





Concienciación en Ciberseguridad y Buenas Prácticas

JORNADA Informativa: Programa de Ayuda Ciberseguridad



Unión Europea

Fondo Europeo
de Desarrollo Regional
"Una manera de hacer Europa"



Cámara
Granada

Sobre mí



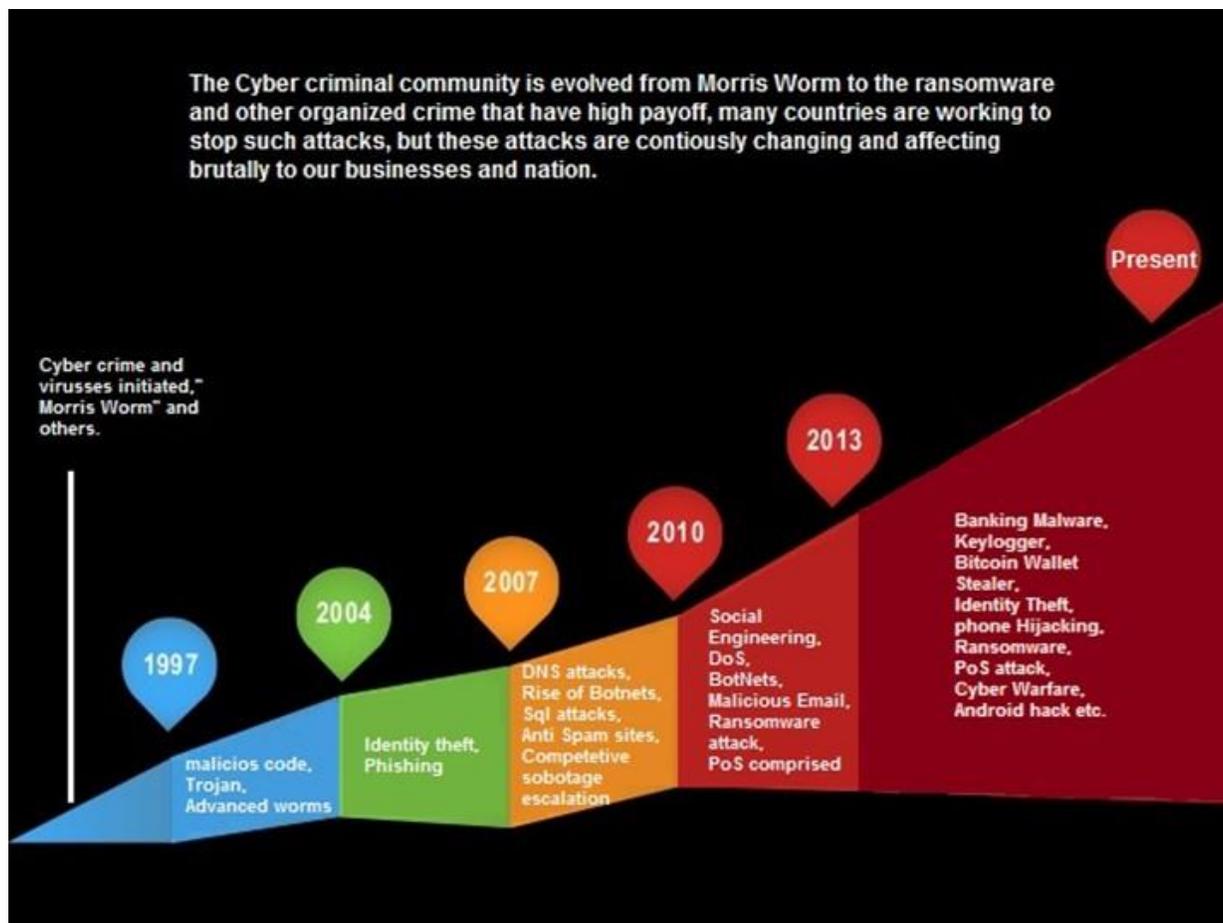
- ❑ **Javier Tallón**
- ❑ Ingeniero en Informática (Universidad de Granada)
- ❑ Co-Fundador & Director Técnico en **jtsec Beyond IT Security S.L.**
- ❑ Full-stack ~~hacker~~ wannabe
- ❑ Experto en Common Criteria, PCI-PTS, FIPS 140-2, ISO 27K1, SOC2
- ❑ Profesor del Máster de Ciberseguridad en la Universidad de Granada
- ❑ Certificado en CISSP & OSCP
- ❑ Miembro del grupo de trabajo Ad-hoc SOG-IS en la Agencia Europea de Ciberseguridad ENISA

