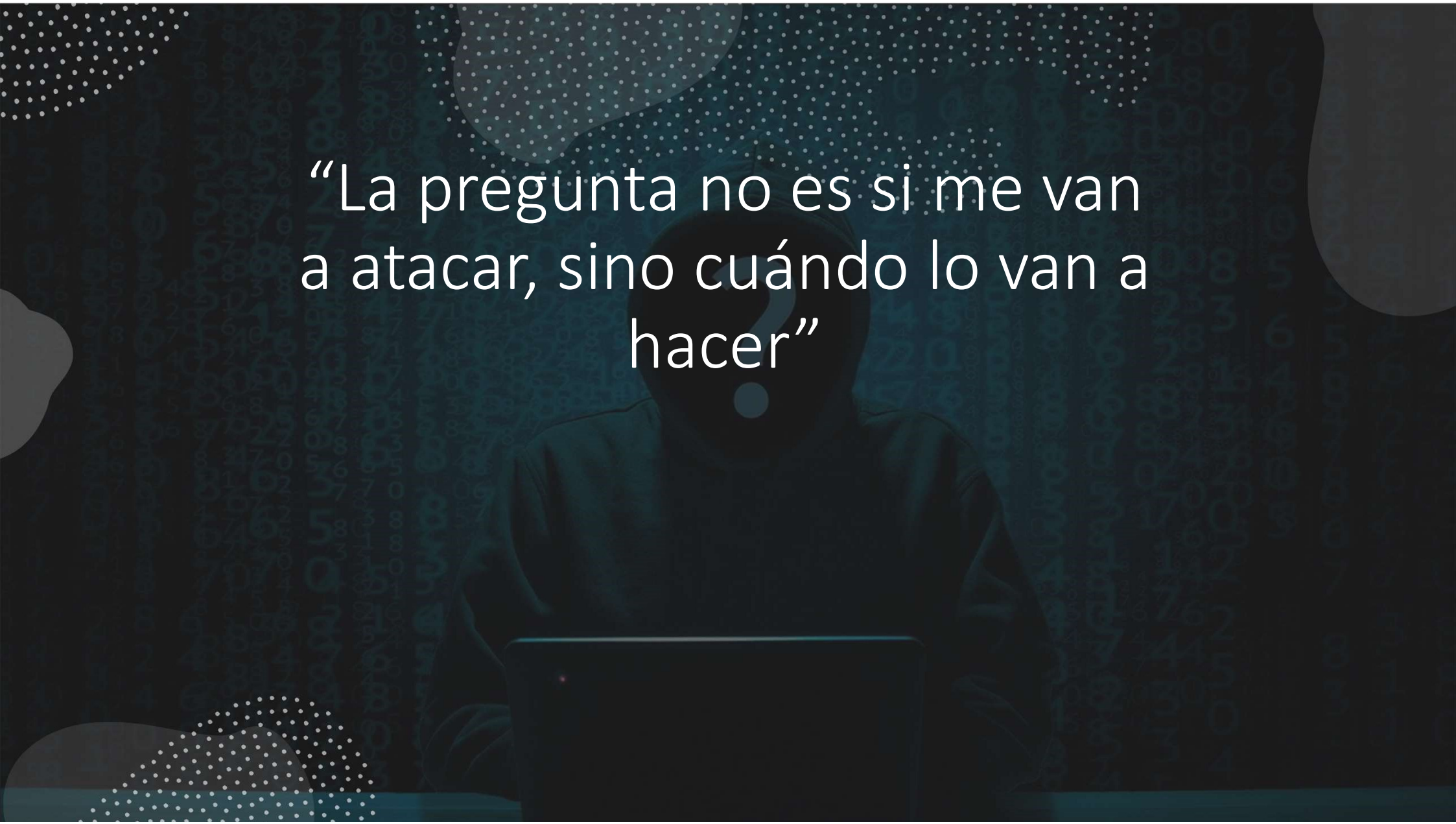
**33% más** solo entre enero y finales de marzo de 2020 (fuente Mimecast)

