



# incibe emprende

Programa de Impulso a la Industria de la  
Ciberseguridad Nacional

#INCIBEemprende



**INCIBE Emprende** desarrolla iniciativas de **ideación, incubación y aceleración** tanto para la promoción del emprendimiento en ciberseguridad, como de la ciberseguridad en el emprendimiento de base tecnológica, con el fin de **Impulsar la Industria Nacional de Ciberseguridad**.

- ◆ **Acompañamos** a emprendedores y start-ups españolas de **ciberseguridad, así como de base tecnológica** para la integración de la ciberseguridad en su proyecto.
- ◆ **Impulsamos el desarrollo de proyectos** independientemente de su grado de madurez: fomento de ideas - incubación de proyectos - aceleración de start-ups e internacionalización.
- ◆ Impulsamos la **innovación** y promocionamos la atracción de **inversión** a la misma.

Plan de Recuperación, Transformación y Resiliencia (PRTR) a través del Componente 15. Inversión 7 Ciberseguridad: Fortalecimiento de las capacidades de ciudadanos, PYMES y profesionales e impulso del sector.

# Start-ups vs emprendimiento tradicional



- ◆ Empresas digitales/base tecnológica
- ◆ Explotación de nuevos modelos de negocio
- ◆ Modelo de negocio escalable: crecimiento exponencial en ventas y crecimiento lineal en costes
- ◆ Ventaja competitiva basada en la innovación
- ◆ Alto riesgo debido a su alto contenido innovador
- ◆ Necesidad de elevado volumen de financiación y dificultad de acceso a la misma en fases iniciales
- ◆ Fuentes de financiación FFF (family, fools and Friends), capital riesgo, business angels. La garantía la supone el equipo.
- ◆ Dependencia en captación y retención de empleados altamente cualificados.

VS



- ◆ Explotación de modelos de negocio convencionales
- ◆ Crecimiento estable, modelo de negocio sostenible
- ◆ Fuente de financiación tradicional: préstamos y recursos propios. Garantía real y/o personal.
- ◆ Centrada en mantener el negocio y/o generar un crecimiento % estable.

# Sector de la ciberseguridad

SECTOR  
EN AUGE

**122.284**

Trabajadores empleados  
(2021)

**24.119**

Brecha de talento  
(2021)

**83.000**

Brecha de talento  
(2024)

## VALOR ECOSISTEMA\*



\*Fuente: Security Spending Guide IDC 2021



Participación mundial en la industria de ciberseguridad

**31% 69%**



Participación estudiantes grados STEM

**24% 76%**



Participación estudiantes cursos ciberseguridad

**18% 82%**

# Sector de la ciberseguridad



## Ciberseguridad

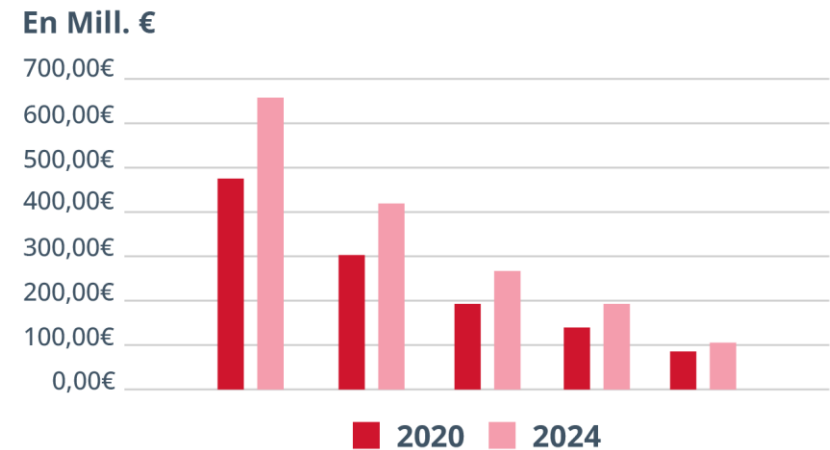
La importancia de la ciberseguridad es **transversal** a todos los sectores de la economía



## Digitalización sectores

La digitalización de todos los sectores está favoreciendo un **crecimiento global del mercado de la Ciberseguridad**

Tamaño mercado de la ciberseguridad por sectores 2020/2024)\*



El sector que más peso aporta a la ciberseguridad es el de **distribución y servicios**, seguido del **financiero**

\*Fuente: Security Spending Guide IDC 2021

# Programa de apoyo al Emprendimiento en ciberseguridad



## incibe emprende 2023-2026

### Captación / Ideación

Charlas  
Talleres  
Eventos

### Incubación

Formación  
Mentorización  
Asesoramiento legal  
Asesor fiscal  
Visita al ecosistema regional  
Demo Day

### Aceleración

Formación  
Mentorización  
Asesoramiento legal  
Asesor fiscal  
Visita al ecosistema regional  
Demo Day  
Aceleración Express



# Agenda y metodología

1. **Presentación personal**
2. **Regulación de la ciberseguridad y ecosistema**
3. **Amenazas y Riesgos**
4. **La Dark Web**
5. **Medidas y buenas prácticas de seguridad para startups**
6. **Gestión de incidentes**
7. **Cibervigilancia. Herramientas OSINT (Wiktor Nykiel)**
8. **Implantar un sistema de monitorización propio (Wiktor Nykiel)**
9. **Desarrollo y despliegue seguro de aplicaciones (Antonio Reche)**
10. **Ciberdelitos (Policía)**



# Presentación personal (Juanjo)



- Ingeniero en Informática. Máster en ciberseguridad y auditoría de sistemas. CISA, CISM...
- Autor de los primeros antivirus (gratuitos) en España a finales de los 80, principios de los 90.
- Autor de los primeros libros sobre seguridad informática (editorial Paraninfo).
- Director del Máster Universitario en Ciberseguridad de UNIE Universidad (Grupo Planeta)
- Coordinador académico del Curso superior en dirección de seguridad digital y gestión de crisis de la Alianza Española de seguridad y Crisis y la Universidad de Alcalá de Henares
- Coordinador del curso de ciberseguridad para Consejeros de aesYc.
- Secretario de la Junta Directiva del capítulo de Madrid de la Asociación de Auditoría y Control de los Sistemas de Información (ISACA) y vocal de la Junta Directiva de la Asociación de Autores Científico Técnico y Académicos.
- Más de 50 colaboraciones con medios de comunicación (TV, radio, prensa).
- Ponente y moderador en múltiples eventos sobre ciberseguridad.
- Autor de numerosos artículos sobre seguridad informática.
- Más de 30 años de experiencia en TIC y ciberseguridad desarrollados en empresas multinacionales como AT&T, Lucent Technologies Bell Labs, Secartis, Giesecke & Devrient Mobile Security, Universidad Internacional de La Rioja (UNIR) y Grupo Proeduca.
- Ha sido director de ciberseguridad global (CISO) del grupo Proeduca, empresa con más de siete mil empleados en ocho países, director de área en la Universidad Internacional de La Rioja y responsable de sistemas IT del área industrial en AT&T y Lucent Technologies Bell Labs.
- Ha sido coordinador académico y profesor del Máster en ciberseguridad de la Universidad Internacional de La Rioja, y profesor del Máster en Gobierno de la Ciberseguridad de la Universidad Politécnica de Madrid e ISMS Forum y del Máster de Seguridad de la Información de la Universidad Pontificia de Salamanca.
- Coautor de una patente sobre Blockchain y líder de un proyecto sobre autenticación móvil ganador de un challenge internacional en el Mobile World Congress (MWC).
- Medalla al mérito en la Ciberdefensa en 2024 por PETEC en el Centro Tecnológico de Seguridad de la Secretaría de Estado de Seguridad.
- Medalla por la colaboración en la lucha contra el Cibercrimen en 2018 por la policía de Colombia.





# Objetivos de los ciberdelincuentes

**LARAZÓN**

## Las PYMES son el objetivo del 70% de los cibertaqués en España

**CincoDías**

**Seis de cada diez pymes en Europa acaba cerrando cuando sufre un ciberataque**

El 66% de las organizaciones mundiales han sido atacadas mediante el robo de información

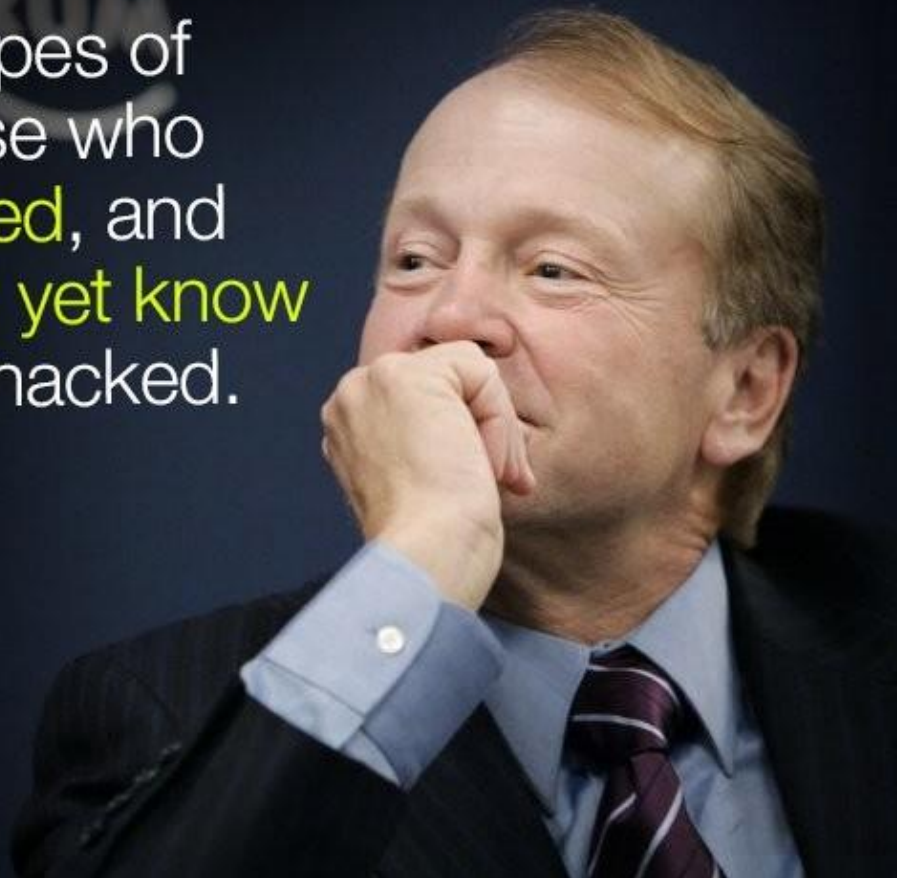
europapress / portaltic / ciberseguridad

El 60% de las pymes que sufren un ciberataque desaparece seis meses después, según Kaspersky Lab

# ¿Te han hackeado o no lo sabes?

There are two types of companies: those who **have been hacked**, and those who **don't yet know** they have been hacked.