Concienciación en Ciberseguridad

- ❑ Los sistemas TIC son fundamentales para el funcionamiento de la empresa
- ❑ Almacenamos y usamos información valiosa, servicios críticos y sistemas de alto valor económico
- ❑ ¿Estamos preparados para defendernos de un ciberataque?
- ❑ ¿Sabemos que probablemente seamos objetivo de un ciberataque?

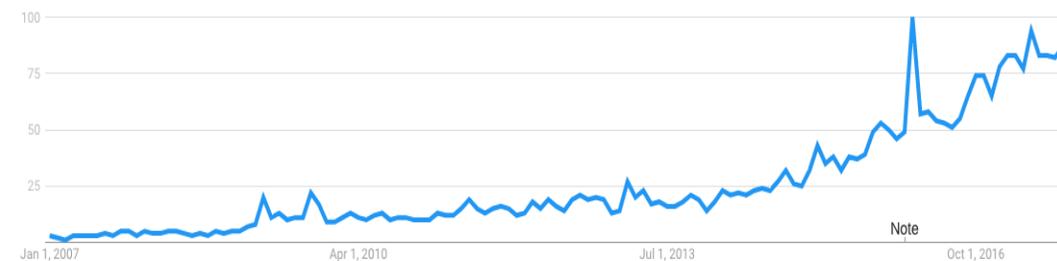


Evolución histórica de las ciberamenazas