**60.000** nuevas webs fraudulentas

Aumento del spam, que se disparó un **6.000%** (fuente IBM)

Además de cuentas falsas en redes sociales, apps para móviles maliciosas (como Coronavirus Finder), troyanos bancarios (Ginp) e incluso suplantaciones de organismos públicos como el del Ministerio de Sanidad

Las empresas ya son responsables por Ciberataques


“La pregunta no es si me van a atacar, sino cuándo lo van a hacer”

# Agenda

1. Situación Actual
2. Principales Riesgos
3. Consejos Prácticos

El 70% de los archivos maliciosos que reciben las empresas en España se produce a través de correo electrónico

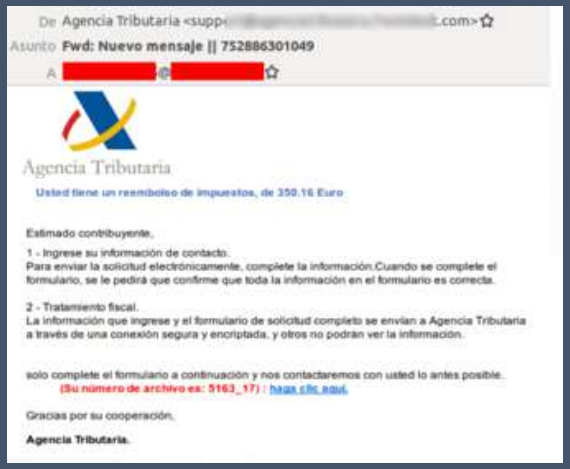
Threat Intelligence Report de Check Point® Software Technologies Ltd

# Principales Fraudes y Riesgos

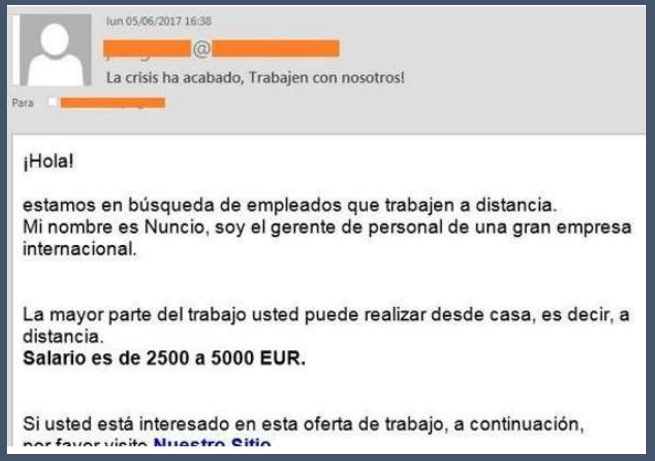
humalia
Solutions

## Ingeniería social a través del correo electrónico

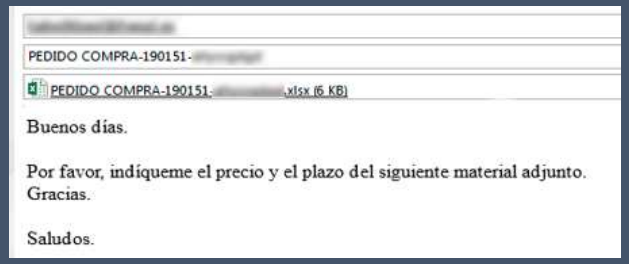
### Phishing




### Scam




### Malware




### Ransonware

Los teléfonos móviles son uno de los objetivos que más interés despiertan en los cibercriminales debido a la gran cantidad de información que almacenan en su interior

Dispositivos **Android** son atacados en un 50% de los casos.