John Chambers  
Chief Executive Officer of Cisco



# Los ciberataques van en aumento

ATAQUES INFORMÁTICOS >

## E Los ciberataques alcanzan su máximo histórico: “No hay nadie a salvo”

Las brechas sufridas por grandes empresas y organismos evidencian una actividad sin precedentes de los criminales, que aprovechan nuevas herramientas y vulnerabilidades

E ECONOMIA DIGITAL • El cibercrimen golpea a los grandes grupos del Ibex

### Ciberataques en Santander, Iberdrola, Telefónica y la DGT

M. JUSTE 1 JUN. 2024 - 18:49

- ➔ Un grupo de hackers ofrece los datos de clientes robados a Santander
- ➔ ¿Por qué están aumentando los casos de ciberataque en España?
- ➔ Iberdrola sufre un ciberataque que deja expuestos los datos de 850.000 clientes
- ➔ Telefónica investiga una supuesta filtración de datos de 120.000 clientes

En lo que va de año, han sufrido ciberataques muchas empresas y organismos públicos, desde ayuntamientos a las propias Fuerzas Armadas. Los últimos afectados son grandes compañías del Ibex35, como el Banco Santander, Telefónica o Iberdrola, además de la filial de la energética francesa TotalEnergies

LARAZÓN 25

Sociedad

EL TIEMPO SUCEOS RELIGIÓN

### Aumenta el mercado negro de datos médicos: un historial entre 30 y 900 euros

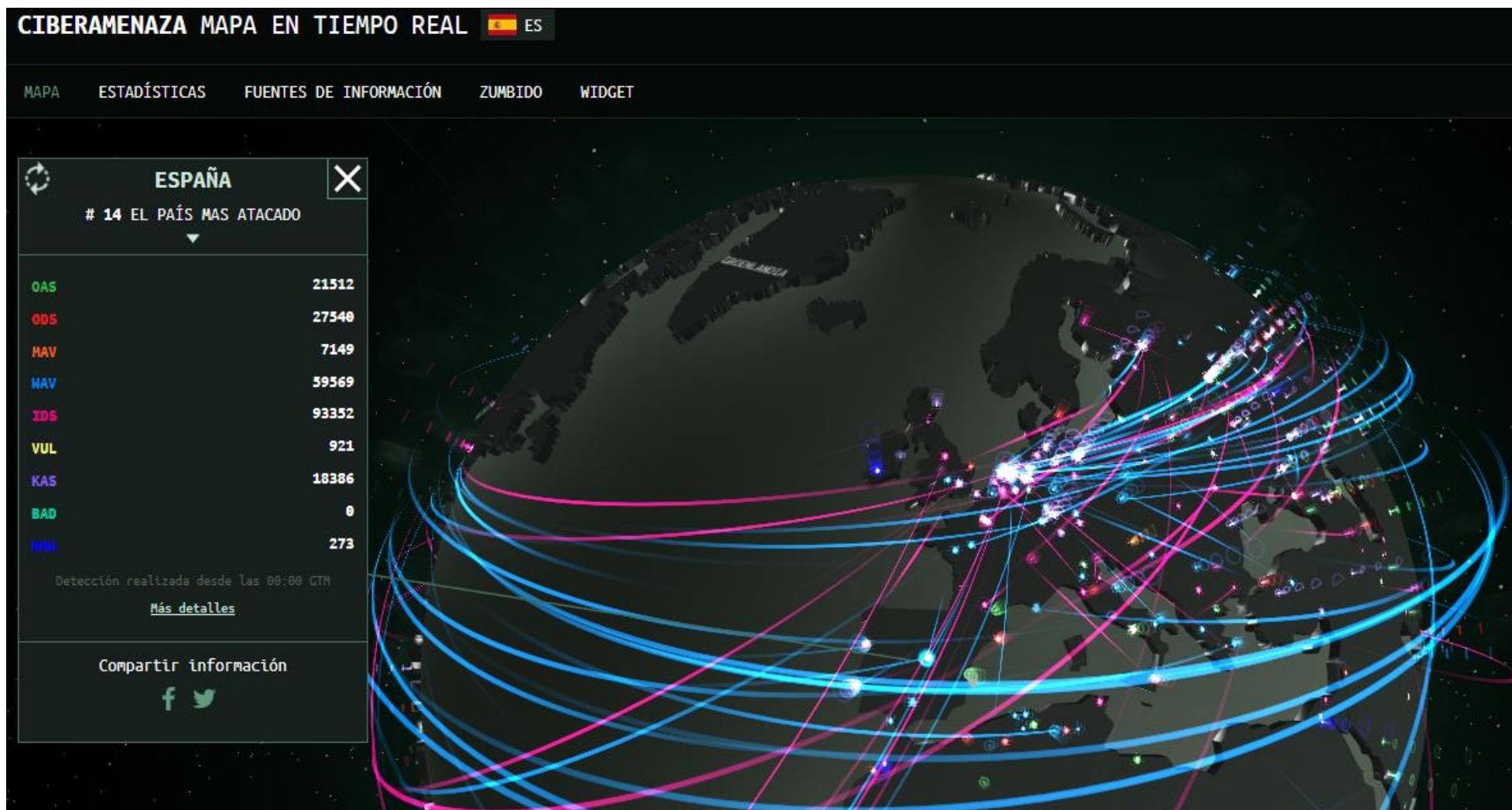
El sector salud registra más ciberataques que la banca. La información de salud puede ser empleada para la extorsión o el plagio de patentes.





# Mapa de cibeataques en tiempo real

<https://cybermap.kaspersky.com/special/ics/es>



# Datos económicos del cibercrimen



## El negocio del cibercrimen mueve ya 9,5 billones de dólares anuales



Por Vanesa García / 20 febrero, 2024

La empresa [Cybersecurity Ventures](#) estima que el cibercrimen manejará una suma considerable de 9,5 billones de dólares este año, y se espera que esta cifra aumente a 10,5 billones para el año 2025. Este dinero proviene del llamado «impuesto revolucionario» que las empresas pagan después de sufrir un ataque cibernético, un tipo de chantaje digital exigido por los cibercriminales tras perpetrar sus ataques.

elDiario.es

Hazte socio/a

Política Internacional Economía Opinión Cultura Clima Desalambre Igualdad Verteles Festival FIC

## La ciberdelincuencia gestiona un negocio oculto de 10,5 billones de dólares en 2023

Las empresas pagan al cibercrimen su propio impuesto revolucionario: este año, este cheque no nominativo superará el valor conjunto de los PIB de Japón, Alemania y España

## El cibercrimen mueve casi el doble de dinero que el tráfico de drogas, armas y trata de personas juntos

Seguridad 14 JUN 2023



Las organizaciones de ciberdelincuentes funcionan ya como cualquier otra empresa. De hecho, sus objetivos son los mismos: reducir costes, incrementar ingresos y mejorar la eficacia y la continuidad de negocio. El cibercrimen ha alcanzado un valor global cercano al 1,5% del PIB mundial.

## La ciberdelincuencia como servicio: el negocio ilegal de robar en Internet



El cibercrimen como servicio se puede utilizar para realizar una multitud de delitos cibernéticos. El **fraude financiero**, la ciberestafa, el **ciberataque de malware**, la denegación de servicio distribuido (DDoS), el ransomware, el phishing y la ingeniería social son sólo algunas de las posibilidades. La Ciberdelincuencia como Servicio (**CaaS** o **Cybercrime as a Service**) es un modelo de crimen organizado que venden sus herramientas, experiencia y servicios a otras personas en formatos que incluyen el **Ransomware como Servicio** (RaaS), el **Phishing como Servicio** (PhaaS) y el **Malware como Servicio** (MaaS).

# La web oscura (dark web)

- Cuando nos conectamos a Internet accedemos a sitios web indexados por motores de búsqueda tradicionales y de fácil acceso con cualquier navegador. Esto es solo la superficie.
- Debajo de esta superficie hay otras capas ocultas conocidas como la web profunda o **deep web** y la web oscura o **dark web** que no están indexadas (accesibles) por los motores de búsqueda. Para acceder a la información de los sitios de la deep web es necesario que nos den acceso.
- La dark web se utiliza comúnmente para comerciar ilegalmente con drogas, armas, etc. y también con contraseñas e información personal robada. Para acceder, es necesario un navegador especial como **Tor**. <https://www.torproject.org/es/download>
- Precios de credenciales, tarjetas y otros en la dark web: <https://www.privacyaffairs.com/dark-web-price-index-2023>



**La dark web, un negocio lucrativo para los ciberdelincuentes: este es el precio que ponen a nuestros datos**

Seguridad 27 JUL 2023



# DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN

# DIMENSIONES DE SEGURIDAD

---

- Salvaguardar la seguridad de los activos de información.

- CONFIDENCIALIDAD

- INTEGRIDAD

- DISPONIBILIDAD

# CIBERAMENAZAS

# PHISHING / SMISHING / VISHING

Multas - Sede Electrónica de la DGT <danifeld.1819969@studenti.uniroma1.it>  
Cco: Usted

Sáb 14/09/2024 16:52

## Pago Pendiente de Multa por Estacionamiento

Estimado Cliente

No hemos recibido su pago de 140€ por estacionamiento no autorizado. Por favor, realice el pago en menos de 24 horas para evitar recargos y acciones legales.

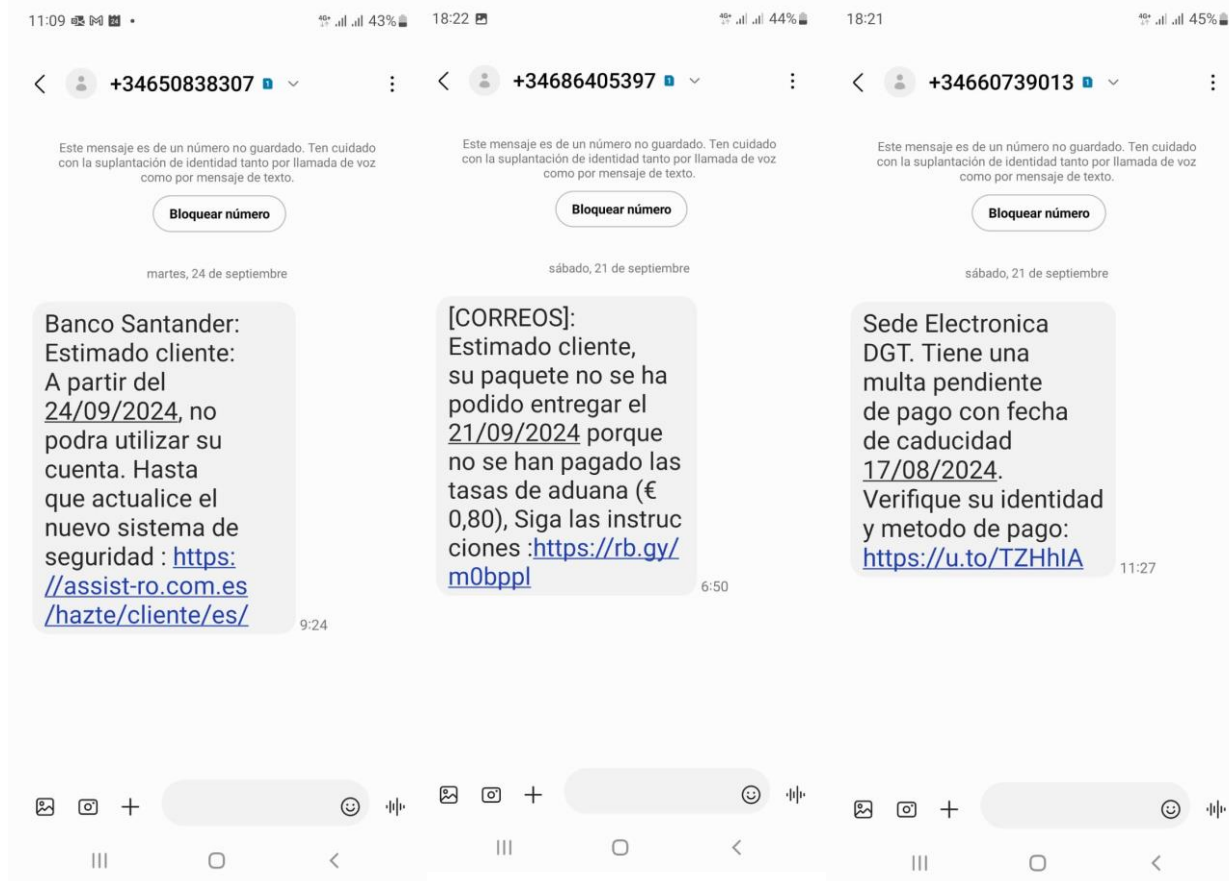
[Pague aquí](#)

Gracias por su pronta atención a este asunto.

Atentamente,

**D-G-T**

Este mensaje es generado automáticamente. Por favor, no responda a este correo.