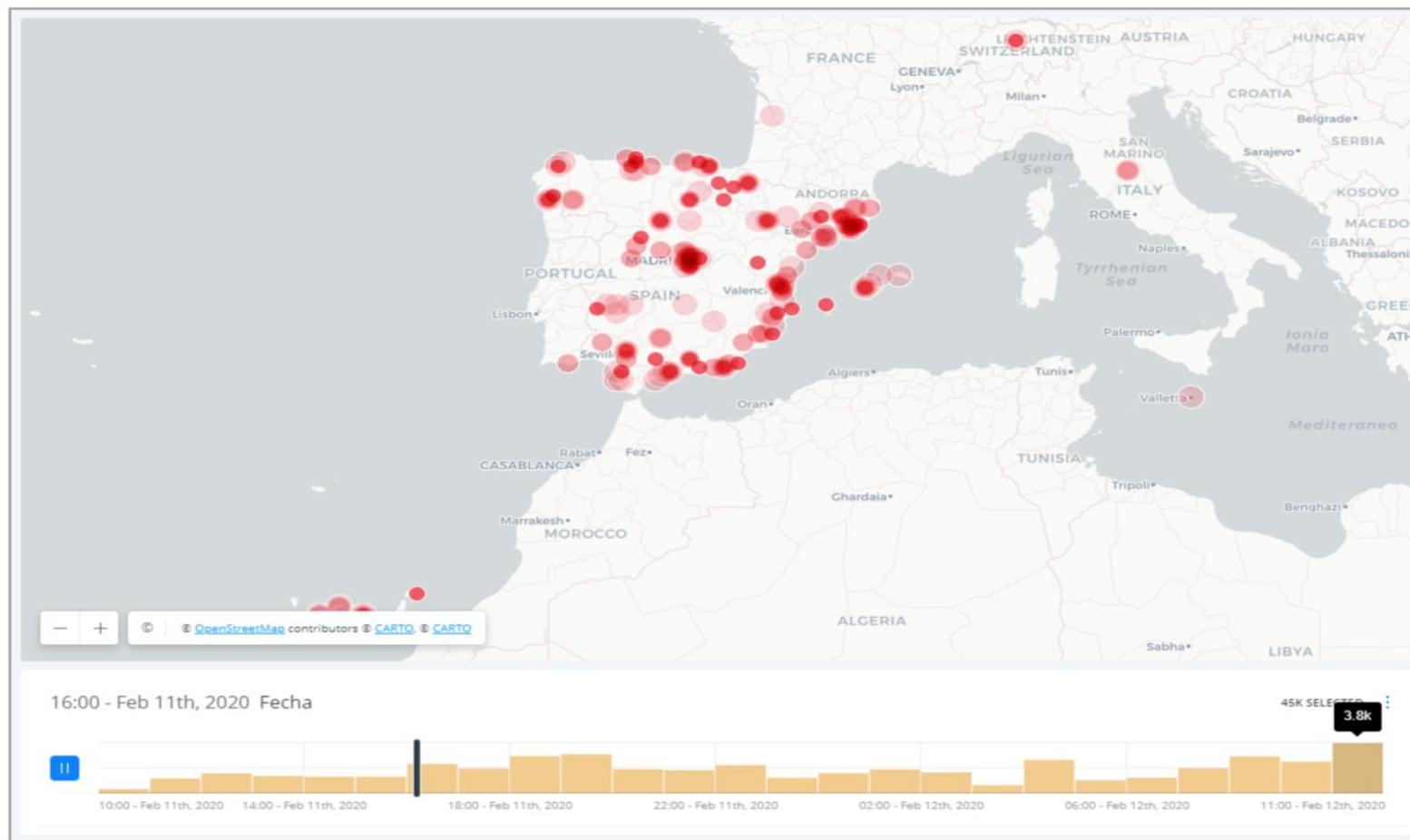


A medida que los atacantes han ido evolucionando y depurando sus métodos, se han desarrollado nuevas defensas y sobre todo concienciación global.

Interest over time ?



¿Puede ocurrirle a mi empresa?



INCIBE registra decenas de ataques diarios a sistemas ligados a la administración.

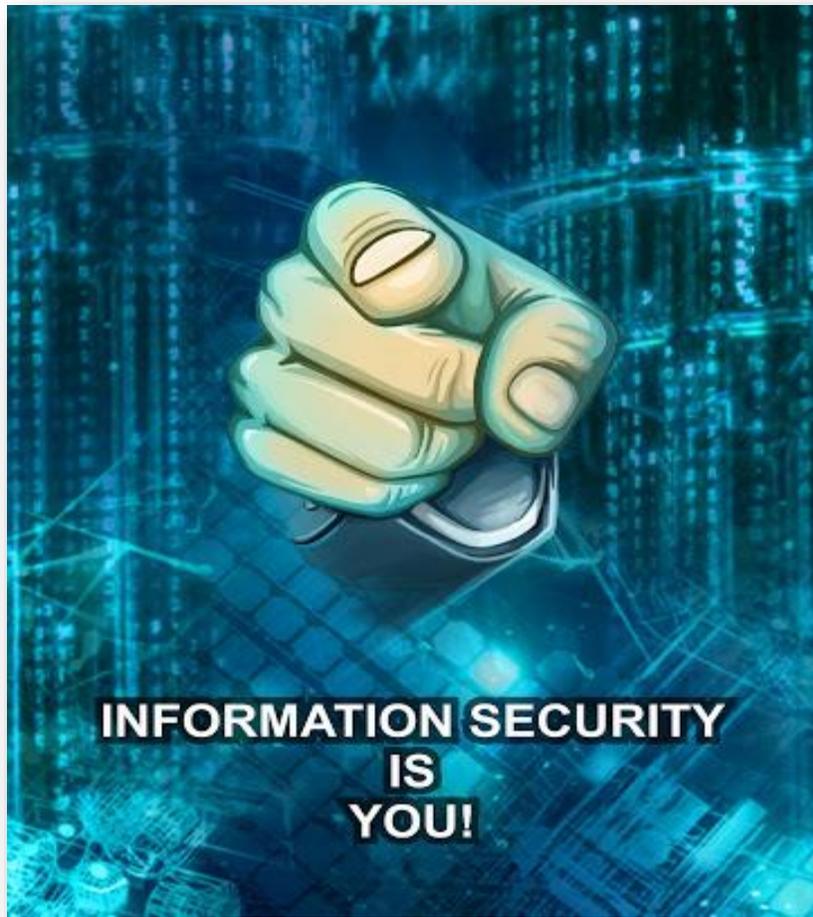
Los ataques a la mayoría de entidades privadas no se contabilizan.