Dispositivos **Windows** un 25%

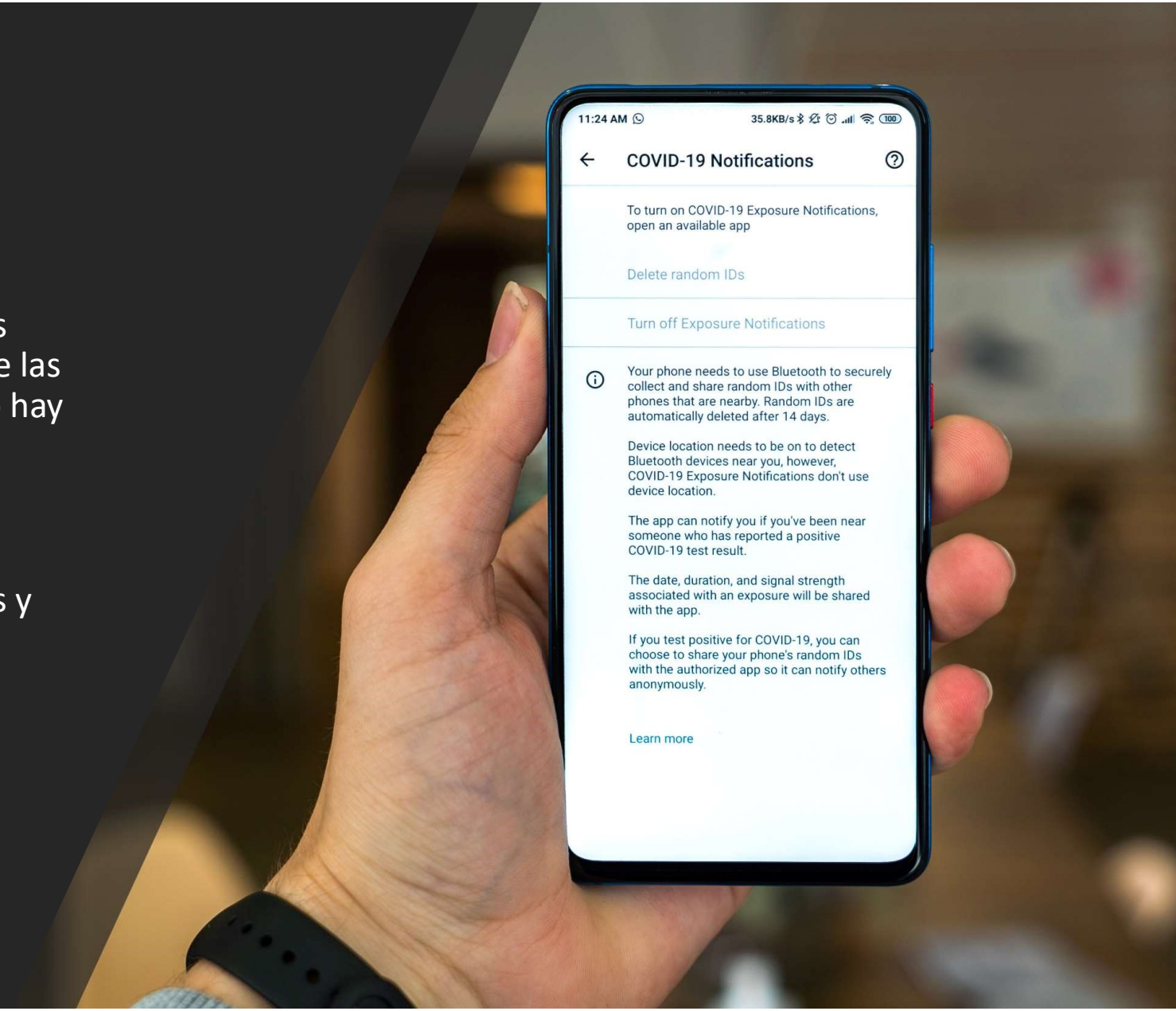
Dispositivos **Apple** un 10%

Estudio de S21sec

# BLURtooth

- Afecta a todos los dispositivos bajo el estándar Bluetooth entre las versiones 4.0 y 5.0, y todavía no hay solución para ello.

- Los dispositivos más recientes y modernos, con una versión de **Bluetooth 5.1 están a salvo** de BLURtooth.