# ROBO DE IDENTIDAD DIGITAL



- Consiste en la obtención de las credenciales de un usuario para suplantar su identidad digital, generalmente para cometer un fraude, robar información o perpetrar un ciberataque.
- **Consecuencias:** acceso a información confidencial, compras y pagos fraudulentos, introducción un malware en el equipo o en la red de la empresa, daños a la reputación de una empresa, etc.
- **Medidas:** una buena política de contraseñas y de control de acceso con la activación del segundo factor de autenticación.

# ROBO DE INFORMACIÓN



- Obtención de información con fines ilícitos.
- El atacante copia o duplica los datos por lo que es difícil detectar el robo.
- Los datos pueden ser robados del disco, de la nube o cuando son transmitidos por redes.
- Pueden robarnos datos individuales, archivos individuales, carpetas o el disco completo.
- Los objetivos principales son datos personales de clientes o empleados, historiales clínicos, patentes, código fuente, información financiera o estratégica, tarjetas de crédito, cuentas bancarias y contraseñas (robo de identidad).
- La información robada puede acabar siendo vendida en la **Dark Web**.
- Puede haber una exfiltración de datos desde dentro por un empleado desleal (**insider**)
- **Consecuencias:** sanciones AEPD, daños a la reputación, demandas de clientes, pérdida de ventaja competitiva, extorsión de ciberdelincuentes,
- **Medidas:** cifrado, mínimo privilegio, contraseñas robustas, segundo factor de autenticación.



# RANSOMWARE

- El ransomware es un tipo de ataque avanzado que se podría categorizar como malware y que toma por completo el control del equipo para:
  1. Robar todos los archivos a los que tengan acceso los ciberdelincuentes.
  2. Cifrar todos los archivos a los que hayan podido acceder (incluso copias de seguridad).
  3. Pedir dinero (rescate) a cambio de proporcionar la clave para descifrar los archivos (2)
  4. Pedir dinero para no hacer pública la información robada (1)
- Es el tipo de ciberataque más peligroso por sus consecuencias (alguna empresa ha cerrado)
- Los ciberdelincuentes pueden acceder aprovechando (explotando) una vulnerabilidad en algún servidor de Internet (p.e. por no estar actualizado), un puerto abierto, un correo con phishing con un enlace que redirige a un sitio infectado con malware, etc.
- **Medidas:** protección de la identidad y copias de seguridad actualizadas para restaurar los datos.

# CIBERATAQUE DE RANSOMWARE

Lo sentimos, la página web no está operativa en este momento



Universidad  
Católica de Valencia  
San Vicente Mártir

20minutos

VALENCIA

## La Universidad Católica de Valencia sufre un ataque informático: los datos personales han sido encriptados

EFE | NOTICIA | 01.10.2024 | 00:28H



- Por el momento, se desconoce si se ha hecho un uso indebido de la información filtrada.

La Universidad Católica de **Valencia** ha sufrido este lunes **un ataque informático en sus servidores** que ha cifrado información de datos identificativos y económicos, además de académica y profesional y detalles de empleo y datos de salud. Por ahora, se desconoce si se ha hecho ya un "uso indebido" de ellos. La institución denunciará este ataque ante la **Policía Nacional** y la **Agencia Española de Protección de Datos (AEPD)**, según ha anunciado en un comunicado.

En el mensaje, la entidad académica ha detallado que ha sufrido un ciberataque de **ransomware** en sus servidores. Se trata de **un código malicioso que ha cifrado información alojada en los mismos**. "Tan pronto como se ha tenido conocimiento, se ha reforzado la seguridad y la Universidad está trabajando con expertos en seguridad cibernética y autoridades competentes para abordar la situación, garantizar que se tomen todas las medidas necesarias para proteger la información de sus usuarios, contener el incidente y proteger los sistemas", ha añadido.

### Los hackers que atacaron a la Católica exigen un pago para liberar los datos bloqueados



Los datos encriptados incluyen detalles críticos para el funcionamiento diario de la universidad, como las **nóminas del personal, registros académicos y administrativos**, y probablemente información sobre **investigaciones** en curso. **Los teléfonos tampoco funcionaban**. La posible filtración o uso indebido de estos datos podría generar **consecuencias graves** para la universidad, tanto en términos de **reputación** como de posibles **sanciones regulatorias**.

Nuestros servidores han sufrido un ataque de *ransomware* y estamos trabajando para solucionar el problema lo antes posible.

Si le surge cualquier duda al respecto, puede ponerse en contacto con: [incidente.seg@ucv.es](mailto:incidente.seg@ucv.es) o con la Delegada de Protección de Datos: [dpd@ucv.es](mailto:dpd@ucv.es)

Recordamos que la docencia sigue su curso habitual, pudiendo entrar a la plataforma a través del siguiente enlace: <https://campusdocencia.ucv.es>

# MEDIDAS Y BUENAS PRÁCTICAS DE SEGURIDAD

# DECÁLOGO DE CIBERSEGURIDAD



# PLAN DIRECTOR DE SEGURIDAD

---



- Elaborar un plan de seguridad contemplando:
  - Medidas que se van a implantar.
  - Planificación.
  - Responsables.
  - Inversiones.

<https://www.incibe.es/empresas/que-te-interesa/plan-director-seguridad>

# POLÍTICAS DE SEGURIDAD



- Elaborar una política de seguridad que los empleados deben conocer y firmar para mostrar el compromiso de la dirección.
  - [www.incibe.es/empresas/herramientas/politicas](http://www.incibe.es/empresas/herramientas/politicas)
- Se puede empezar con un documento básico que se podrá ir mejorando a medida que la empresa crezca, asuma más riesgos y tenga que madurar en nivel de seguridad.
- En empresas más grandes, se debe designar un responsable de seguridad de la información (**CISO** por su acrónimo en inglés)
  - Si la PYME no puede permitirse tener una figura dedicada, este rol puede recaer en el responsable de sistemas / IT o externalizarlo en un tercero como un servicio.
  - A medida que la empresa crezca y tenga presupuesto, el rol debe ser dedicado o compaginado con DPD/DPO, **pero independiente de Sistemas y reportando directamente a la Dirección.**



# CULTURA DE SEGURIDAD

## FORMACIÓN Y CONCIENCIACIÓN

- Hay que capacitar regularmente a los empleados sobre los riesgos, procedimientos y las buenas prácticas de ciberseguridad.
- Asegurar que son conscientes de las amenazas del phishing, malware, ransomware, fraude del CEO, suplantación de la identidad profunda (deep fakes) mediante herramientas de Inteligencia Artificial generativa y otras amenazas.
- Dossier de INCIBE para desarrollar cultura en seguridad:
  - [https://www.incibe.es/sites/default/files/contenidos/dosieres/metad\\_desarrollar-cultura-en-seguridad.pdf](https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf)
- Existen multitud de recursos gratuitos que pueden facilitar el trabajo como el Kit de concienciación de INCIBE.
  - <https://www.incibe.es/empresas/formacion/kit-concienciacion>
  - [https://files.incibe.es/incibe/kit\\_concienciacion/kit\\_concienciacion.zip](https://files.incibe.es/incibe/kit_concienciacion/kit_concienciacion.zip)

**Sauron04**  
**Aragorn5**  
**Gollum06**  
**Gandalf7**  
**+Va1ePrev3nirQqrar!**

## EL TIEMPO QUE CUESTA UN HACKER PARA ROBAR TU CONTRASEÑA A TRAVÉS DE UN ATAQUE DE FUERZA BRUTA EN 2024

12 x RTX 4090 | bcrpt

Número de caracteres	Sólo numeros	Sólo minúsculas	Mayúsculas y minúsculas	Numeros, mayúsculas y minúsculas	Numeros, mayúsculas y minúsculas, y símbolos
4	Instantáneo	Instantáneo	3 segundos	6 segundos	9 segundos
5	Instantáneo	4 segundos	2 minutos	6 minutos	10 minutos
6	Instantáneo	2 minutos	2 horas	6 horas	12 horas
7	4 segundos	50 minutos	4 días	2 semanas	1 mes
8	37 segundos	22 horas	8 meses	3 años	7 años
9	6 minutos	3 semanas	33 años	161 años	479 años
10	1 hora	2 años	1000 años	9 mil años	33 mil años
11	10 horas	44 años	89 mil años	618 mil años	2 millón años
12	4 días	1 mil años	4 millón años	38 millón años	164 millón años
13	1 mes	29 mil años	241 millón años	2 mil millones años	11 mil millones años
14	1 año	766 mil años	12 mil millones años	147 mil millones años	805 mil millones años
15	12 años	19 millón años	652 mil millones años	9 billón años	56 billón años
16	119 años	517 millón años	33 billón años	566 billón años	3 mil billones años
17	1000 años	13 mil millones años	1 mil billones años	35 mil billones años	276 mil billones años
18	11 mil años	350 mil millones años	91 mil billones años	2 trillón años	19 trillón años

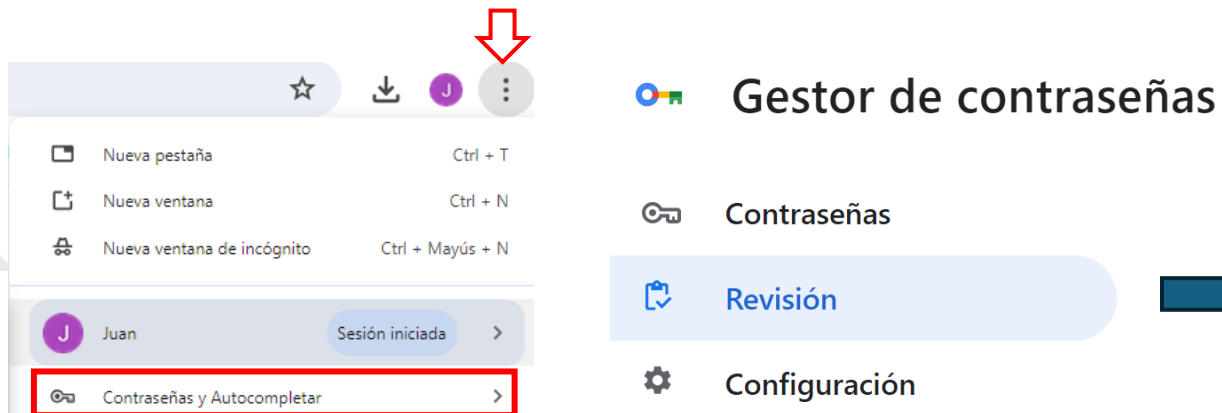
# CONTRASEÑAS Y CONTROL DE ACCESO



- Crear una política de contraseñas en la empresa de obligado cumplimiento para todos los empleados y colaboradores.
- Utilizar siempre contraseñas robustas y diferentes para cada sistema.
- Cómo crear una buena contraseña:
  - Un mínimo de **8 caracteres** combinando minúsculas, mayúsculas, números y caracteres especiales. Recomendado 12 caracteres.
  - Las de las cuentas privilegiadas como las de los administradores deben tener una **longitud mínima de 12**.
  - **No usar** palabras de diccionario ni **nombres de personas, personajes, mascotas o lugares** que puedan asociarse al usuario.
  - Una buena alternativa es usar frases de contraseña, que sean largas pero fáciles de recordar, como **"+Va1ePrev3nirQcurar!"**
- Cambiarlas regularmente (máximo 1 año). Mayor frecuencia las más importantes como las de administración o bancos.
- Evitar cuentas genéricas. Si fuesen necesarias, cambiar la contraseña cuando un usuario ya no la necesite o un empleado que la conozca cause baja en la empresa. Seguir siempre el principio de mínimo privilegio al asignar accesos.
- Para las contraseñas más sensibles, se desaconseja su almacenamiento en el navegador con la opción de autocompletar y sincronizarlas en la nube.
- Almacenarlas de forma segura en un **gestor de contraseñas** como alguno de los siguientes gratuitos poniendo una contraseña maestra robusta. Si se usa otro programa, comprobar su valoración y reputación.