Cómo afectan los ciberataques a las empresas

- ❑ El **43%** de los ciberataques tienen como objetivo empresas pequeñas o medianas
- ❑ El **coste medio** de filtraciones de datos en 2020 será superior a 150 millones de dólares
- ❑ Las compañías tardan unos **seis meses** en **detectar** una brecha de datos (incluso grandes compañías)
- ❑ El **precio de las acciones** cae un 7% de media después de una brecha de datos.



Cómo ganar concienciación en Ciberseguridad



- ❑ Conocer nuestra información y sistemas IT
 - Qué debo proteger y cuánto valor tiene
 - Cuántos recursos emplear en proteger
 - Nuestros puntos fuertes
 - Nuestros puntos débiles
- ❑ Quiénes son nuestros **enemigos**
- ❑ Quiénes son nuestros **aliados**
- ❑ ACTUAR mediante buenas prácticas

¿Qué debo proteger?



INFORMACIÓN

Propiedad intelectual
Datos de clientes
Datos bancarios
Datos de negocio
Información privilegiada



SERVICIOS

Páginas web
Correo electrónico
Comercio online
Portales de cliente
Servicios internos



SISTEMAS IT

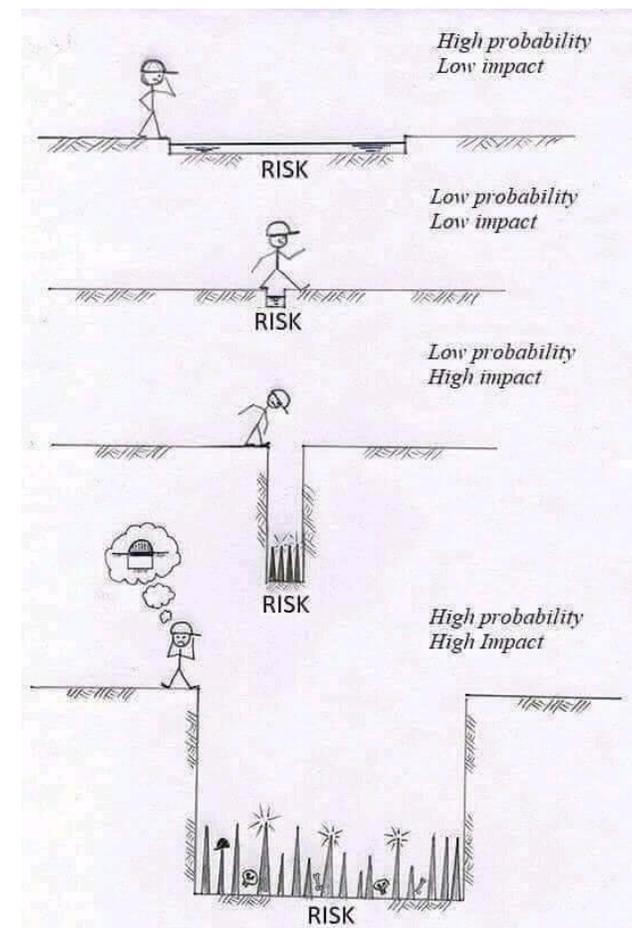
Servidores web
Portátiles y móviles
Equipamiento de red
Webcams
CPDs

ACTIVOS DE LA EMPRESA

¿Cuánto invertir en proteger la seguridad?