FREE
WiFi
INSIDE

# Agenda

1. Situación Actual
2. Principales Riesgos
3. Consejos Prácticos

# Activo más importante a proteger

Todas las empresas y particulares deben preocuparse por su información digital

**INTANGIBLE**

- Know-How
- Reputación
- Propiedad intelectual


**TANGIBLE**

- Ordenadores
- Dispositivos de almacenamiento
- Teléfonos móviles

Disponibilidad | Integridad | Confidencialidad

# ¿Qué puedo hacer?

## Sistema de Gestión de Seguridad de la Información (SGSI)

Políticas
Procedimientos
Tareas

Reducir el Riesgo
Minimizar los Daños

## Establecer una cultura de ciberseguridad

Todos los empleados tengan una formación básica al respecto

Web del INCIBE
(www.incibe.es)

## Implantar medidas técnicas

Dependen de las características de la empresa, tamaño, objetivo, sistemas, presupuesto

1. Equipos
2. Red en general

# Contraseñas para Control de Acceso

La robustez es la principal medida de seguridad

- Longitud mínima de 8 caracteres, cuanto más larga mejor
- Combinación de letras, minúsculas, mayúsculas, números y símbolos.

## Utilizar para su creación reglas nemotécnicas

Seleccionamos una frase: «**en un lugar de la mancha**».

Hacemos uso de mayúsculas: «**En un lugar de la Mancha**».

Incluimos el servicio: «**En un lugar de la Mancha Correo**».

Añadimos números: «**En un lugar de la Mancha Correo de 2019**».

Añadimos caracteres especiales: «**En un lugar de la Mancha Correo de 2019!**».

La comprimimos utilizando la primera letra de cada palabra: «**EuldlMCd2019!**».

## Buenas Prácticas de Uso

No compartidas

Doble Factor de Autenticación

Una para cada servicio

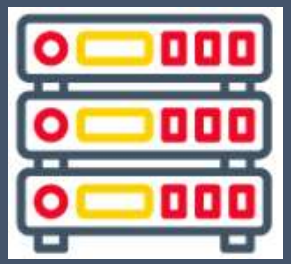
Gestores de Contraseñas

**1Password** **KeePass** **LastPass**

# Backup - Copia de Seguridad

Proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlas

Discos duros externos



Dispositivos NAS

Servicios en la Nube


## La estrategia 3-2-1

- **3** Copias de seguridad de cualquier archivo importante
- **2** Soportes distintos de almacenamiento
- **1** Copia fuera de la empresa «*Backup Offsite*»