# ALMACENAR CONTRASEÑAS EN EL NAVEGADOR

- Opción: Contraseñas y Autocompletar  
Chrome: <https://passwords.google.com>
- Buena opción para sugerir contraseñas seguras
- Muy cómodo, aunque no se recomienda para las contraseñas más sensibles.
- Solo para contraseñas de sitios web.
- Recomendación: revisar regularmente contraseñas reutilizadas y poco seguras.



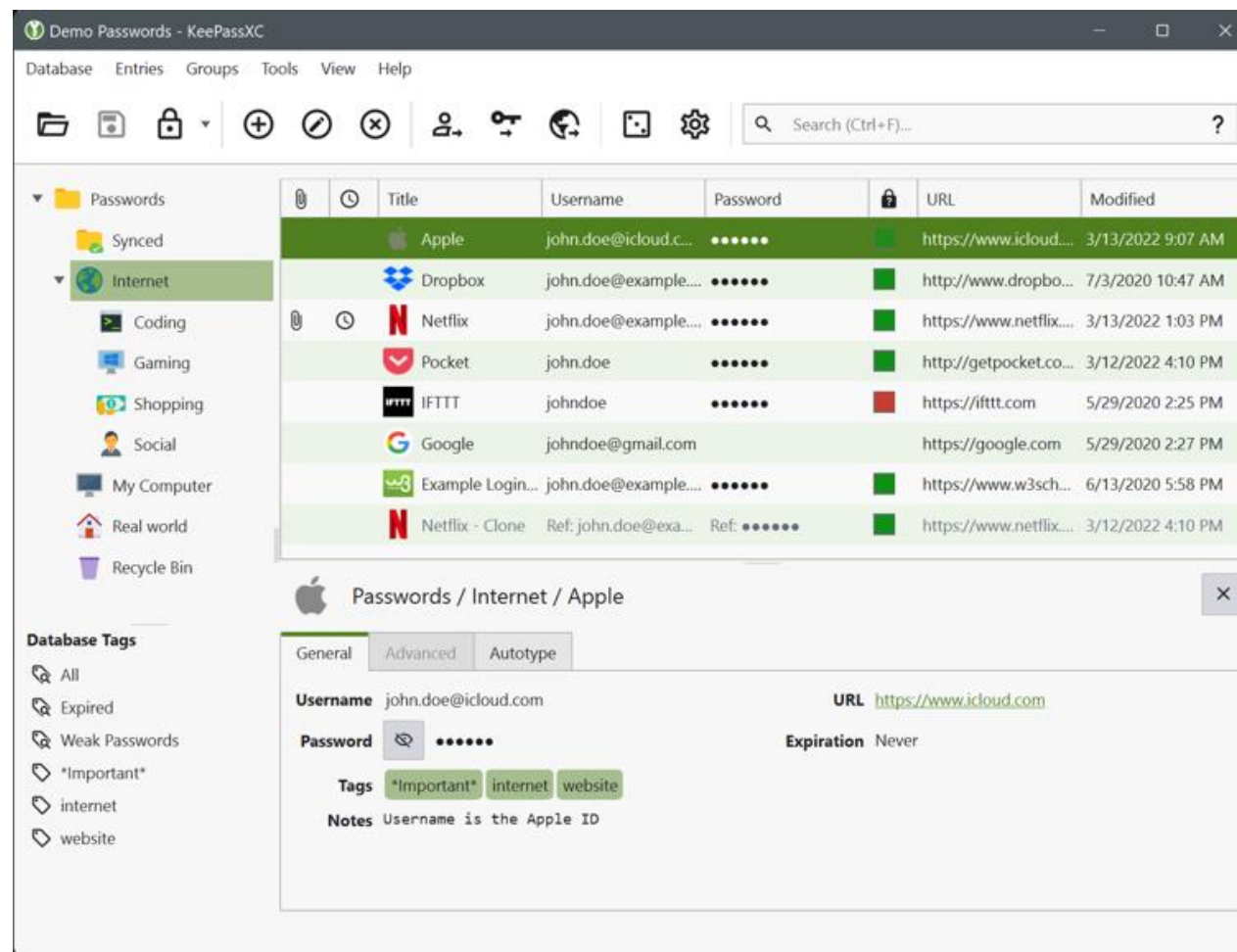
## Revisión de contraseñas

The screenshot shows the 'Revisión' screen of the Password Manager. At the top, it says 'Contraseñas de 263 sitios o aplicaciones comprobadas Justo ahora'. Below this, there are three status items:

- ✓ No hay contraseñas vulneradas  
Si se vulneran tus contraseñas, te avisaremos
- ! 63 contraseñas reutilizadas  
Crea contraseñas únicas
- ! 54 contraseñas poco seguras  
Crea contraseñas seguras

# GESTORES DE CONTRASEÑAS

[www.keepassxc.org](http://www.keepassxc.org)



Apps para móvil:

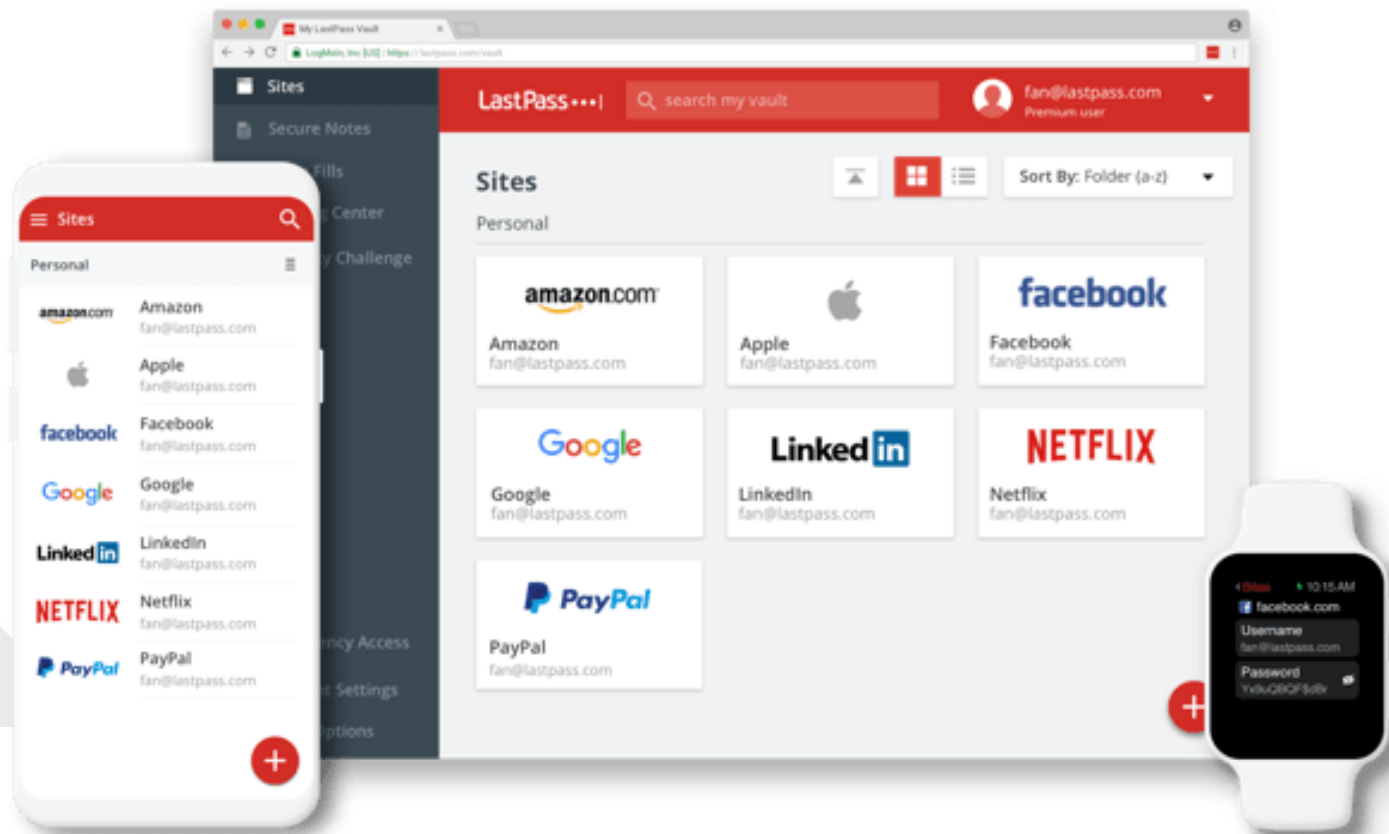
<https://play.google.com/store/apps/details?id=keepass2android.keepass2android&hl=es>

<https://play.google.com/store/apps/details?id=com.android.keepass>



# GESTORES DE CONTRASEÑAS

[www.lastpass.com](http://www.lastpass.com)



## Free

- Sin límite de contraseñas
- 1 cuenta de usuario
- Acceso desde 1 tipo de dispositivo
- Guardar y autocompletar contraseñas
- Uso compartido con una persona
- Inicio de sesión sin contraseñas
- Generador de contraseñas
- Panel de Seguridad
- Supervisión de Dark Web

## Families

Gestión segura de contraseñas para un máximo de 6 usuarios, con uso compartido de contraseñas sencillo e ilimitado.

€3.<sup>90</sup> al mes  
con pago anual\*

# COMPROBAR FILTRACIÓN DE CREDENCIALES



<https://haveibeenpwned.com>

A screenshot of the 'have i been pwned?' website. The main heading is '';--have i been pwned?'. Below it, the text says 'Check if your email address is in a data breach'. A search bar contains the email address 'mentor@clubdeemprendimiento.es' and a button labeled 'pwned?'. The result is 'Good news — no pwnage found!' with a sub-message: 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. The background is blue and green.

# HUELLA DIGITAL (Digital Footprint)

<https://www.malwarebytes.com/digital-footprint-app>

Has your personal data been exposed?

Scan your primary email to see your digital footprint.

cuentadecorreo@gmail.com

Scan Now

## Hallazgos sobre los usuarios:

- 60% tiene contraseñas expuestas
- 50% el nombre completo
- 40% la fecha de nacimiento
- 25% el teléfono

Malwarebytes

Hi Kate,  
Here's your Digital Footprint.

Be aware: this information is exposed to every hacker and scammer on the planet.  
Learn how to protect your identity.

Take another scan

My Exposed Location  
Oregon, USA  
IP address 67.169.210.236

My Device  
Mobile

My Email  
ros\*\*\*rett@yahoo.com Scanned

Exposed Password High Risk  
pon\*\*\*3910

Exposed Password High Risk  
pon\*\*\*3910

Date of birth  
21/03/1982

Breach  
AT&t 2024

7 Social Accounts

+ Try another

# PROTECCIÓN DE LA IDENTIDAD DIGITAL

- Algunos antivirus comerciales ofrecen la opción de monitorizar continuamente la filtración de nuestra información en la dark web.

## Añadir datos para supervisar

### Información más supervisada

**Tarjeta de crédito**  
0/10 bajo supervisión  
[+ Añadir](#)

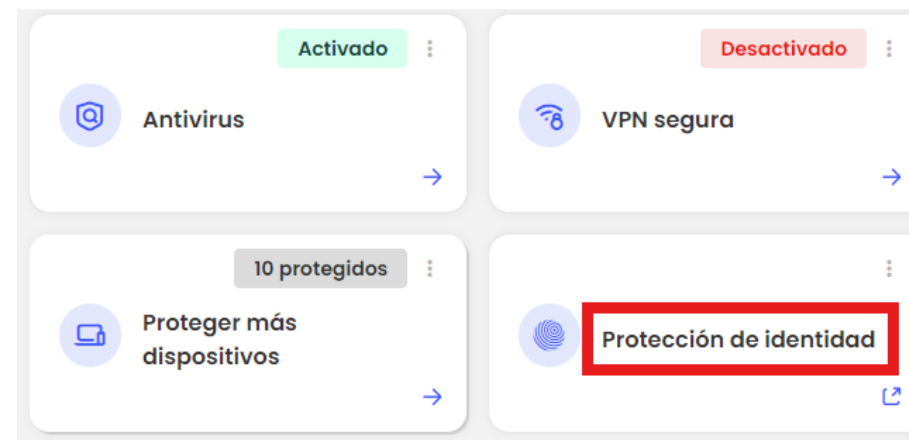
**Cuenta bancaria**  
0/10 bajo supervisión  
[+ Añadir](#)

**NIF**  
1/2 bajo supervisión  
[+ Añadir](#)

**Dirección de correo electrónico**  
4/10 bajo supervisión  
[+ Añadir](#)

**Nombre de usuario**  
0/10 bajo supervisión  
[+ Añadir](#)

**Número de teléfono**  
1/10 bajo supervisión  
[+ Añadir](#)



### Hemos encontrado tus datos en 1 filtraciones

Revisa las siguientes filtraciones para averiguar qué datos han quedado expuestos y cómo protegerlos.