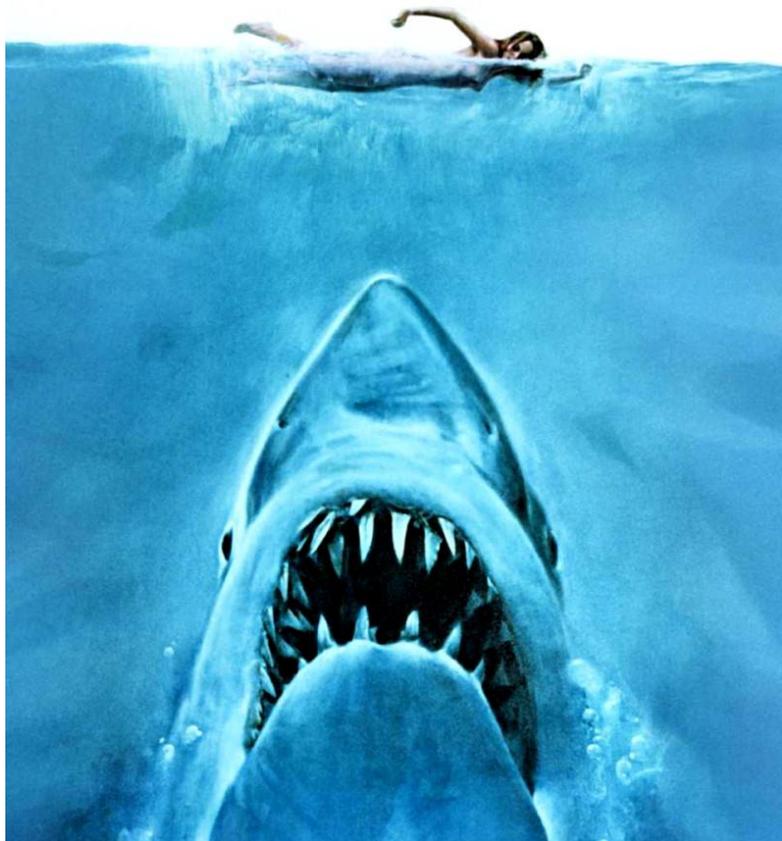
- ❑ Según el **valor** de los activos a proteger, según:
 - ❑ Impacto: ¿qué ocurre si se compromete?
 - ❑ Probabilidad: ¿cómo de probable?

- ❑ **Regla general:** la inversión en ciberseguridad debería ser equivalente a la inversión en seguridad física.



Nuestros puntos débiles

No ser conscientes del peligro



No estar preparados para defendernos



El factor humano es el eslabón más débil



Nuestros puntos fuertes

- ❑ Contamos con **más información y recursos formativos** que nunca...
 - ❑ Para personal técnico encargado de la protección
 - ❑ Para la concienciación de los usuarios
- ❑ Canales de avisos de ciberseguridad
- ❑ Gran cantidad de herramientas gratuitas

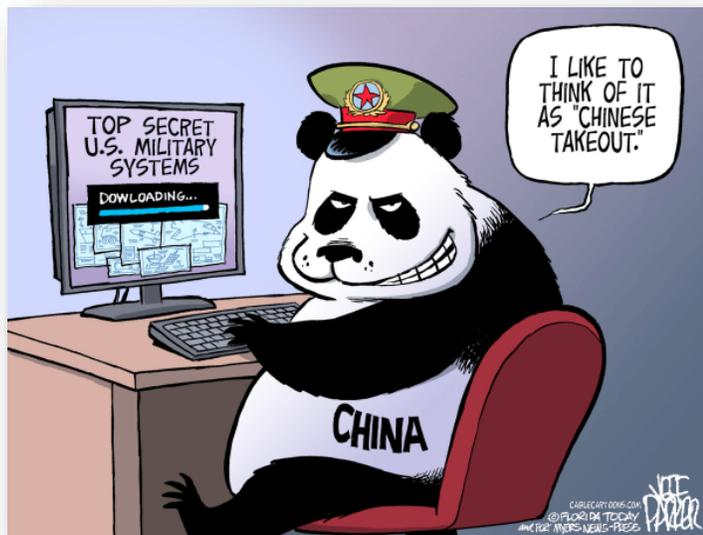


Conocer al enemigo

¿Quiénes son?

Ciberespías

- Roban información para vender a competidores
- Alta capacitación técnica
- Ligados a organizaciones o gobiernos



Cibercriminales

- Cometen ciberdelito y fraude para obtener beneficios económicos
- Organizados o en solitario
- A veces ligados a movimientos ideológicos



Conocer al enemigo

¿Qué quieren de nosotros?