# SW Actualizado, Antivirus y Firewall

## SW Actualizado

Actualizaciones Automáticas

SW desactualizado es un peligro

No instalar nunca SW Pirata o de fuentes no fiables

## Antivirus

Siempre Activado

Protege tu información de SW malware, sitios web maliciosos y amenazas

Avast
Avira
safer-networking.org

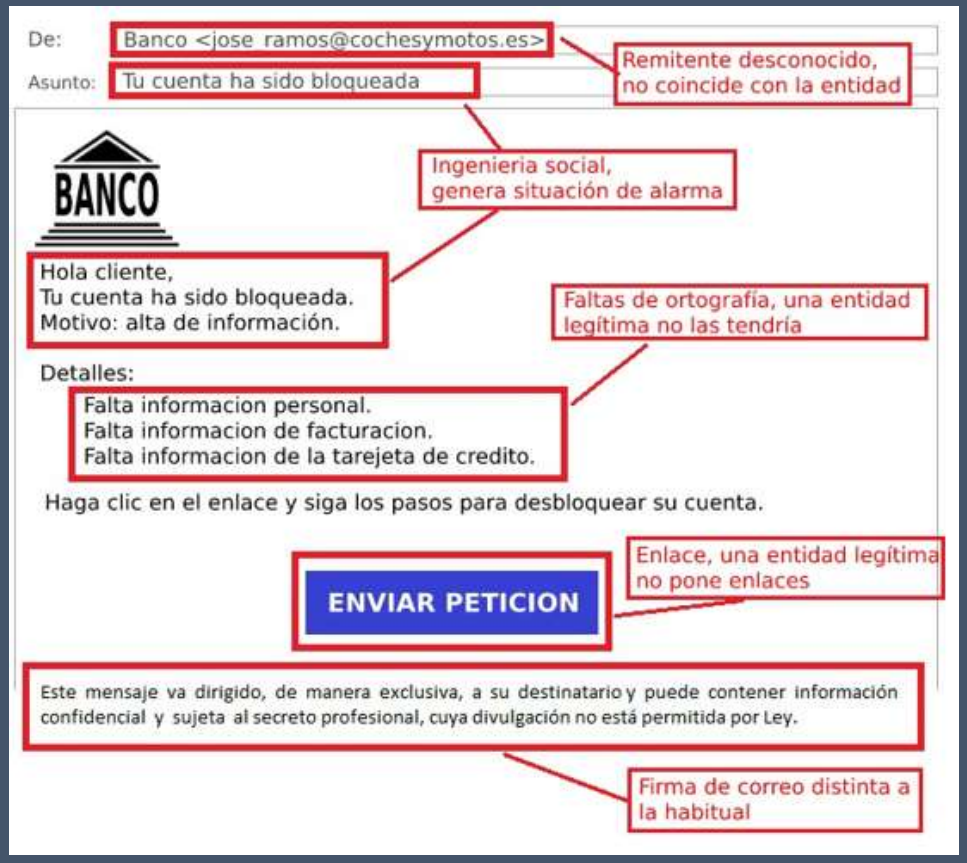
## Firewall

Siempre Activado

Controlar tráfico desde y hacia Internet

Evita que el malware pueda comunicarse con el exterior y que ataques desde Internet sean bloqueados

# ¿Cómo detectar correos fraudulentos?




- Sospechar de remitentes desconocidos
- Revisar cada carácter
- Estar atentos ante cambios de la firma
- Generan alerta o urgencia para hacer una acción (ingeniería social)
- Comunicaciones impersonales
- Mala redacción (Faltas de ortografía o expresiones no habituales)
- Ante cualquier adjunto, extremas precauciones
- Entidades legítimas no suelen enviar adjuntos
- Extensiones especialmente peligrosas:
  - .exe - .vbs - .docm - .xlsm - .pptm
- Ante cualquier duda, nunca descargar ni ejecutar el archivo
- Enlaces falseados pretenden redirigir a web fraudulenta (*Cybersquatting)*

# Metadatos, Riesgos y cómo Eliminarlos

**Metadato:** Es aquella información que incluyen los ficheros digitales pero que no forma parte del contenido, como por ejemplo fechas de creación o modificación, autor del fichero o ubicación GPS

Es información que puede ser utilizada por los ciberdelincuentes


Debemos eliminar metadatos antes de compartir ficheros

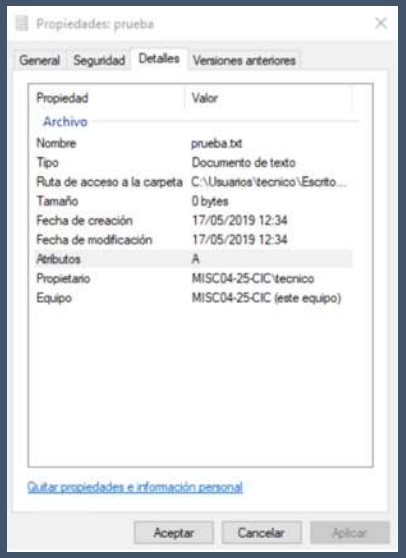
Eliminación posible desde *software* ofimática o SO como Windows:

**Botón derecho →**

**Propiedades →**

**Detalles →**

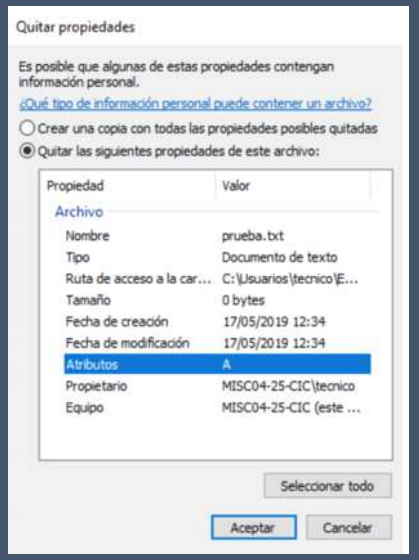
**Quitar propiedades e información personal →**