[Más información sobre filtraciones](#)

Filtraciones nuevas (1)

Filtraciones revisadas (22)

Número de teléfono



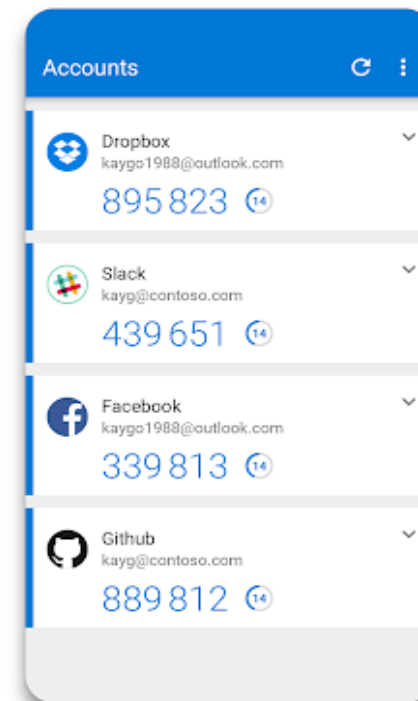
**facebook.com**  
Notificado el 8/4/2021

[Revisar](#)

# SEGUNDO FACTOR DE AUTENTICACIÓN

- Para evitar el riesgo de suplantación de identidad si las contraseñas son robadas o exfiltradas, se debe implantar el segundo factor de autenticación en todas las aplicaciones utilizadas que lo soporten.
- También es conocido como **verificación en dos pasos**, 2FA y **MFA** (múltiple)
- Activar la verificación en dos pasos también en las Redes Sociales de la empresa (LinkedIn, Instagram, Facebook, X) y cualquier sistema que lo soporte como PayPal para hacer pagos, Amazon o Temu para hacer compras, Wordpress, Dropbox, Zoom, etc.
- Instalar Microsoft **Authenticator** o Google Authenticator en el móvil para usarlo como segundo factor de autenticación.

Más seguro





# MICROSOFT AUTHENTICATOR

- <https://play.google.com/store/apps/details?id=com.azure.authenticator>
- <https://apps.apple.com/es/app/microsoft-authenticator/id983156458>



# SEGUNDO FACTOR DE AUTENTICACIÓN en LINKEDIN

## MÓVIL

1. Instalar Microsoft Authenticator



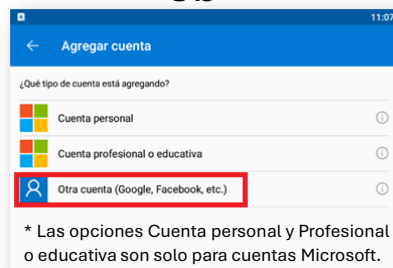
3. Abrir Microsoft Authenticator.

- Agregar cuenta +
- Elegir Otra cuenta\*
- Escanear el QR mostrado en LinkedIn.
- Introducir código de 6 dígitos en LinkedIn

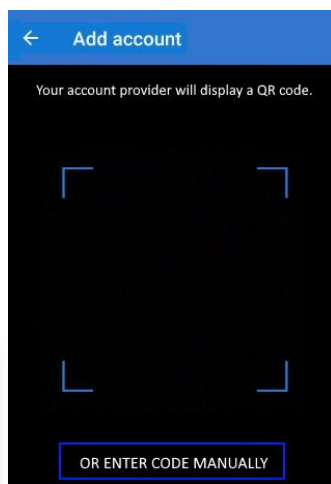
3a



3b



\* Las opciones Cuenta personal y Profesional o educativa son solo para cuentas Microsoft.



3c



O bien escribe esta clave secreta en tu aplicación de autenticación:  
OR56FQFDWSQSNVQLSCQ2POJACV62MPNO

4. Introduce el código de verificación de 6 dígitos generado por la aplicación de autenticación.

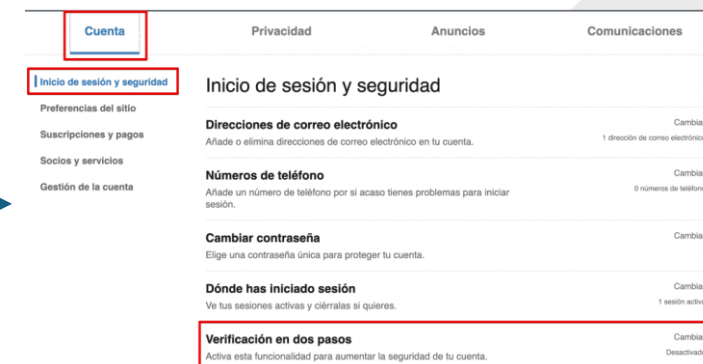
3d



## LINKEDIN

2. Ir a Verificación en dos pasos en Inicio de sesión y seguridad

2a



### Verificación en dos pasos

Activa esta funcionalidad para aumentar la seguridad de tu cuenta.

#### Con la aplicación de autenticación

- Instala **Microsoft Authenticator** o usa otra aplicación de autenticación.
- Abre la aplicación Microsoft Authenticator y selecciona Agregar cuenta > Cuenta de LinkedIn.
- Escanea el siguiente código QR.

2c

### Verificación en dos pasos

Activa esta funcionalidad para aumentar la seguridad de tu cuenta.

2b

Elige la forma de verificación

Aplicación de autenticación

Cancelar Continuar

La activación de esta función finalizará tu sesión en cualquier lugar donde tengas una sesión iniciada en esos momentos. Luego te pediremos que introduzcas un código de verificación la primera vez que inicies sesión con un dispositivo nuevo o en la aplicación móvil de LinkedIn. [Más información](#)

# USO DEL SEGUNDO FACTOR DE AUTENTICACIÓN

## Solicitud del código de un solo uso en **LinkedIn**.

Si se marca la casilla **Reconocer este dispositivo en el futuro** no se volverá a solicitar el código en ese equipo y navegador.

Introduce el código que aparece en la aplicación de autenticación

123 456

Reconocer este dispositivo en el futuro

Enviar

Nota: Si no puedes acceder a tu teléfono o al dispositivo reconocido anteriormente, contacta con el [Servicio de atención al cliente de LinkedIn](#)

## Solicitud del código de seguridad en otras aplicaciones: PayPal y Amazon



### Introducir código

Introduce el código de seguridad de 6 dígitos que aparece en la aplicación de autenticación.

Continuar

[Intentarlo de otro modo](#)



### Verificación en dos pasos

Introduzca el código generado por su app Authenticator

Indicar contraseña de un solo uso:

No vuelvas a pedir ningún código en este navegador

Iniciar sesión

• [¿No has recibido la contraseña de un solo uso?](#)

# ANTIMALWARE / ANTIVIRUS

- Para proteger de malware el puesto de trabajo, servidores y móviles se debe instalar un programa antivirus en todos los equipos independientemente del sistema operativo, ya sea gratuito o comercial.
- Recomendaciones para elegir antivirus:
  - Hacer un Checklist con las características que debe cumplir el producto, por ejemplo: la compatibilidad con los sistemas operativos usados, el rendimiento (hacer pruebas), precio, características adicionales, etc. para ayudar a saber cuál cumple con lo que se busca.
  - Valorar que cuente con antiphishing, VPN para el acceso remoto seguro, gestor de contraseñas, firewall, protección de la identidad (búsqueda de credenciales filtradas), etc.
  - Si el presupuesto lo permite, se recomienda elegir un producto que tenga protección frente al **Ransomware**, aunque esta funcionalidad solo estará disponible en las versiones premium de algún producto o los que se denominan EDR (Endpoint Detection and Response) que detectan y bloquean ataques avanzados.

# ANTIVIRUS

- Algunos productos ofrecen **gestor de contraseñas**, aunque tienen la desventaja de que si se cambia de antivirus, habrá que volver a introducirlas en otro gestor.
  - La funcionalidad de **protección de identidad** nos avisa de filtración de credenciales (usuarios y contraseñas) y otros datos. Es muy útil cuando alguna cuenta ha sido comprometida.
  - Se recomienda instalar también en el móvil, preferentemente con **VPN**
  - Recomendaciones de INCIBE respecto a antivirus / antimalware.
- <https://www.incibe.es/empresas/blog/protegiendo-nuestra-empresa-productos-anti-malware>



# ANTIVIRUS GRATUITOS

## 1. Bitdefender Antivirus Free

<https://www.bitdefender.com/solutions/free.html>

<https://www.bitdefender.com/solutions/antivirus-free-for-android.html>

## 2. Avast Free Antivirus. También app móvil. Incluye VPN de pago.

[www.avast.com](http://www.avast.com)

## 3. AVG Free antivirus. Recomendado para Mac y también para móvil.

[www.avg.com](http://www.avg.com)

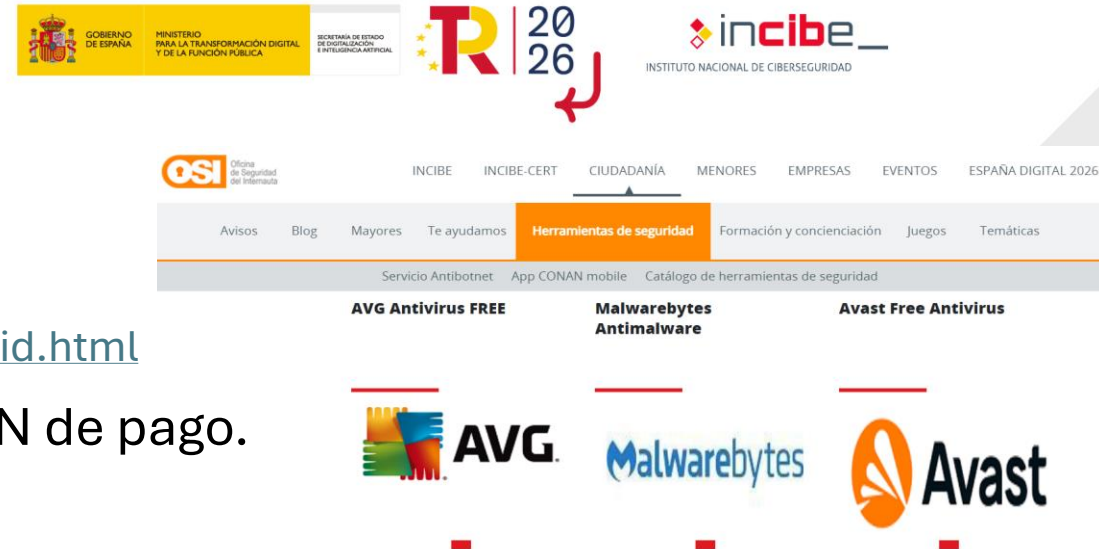
## Otros:

- Malwarebytes

[es.malwarebytes.com](http://es.malwarebytes.com)

- Windows Defender. Versión gratuita limitada preinstalada en el sistema operativo. Se desactiva al instalar otro.