Nuestra
información

ROBAR



Secretos industriales, Propiedad intelectual
Datos de clientes
Información de mercado o negocio
Nuestras cuentas bancarias

SECUESTRAR



Cifrar y pedir un rescate a cambio de la clave

FILTRAR



Generar pérdida de imagen y de reputación
Generar problemas legales y económicos

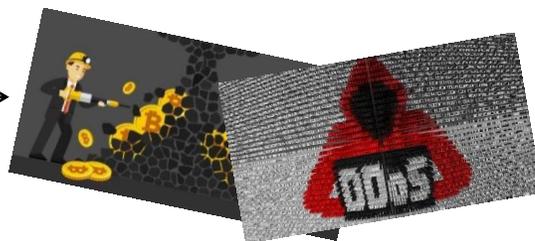
Conocer al enemigo

¿Qué quieren de nosotros?



**Nuestros sistemas
y servicios**

USO ILÍCITO



Minado de criptodivisas
Cyberataques desde nuestros equipos

INTERRUMPIR



Interrumpir los servicios al público
Generar perjuicio a clientes y a empresa
Deteriorar la imagen de la empresa

Conocer al enemigo

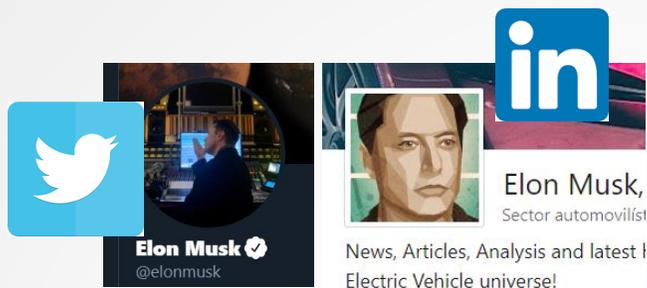
¿Cómo nos atacan?



- Existen multitud de métodos y vectores de ataque
- Es difícil protegerse de todos.
- Pero unos pocos son:
 - Los más **comunes**
 - Los más **efectivos**
 - Los más **conocidos**

Spear phishing a través de e-mail

El 75% de los ataques son a través de spear phishing a través de correo electrónico.



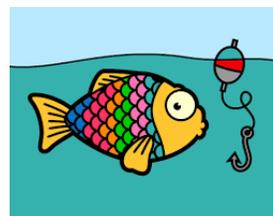
Se estudia a la víctima: su trabajo, sus proveedores, sus intereses, sus aficiones..



Se diseña un e-mail para que parezca de un tercero confiable: su banco, su teleoperadora, Google...



Nos urge a resolver un problema: fondos, password cambiado...
Contiene campos y un enlace para robar credenciales, instalar malware...



El usuario ¿hace click?

Ataques a sistemas desactualizados

Los sistemas desactualizados contienen **vulnerabilidades públicas fácilmente explotables**