**Quitar las siguientes propiedades de este archivo →**

**Seleccionar todo →**

**Aceptar**



# Cifrado de Datos – PGP (Pretty Good Privacy)

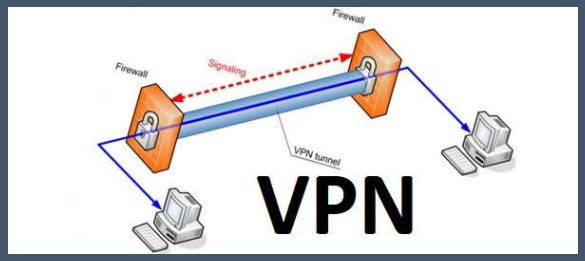
El cifrado de datos mediante PGP se puede aplicar a cualquier elemento digital: mensajería, comunicaciones, todo tipo de archivos, y documentos. Puede ser utilizado para firmar digitalmente un mensaje y que pueda verificarse el remitente como autentico

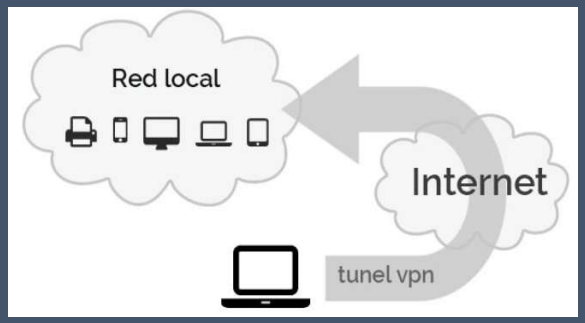

**Gpg4win** es una suite de **software libre para Windows**

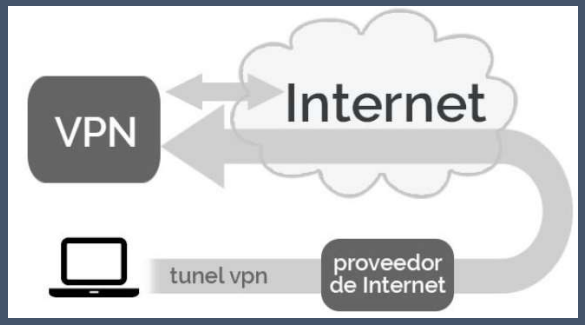
- **GnuPG**, la herramienta de encriptación principal
- **Kleopatra**, un gestor de certificados OpenPGP y X.509
- **GPA**, un gestor alternativo de certificados OpenPGP y X.509
- **GpgOL**, un plugin para Microsoft Outlook para cifrar emails
- **GpgEX**, un plugin para Microsoft Internet Explorer para cifrar archivos

# VPN – Virtual Private Network

Una red privada virtual capaz de conectar varios dispositivos como si se encontrasen físicamente en el mismo lugar




**Una VPN es parte de una red corporativa:**

- Es un elemento sensible al formar parte del perímetro corporativo, pero NO protege al endpoint (dispositivo) de otros ataques.
- Podría ser utilizado como puerta de entrada a la empresa de manera ilegítima.
- Si conectamos nuestro ordenador de trabajo, con información sensible, a una red Wifi, estamos compartiendo la red con otros dispositivos no controlados por políticas corporativas.
- Si uno de estos dispositivos es atacado, se puede comprometer también la VPN corporativa y por ende, abrir la puerta de entrada a la red de la empresa.

# Redes WiFi – Populares pero inseguras. ¿Qué podemos hacer?

humalia
Solutions

## Bastionado del Router

Cambiar nombre por defecto de la red WiFi

Cambiar la contraseña de la red WiFi y que sea segura

Cambiar la contraseña por defecto de acceso al router.

Filtrado MAC?

Ocultar red WiFi?

## WiFi Segura

wefender

**Tecteco.com**

# Gracias!


Oscar Jimenez
ojimenez@humalia.es
www.humalia.es