[www.microsoft.com/es-es/security/business/microsoft-defender-for-business-and-individuals-free-trial](http://www.microsoft.com/es-es/security/business/microsoft-defender-for-business-and-individuals-free-trial)



# ANTIVIRUS COMERCIALES



Por orden alfabético:

- AVG
- Avast
- Bitdefender. Protección Ransomware y VPN.
- ESET
- Kaspersky
- McAfee Total Protection. Protección de identidad. Gestor de contraseñas y VPN. Ofertas interesantes en Amazon.
- Norton
- Panda
- Sophos

➤ Se pueden financiar con el **Kit Digital**

<https://www.acelerapyme.gob.es/kit-digital>



## Ciberseguridad

Hasta 29.000€



## Comunicaciones seguras

Hasta 29.000€



## Puesto de trabajo seguro

Hasta 1.000€

Solo para Segmento III.  
Pequeñas empresas o  
Microempresas de entre 0 y menos  
de 3 empleados y personas en  
situación de autoempleo 3.000 €



## Servicio de Ciberseguridad Gestionada

Hasta 29.000€

*Exclusiva para los  
segmentos IV y V*

<https://www.acelerapyme.gob.es/kit-digital/ciberseguridad>

### Funcionalidades y servicios

- **Antimalware y Antispyware**
- **Correo seguro: Antispam y Antiphishing**
- **Navegación segura**
- **Análisis y detección de amenazas.**
- **Monitorización de la red**
- **Configuración inicial y actualizaciones de seguridad**
- **Requisitos especiales de formación:** dispondrás de formación para la configuración del software de seguridad, y tendrás un **kit de concienciación en ciberseguridad** para complementar la solución con habilidades de firewall humano.

# PROTECCIÓN DE LA INFORMACIÓN

- Proteger adecuadamente los datos de los clientes, empleados y otra información sensible para el negocio.
- Con cifrado/criptación.
- Es un requisito para el cumplimiento del RGPD con determinados tipos de datos personales.
- Los documentos como Word, Excel o pdf con información sensible se deben proteger con, al menos, una contraseña.
- Hay varias herramientas gratuitas para ello como **Cryptomator** o Veracrypt
- También con algún compresor de archivos como **WinRAR** o 7-Zip usando la opción de **Establecer contraseña**.



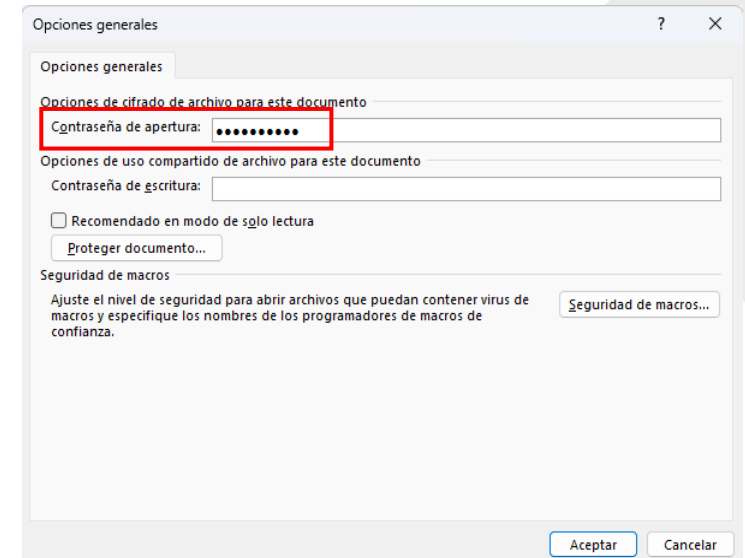
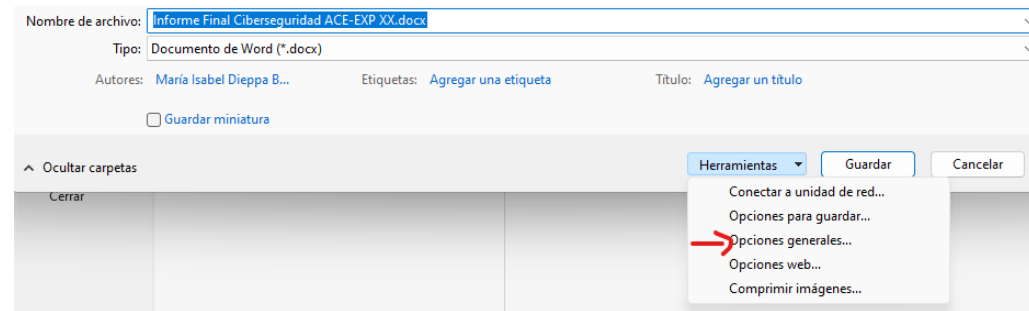
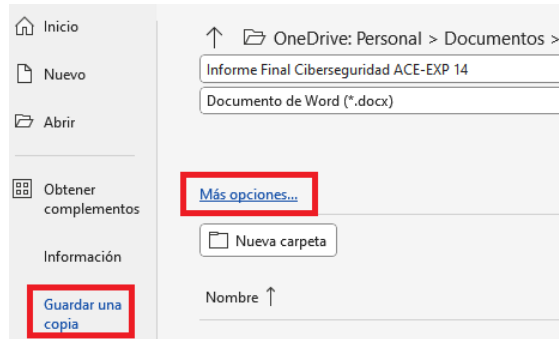
## ¿POR QUÉ DEBERÍAS CIFRAR TUS DATOS?

El cifrado es como ponerle un "candado secreto" a tus mensajes y archivos, para que solo tú y las personas que tú autorices puedan ver su contenido.

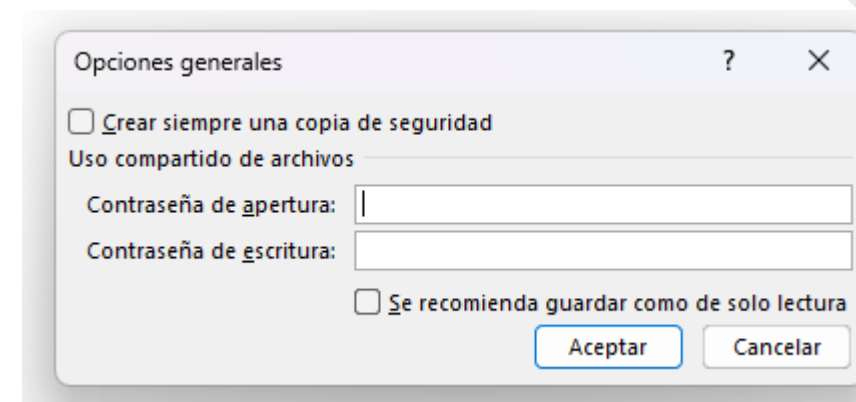
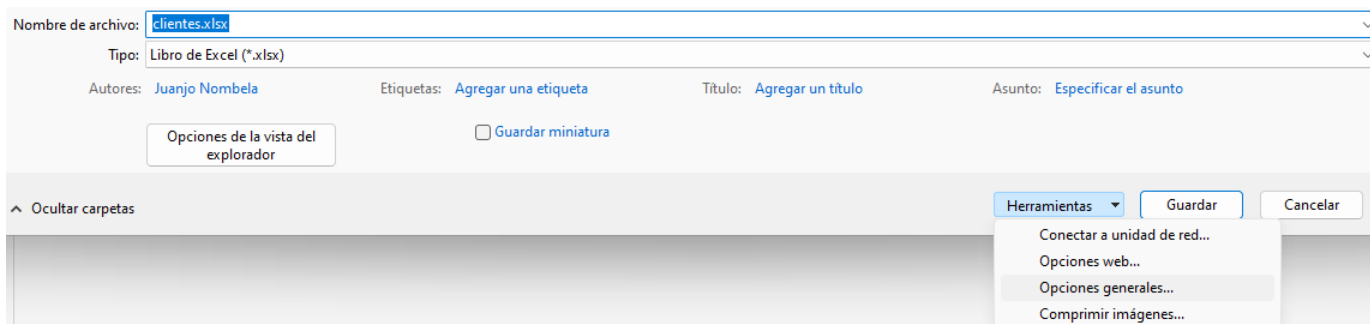
### ¡Aprovechate de estas ventajas!

- 01** Solo tú o la persona que tenga la clave de descifrado podréis ver la información que contienen tus archivos.
- 02** Tus datos personales no podrán ser utilizados para suplantar tu identidad o para cometer fraudes en tu nombre.
- 03** La información crítica o confidencial estará más segura ante posibles intentos de extorsión.
- 04** Minimizarás las repercusiones de enviar un archivo por error a alguien no deseado.
- 05** Obtendrás un extra de seguridad y privacidad en caso de acceso no autorizado a tus dispositivos o servicios en la nube.

# PONER CONTRASEÑA A UN WORD



# PONER CONTRASEÑA A UN EXCEL



En **OpenOffice** y **LibreOffice** también se pueden poner contraseñas en Guardar como y marcando la casilla Cifrar con contraseña.



# PONER CONTRASEÑAS A UN PDF

- Poner una contraseña en un pdf de forma gratuita (requiere subir el archivo a la nube de Adobe):

➤ <https://www.adobe.com/es/acrobat/online/password-protect-pdf.html>



## Proteger un PDF con contraseña



Seleccione un archivo PDF para añadir una contraseña.

Seleccionar un archivo

Si un documento Word o un Excel se convierte a pdf, se perderá la contraseña.

# CRYPTOMATOR

- Herramienta recomendable para cifrar archivos, carpetas y la información subida a la nube.
- En la nube crea una unidad cifrada donde se pueden subir todos los archivos que se desean proteger de forma sencilla.
- Se integra con Dropbox, Google Drive, OneDrive de Microsoft, etc. Es compatible con el RGPD
- Está disponible para Windows, Mac, Android e iOS. Solo en inglés.

<https://cryptomator.org>

Vídeo sobre el uso

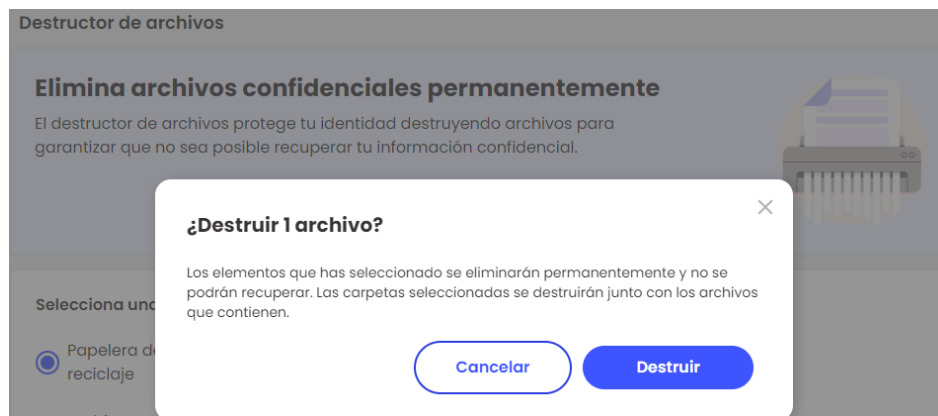
You see just another drive

The cloud can't see anything

# ELIMINACIÓN SEGURA DE INFORMACIÓN

- La información sensible debe borrarse de forma segura.
- OjO! los archivos eliminados de la papelera son recuperables si no se borran de forma segura.
- Herramientas de seguridad como los antivirus suelen incluir un destructor de archivos para eliminar los archivos confidenciales de forma permanentemente sin posibilidad de recuperación.
- En la web de herramientas de seguridad gratuitas de INCIBE también se pueden encontrar utilidades para este propósito.