Sistemas accesibles desde el exterior



Webs con CMS y sus plugins



Sistemas internos desactualizados



Aplicaciones de uso común



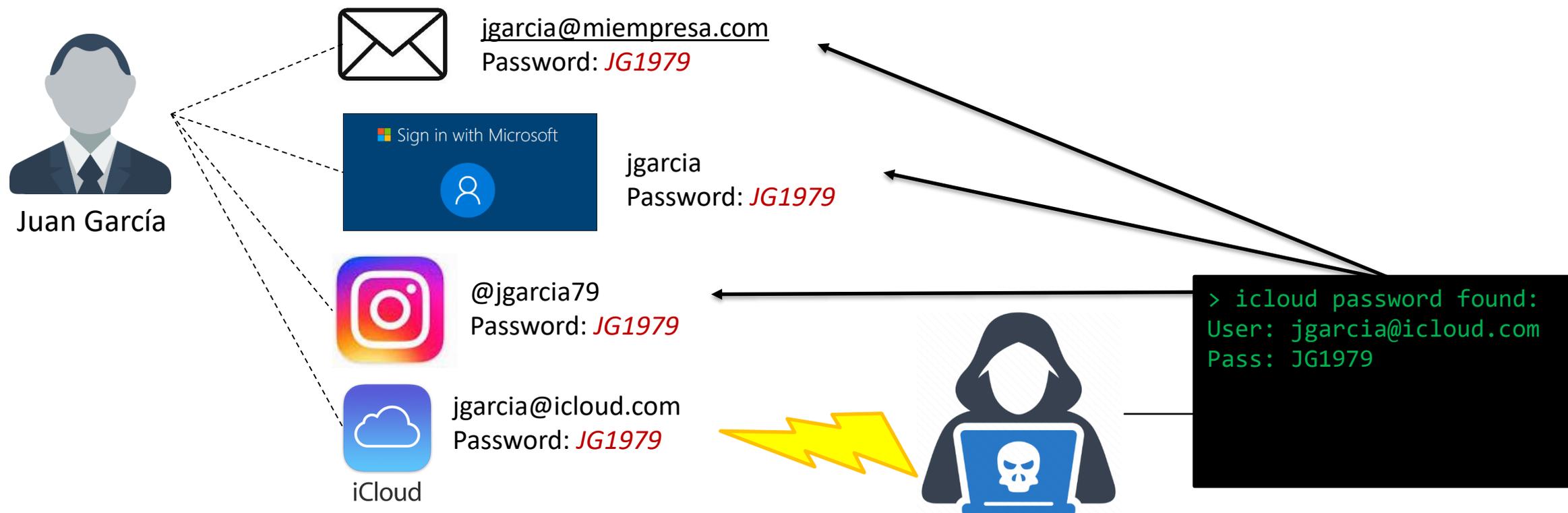
Hardware con firmware vulnerable



Uso de librerías vulnerables

Ataques a contraseñas inseguras

- ❑ Una contraseña corta, sencilla o deducible es **INSEGURA**
- ❑ Una contraseña **reutilizada** es **INSEGURA^N** (N = número de servicios donde se usa)



¿Y si el enemigo está en casa?

- Usuarios:**
 - Poco formados
 - Poco prudentes, vulnerables a ingeniería social
 - Con demasiados permisos de acceso

- Administradores de sistemas:**
 - Poco formados en seguridad

- Directiva:**
 - Se consideran por encima de la seguridad
 - ¿Proporcionan los recursos necesarios para proteger?
 - ¿Promueven la cultura de seguridad en la empresa?
 - ¿Promueven auditorías de seguridad?



Conocer a nuestros amigos

- ❑ No solo existen **multitud de recursos** formativos online

- ❑ También existen **entidades públicas y privadas** que publican abundantes recursos para formación, concienciación, detección y solución
 - **INCIBE** – boletines de noticias, blogs, artículos, guías de seguridad.
 - Línea de atención **017** ante incidentes de ciberseguridad
 - **AEPD** – Guías para implementar protección de datos personales
 - **nomoreransom.org** – Ayuda a recuperarse de ataques de ransomware conocidos.
 - **haveibeenpwned.com** – Comprobar si nuestra clave de e-mail ha sido filtrada



NO MORE RANSOM!

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Conocer a nuestros amigos

Recurrir a **profesionales** que nos ayuden a evaluar y mejorar la seguridad de nuestros sistemas

- ❑ **Auditorías de seguridad** (tests de intrusión).
 - ❑ Expertos en seguridad realizan pruebas de penetración para comprobar si un atacante podría entrar con éxito en nuestros sistemas.
 - ❑ Evalúan la seguridad a nivel técnico, a nivel humano (ingeniería social) y a nivel de gestión de la seguridad.
 - ❑ Identifican los problemas, proponen soluciones y forman al personal.
- ❑ **Consultoría de seguridad.**
 - ❑ Profesionales que ayudan a diseñar una arquitectura segura y líneas de defensa adecuadas.



Buenas prácticas en ciberseguridad

La concienciación debe ponerse en práctica para protegernos de los ciberdelincuentes y las amenazas



Presentaremos un decálogo de buenas prácticas en ciberseguridad que nos ayudará a mantener nuestros sistemas y su información seguros

Decálogo de buenas prácticas en ciberseguridad

1. Implantar la cultura de la ciberseguridad en la empresa

- La directiva debe promover la ciberseguridad
- Fomentar la formación y concienciación
- Desarrollar políticas, normativas y procedimientos de seguridad
- La ciberseguridad debe tomarse como una inversión
- Estar al día: boletines de noticias, avisos INCIBE
- Diseñar plan de recuperación ante ataques



Decálogo de buenas prácticas en ciberseguridad

2. No abrir enlaces ni descargar ficheros sospechosos



- El phishing se evita con precaución
- Evitar abrir adjuntos en correos, pueden contener virus
- Revisar dominio del remitente en los correos
- Revisar URL de los enlaces en los correos
- Nunca introducir nuestras credenciales en enlaces recibidos
- Ante la duda, consultar con el personal de IT

Decálogo de buenas prácticas en ciberseguridad

3. Utilizar software y hardware de seguridad



- Antivirus instalado y actualizado en todos los equipos
- Protección en tiempo real activada
- Escanear ficheros descargados
- Utilizar un cortafuegos para la salida a internet

Decálogo de buenas prácticas en ciberseguridad

4. Utilizar contraseñas seguras

- Más larga = más segura (mínimo 10)
- Combinar números, mayúsculas, minúsculas y símbolos
- Mejor una frase que una palabra
- NO reutilizar contraseñas en varios sitios
- Cambiarlas periódicamente
- No recordar contraseñas en el navegador
- No introducirla en webs que miden la complejidad!



Decálogo de buenas prácticas en ciberseguridad

5. Limitar superficie de exposición



- Instalar sólo el software necesario
- No tener servicios innecesarios corriendo en servidores
- Limitar al mínimo necesario los permisos
- Si usas la nube para trabajar, elige una profesional y segura (Google Drive, Microsoft OneDrive...)
- No usar red WIFI si no es estrictamente necesario
- Desconectar tomas de red sin uso del switch

Decálogo de buenas prácticas en ciberseguridad

6. Cifrar información sensible y borrado seguro



- La información más crítica debería estar cifrada
- Los equipos portátiles de trabajo deben estar cifrados
- La información en discos extraíbles debe cifrarse
- Antes de tirar o reutilizar equipos, hacer borrado seguro

Decálogo de buenas prácticas en ciberseguridad

7. No usar software ilegal



- El software pirata descargado de internet suele contener malware
- El software pirata puede permitir acceso remoto al equipo
- No usar cracks ni keygens: suelen estar infectados
- El software ilegal termina en auditorías y multas económicas

Decálogo de buenas prácticas en ciberseguridad

8. Hacer copias de seguridad periódicas

- Si la información se borra por accidente, necesitas un backup
- Si un equipo se estropea, necesitas un backup
- Permiten recuperarse de un ataque Ransomware
- Muy recomendable almacenarlas en otra ubicación
- Muy recomendable almacenarlas cifradas
- Si guardas los backups en la nube, ¡almacénalos cifrados!



Decálogo de buenas prácticas en ciberseguridad

9. Mantener los sistemas actualizados



- Los sistemas desactualizados son vulnerables
- Las actualizaciones deben ser periódicas y programadas
- No ignorar avisos de actualizaciones!
- Prioridad:
 1. Antivirus
 2. Sistema operativo
 3. Aplicaciones

Decálogo de buenas prácticas en ciberseguridad

10. Revisiones periódicas - auditorías

- Revisar periódicamente el estado de la seguridad
- Revisar permisos de carpetas
- Revisar si hay usuarios obsoletos antiguos
- Realizar auditorías de seguridad (tests de intrusión) periódicamente



Un breve resumen

- ❑ La ciberseguridad es una inversión
- ❑ La ciberseguridad debe estar en la cultura de la empresa
- ❑ Formación y concienciación: conocer al enemigo para defendernos
- ❑ Usar el decálogo de buenas prácticas
- ❑ Contratar profesionales para auditar y mejorar nuestra seguridad



Contacto

jtsec Beyond IT Security

Granada / Madrid

hola@jtsec.es

@jtsecES

<https://www.linkedin.com/company/jtsec/>

<https://www.jtsec.es/es>



“Cualquier loco puede hacer que algo parezca complicado.
Se necesita un genio para hacerlo sencillo.”

Woody Guthrie