<https://www.incibe.es/ciudadania/filtro/herramientas?tid=231>



# COMPARTIR ARCHIVOS DE FORMA SEGURA



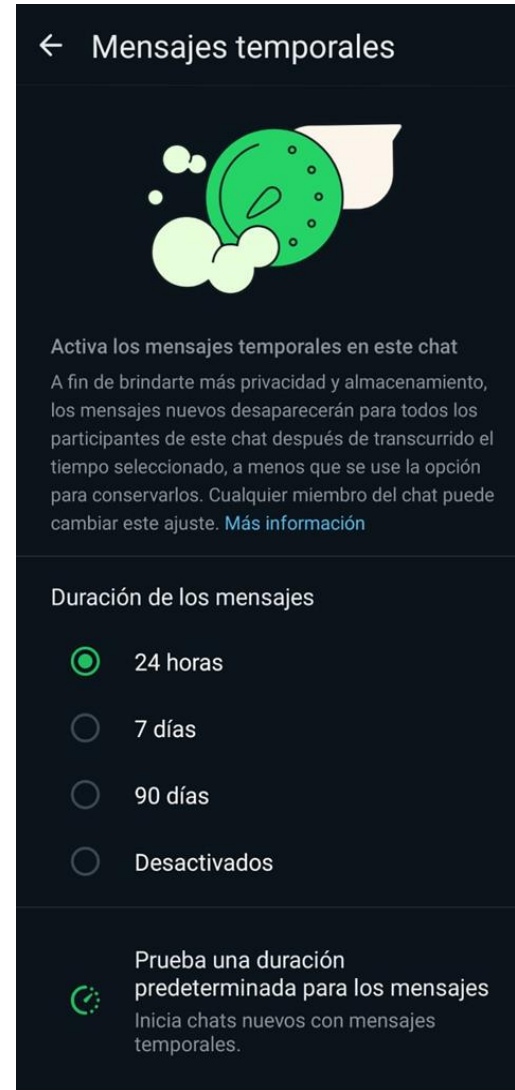
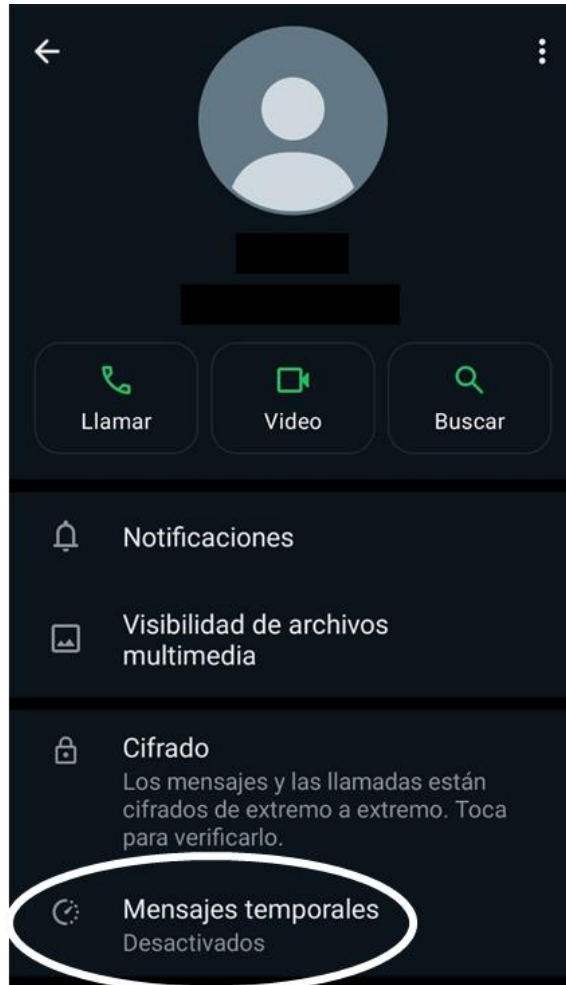
## Por correo electrónico

- Para compartir datos sensibles con terceros por correo electrónico o por un servicio de compartición en la nube, es recomendable enviarlos cifrados con la protección de una contraseña.
- Una opción es comprimir el archivo o archivos con una herramienta tipo WinRAR en un .zip o .rar, protegiéndolos con una contraseña
- Si el archivo se envía por correo, las contraseñas se tienen que compartir **por un canal diferente:**
  - Whatsapp, Telegram o SMS
  - Password Pusher: <https://pwpush.mur.at/es>

## Compartir archivos de la nube


- Tener siempre en cuenta el principio del mínimo privilegio a la hora de compartir archivos almacenados en la nube (OneDrive, Dropbox, Drive, etc.). Si no es necesario que la persona con la que se van a compartir archivos los modifique, dar solo permiso de lectura.
- Poner una **fecha de caducidad** cuando se compartan archivos y limitar el número de accesos, por ejemplo, a solo 1.
- Intentar evitar los enlaces (vínculos) abiertos que podría utilizar cualquier persona que los tenga. Si se usan, poner una contraseña a los archivos compartidos.

# COMPARTIR ARCHIVOS DE FORMA SEGURA



# COMPARTIR CONTRASEÑAS DE FORMA SEGURA

<https://pwpush.mur.at/es>

 **Password Pusher**  
Go Ahead. Email Another Password.

Idioma

ContraseñaSegura123#

20 / 1048576 Caracteres

Caducar el enlace secreto y eliminarlo después de:

1 Día  
 3 Vistas  
(lo que sea que ocurra primero)

Utilice un paso de recuperación de 1 clic

Ayuda a evitar que los sistemas de chat y los escáneres de URL consuman vistas.

Permitir eliminación inmediata

Permita que los usuarios eliminen este enlace una vez visto.

Bloqueo de contraseña Opcional: solicitar a los destinatarios que ingresen una frase a modo d

[Guardar](#) la configuración anterior como la página predeterminada.

Generar Contraseña

Use el botón de arriba para generar una contraseña aleatoria.

*Sugerencia: solo ingrese una contraseña en el cuadro. Cualquier otra información de identificación puede comprometer la seguridad.*

*Todas las contraseñas están encriptadas antes del almacenamiento y están disponibles solo para aquellos con el enlace secreto. Una vez caducadas, las contraseñas encriptadas se eliminan de forma inequívoca de la base de datos.*

¡Compartir!

## Tu enlace ha sido creado.

Utiliza este enlace secreto para compartirlo:

[https://pwpush.com/p/xfrpgi4\\_qrs/r](https://pwpush.com/p/xfrpgi4_qrs/r)

Detección automática



Imprimir y compartir

Este enlace secreto y todo el contenido se eliminarán en **2 días** o **5 más vistas**, lo que ocurra primero.

[Ver este enlace ahora](#) (quemará una vista) o [Compartir otro](#)



# COPIAS DE SEGURIDAD

- Las copias de seguridad son la **mejor medida de prevención** para recuperar los datos en un escenario de ransomware, malware, robo o ante desastres como el fuego.
- Se deben realizar de forma **regular**, ya sea en un dispositivo externo como un disco duro o un pendrive rápido con la capacidad suficiente, o en la nube.
- Las copias de seguridad **híbridas** (local+nube) son una buena opción.
- La **frecuencia** para hacer las copias dependerá de la importancia de los datos y de la frecuencia con la que se actualizan los datos.
- Guardar una copia de seguridad en un **lugar alternativo**. Si la copia se guarda junto al equipo donde están los datos, también podría perderse por robo o incendio.
- **Probar** a restaurar las copias de seguridad periódicamente para asegurar que son operativas.

[https://www.incibe.es/ciudadania/filtro/herramientas?tid=124&tid\\_2=All&tid\\_3=All](https://www.incibe.es/ciudadania/filtro/herramientas?tid=124&tid_2=All&tid_3=All)

# COPIAS DE SEGURIDAD

Inicio

Buscar una configuración

## Actualización y seguridad

Windows Update

Optimización de distribución

Seguridad de Windows

Copia de seguridad de archivos

## Copia de seguridad de archivos

### Copia de seguridad con Historial de archivos

Realiza una copia de seguridad de tus archivos en otra unidad y restáuralos si los originales se han perdido, están dañados o se han eliminado.

Realizar una copia de seguridad automática de mis archivos

Activado

[Más opciones](#)

¿Buscas una copia de seguridad anterior?

## Hacer una copia de seguridad de tu Mac con Time Machine

Si tienes una unidad USB u otro dispositivo de almacenamiento externo, puedes usar Time Machine para hacer una copia de seguridad automática de tus archivos, como aplicaciones, música, fotos, correo electrónico y documentos.

- Los móviles deben protegerse adecuadamente por la información que puedan contener y porque pueden ser la llave de acceso a ciertas aplicaciones.
- Las amenazas más comunes dirigidas contra los móviles son:
  - Instalación de Apps maliciosas
  - Malware
  - Smishing. Fraude mediante SMS equivalente al Phishing.
  - Robo de dispositivos
  - SIM swapping
  - Interceptación de comunicaciones WiFi en redes inseguras (Man in the Middle)

# PREVENIR SMISHING

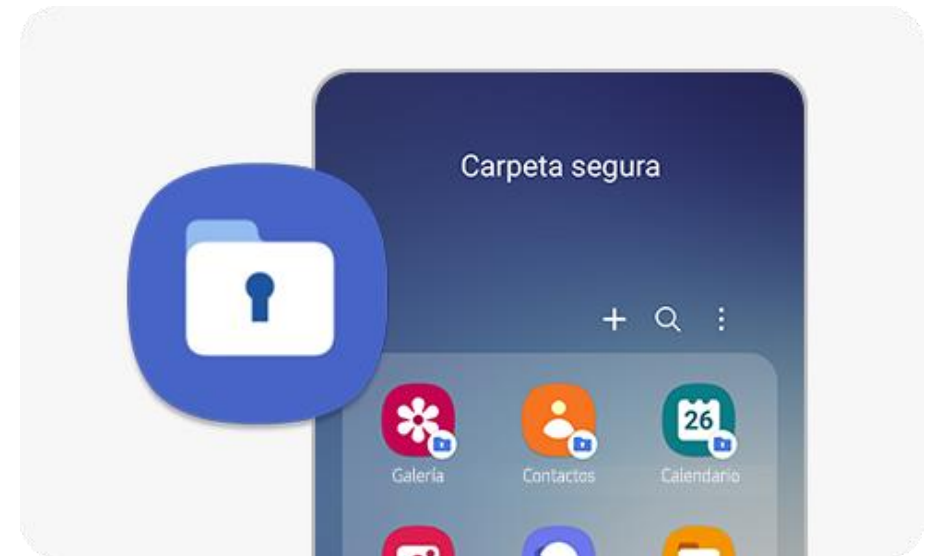


- Configuración segura de las Apps
  - Ajustar los permisos de las aplicaciones para que no tengan más de los necesarios (micrófono, cámara, ubicación, acceso a archivos, etc)
  - No instalar aplicaciones innecesarias y antes de hacerlo comprobar que tienen un número mínimo de instalaciones.
  - No instalar aplicaciones externas a la tienda oficial (Google Play, App Store).
  - Desinstalar las que no se usen.
- Bloquear siempre el acceso con contraseña/PIN (adicional al PIN de la SIM) o con huella dactilar si el móvil lo permite.
- Hacer copias de seguridad en algún dispositivo externo, aunque estén los archivos sincronizados en la nube.
- **Desactivar el Bluetooth y NFC** cuando no sea necesario.

- Activar el cifrado completo del almacenamiento.
- Crear una carpeta segura para almacenar los archivos más sensibles como documentos, imágenes, contactos, etc..
- En **Android**: Files de Google



- En los móviles **Samsung**: carpeta segura





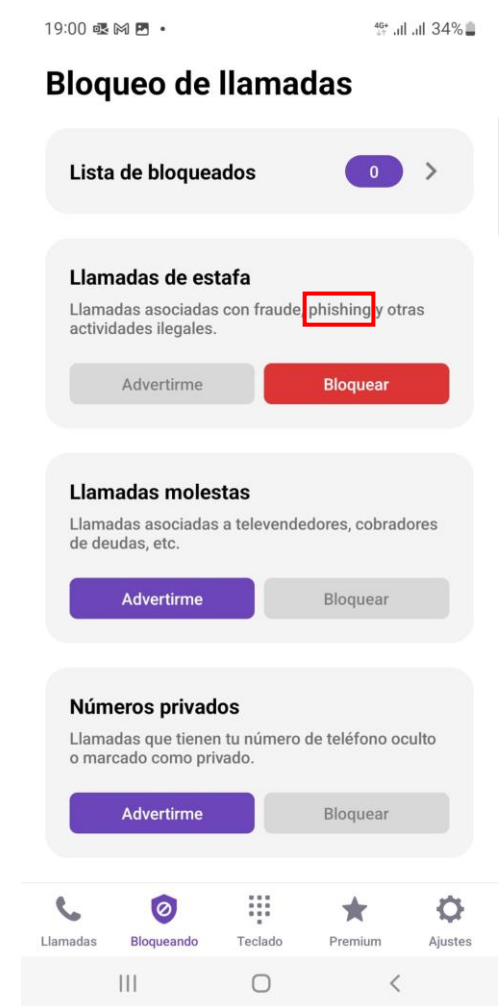
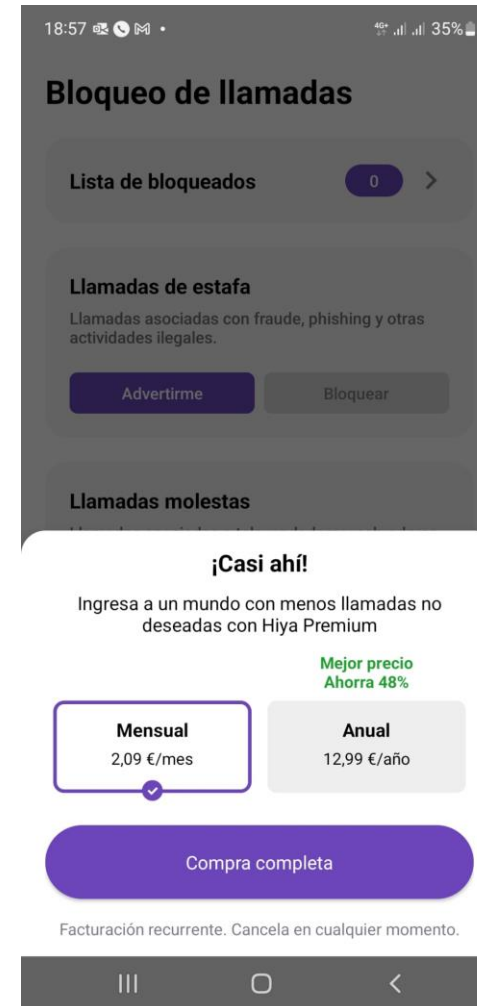
# ESTAFAS TELEFÓNICAS

- Aplicaciones para bloquear llamadas fraudulentas (y comerciales)

➤ <https://es.hiya.com>

<https://play.google.com/store/apps/details?id=com.webascender.callerid&hl=es>

<https://apps.apple.com/es/app/hiya-caller-id-spam-blocker/id986999874>



- Para reducir las llamadas molestas: apuntarse en la lista Robinson para reducir las llamadas, SMS y correos comerciales no deseados.

<https://www.listarobinson.es>

# NAVEGACIÓN SEGURA EN INTERNET

## • En Privacidad y Seguridad: Activar Protección mejorada

Configuración

- Tú y Google
- Autocompletar y contraseñas
- Privacidad y seguridad**
- Rendimiento
- Aspecto
- Buscador
- Navegador predeterminado
- Al iniciar
- Idiomas
- Descargas
- Accesibilidad
- Sistema
- Restablecer configuración
- Extensiones

Buscar ajustes

Comprobación de seguridad

Chrome ha encontrado algunas recomendaciones de seguridad para que las revises  
Contraseñas, Actualización de Chrome

Ir a Comprobación de seguridad

Privacidad y seguridad

- Eliminar datos de navegación
- Guía de privacidad
- Cookies de terceros
- Privacidad en la publicidad
- Seguridad**
- Configuración de sitios



Seguridad de un vistazo

- 63 contraseñas reutilizadas  
Crea contraseñas únicas
- Chrome está actualizado  
Versión 127.0.6533.122 (Build oficial) (64 bits)
- Navegación segura mejorada está activada**  
Disfrutas de la seguridad más potente de Chrome



Elige tu nivel de protección de Navegación segura

- Protección mejorada**  
Protección proactiva en tiempo real (frente a sitios, descargas, y extensiones peligrosos) que se basa en el envío de tus datos de navegación a Google

Cuando está activada

- Te envía advertencias sobre sitios peligrosos (aunque Google no los conozca) analizando más datos de sitios que la protección estándar. Si quieres, puedes omitir las advertencias de Chrome.
- Análisis exhaustivos para detectar descargas sospechosas.
- Cuando inicias sesión, te protege en los servicios de Google.
- Mejora tu seguridad y la de todo el mundo en la Web.
- Te avisa si usas una contraseña vulnerable en una brecha de seguridad de datos.

Notas importantes

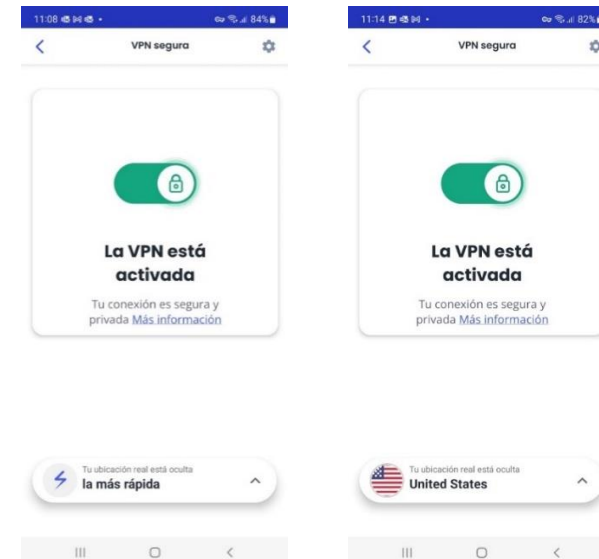
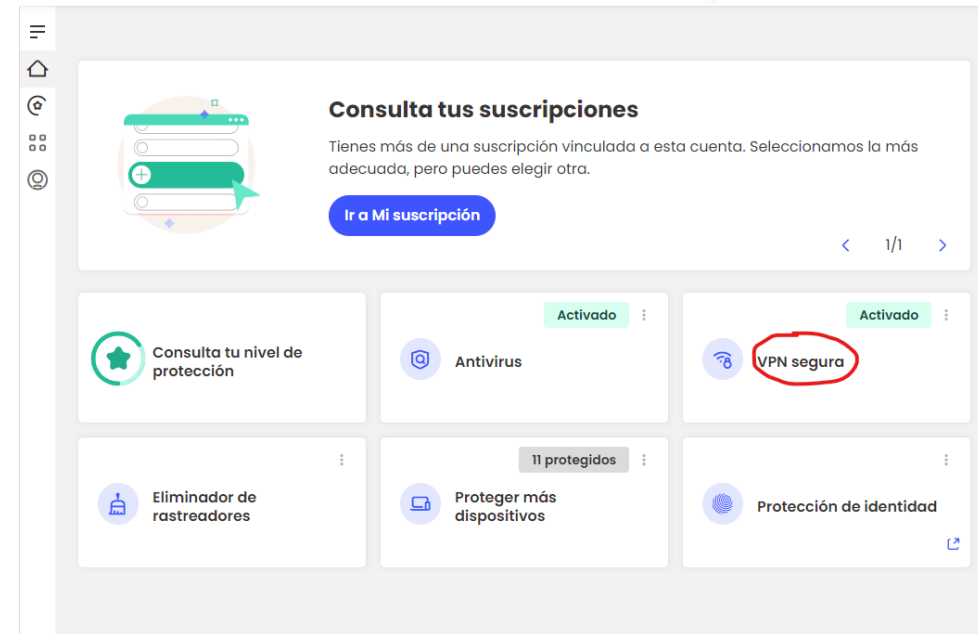
- Envía las URLs de los sitios que visitas y una pequeña muestra del contenido de la página, de las descargas, de la actividad de las extensiones y de la información del sistema a Navegación segura de Google para comprobar si son dañinas.
- Cuando inicias sesión, estos datos se vinculan a tu cuenta de Google para protegerte en los servicios de Google (por ejemplo, con una mayor protección en Gmail tras un incidente de seguridad).
- No ralentiza de forma significativa tu navegador ni tu dispositivo.

- Instalar un firewall para evitar conexiones no deseadas a la red y los equipos. El sistema operativo trae uno y los antivirus también lo suelen incorporar en sus versiones de pago.
- Configuración segura del router y WiFi:
  - Cambiar la contraseña que viene por defecto poniendo una robusta (guardarla en el gestor de contraseñas)
  - Cambiar las claves del WiFi regularmente o después de compartirla con alguna persona para una conexión puntual.
  - Comprobar que no hay dispositivos ajenos conectados. Para evitar conexiones indeseadas que pudiesen haber obtenido la contraseña del WiFi, limitar las conexiones en el router mediante el filtrado por MAC (lista blanca).
  - Para acceder al router, consultar las instrucciones o probar tecleando <http://192.168.1.1> o <http://192.168.0.1> en la barra de direcciones del navegador.
- Evitar conectarse a WiFi públicas de hoteles, aeropuertos, etc. Usar la conexión 4G/5G si hay buena cobertura de datos y se tienen datos suficientes o ilimitados. Si es imprescindible, usar una VPN.
- Desactivar el Bluetooth en el portátil cuando no se use.

# VPN (Red Privada Virtual)

- Se utilizan para una conexión/navegación:
  1. Segura: cifrar datos transmitidos.
  2. Privada: ocultar origen (IP)
- Activar si es necesario conectarse a una WiFi pública, de un hotel, aeropuerto, etc.
- Desde el portátil y desde el móvil.
- Ocultan la dirección IP para evitar la geolocalización y permiten elegir el país que queremos que aparezca.

➤ Ver tu IP y ubicación: <https://ipapi.co>



- Un mal uso de las redes sociales podría dañar la reputación de la organización por lo que debemos protegerlas adecuadamente.
- Existe el riesgo de la suplantación de identidad que permitiría escribir a nuestros contactos, crear o cambiar publicaciones, acceder a nuestros mensajes privados o incluso secuestrar el perfil.
- Recomendaciones con las RRSS:
  - Utilizar contraseñas robustas y almacenarlas de forma segura.
  - Activar el segundo factor de autenticación en todas las RRSS del negocio y personales.
  - Revisar las opciones de privacidad y desactivar las que no sean necesarias. Ocultar correo electrónico personal o corporativo.
  - Definir roles y responsabilidades. Cada miembro del equipo debe conocer su rol en la gestión de las cuentas de redes sociales. Esto puede incluir asignar a alguien como administrador principal de cuentas, a otro como gestor de contenido y a otros como colaboradores.
  - Crear una política de uso de redes sociales.
  - Hacer copias de seguridad de las publicaciones y otros datos por si se produce una violación de seguridad.

- Recomendaciones de INCIBE para evitar fraudes en el comercio electrónico:
  - Utilizar pasarelas de pago seguras como Redsys o Stripe que estén certificadas y cumplan con los estándares de seguridad de la industria, como el PCI DSS lo que asegura que los datos del cliente están siendo cifrados durante la transacción.
  - Solicitar siempre el código CVV (también llamado CVC)
  - No almacenar los datos de las tarjetas y menos el CVV (caso AirEuropa)
  - Forzar a los clientes a usar contraseñas robustas, que las cambien regularmente y, para mayor seguridad, implementar doble factor de autenticación con SMS, Authenticator, etc.
  - Prevenir el fraude de devolución de cargo. Este fraude ocurre cuando un cliente solicita un reembolso directamente al emisor de su tarjeta en lugar de hacerlo al negocio online.
  - Monitorización continua de transacciones para detectar y responder rápidamente a cualquier actividad sospechosa como múltiples intentos de compra con diferentes tarjetas desde la misma dirección IP o la misma tarjeta desde diferentes ubicaciones.

➤ <https://www.incibe.es/empresas/blog/tienes-una-tienda-online-conoce-las-claves-para-detectar-una-compra-fraudulenta>



# SI COMPRAS ONLINE

- Ojo con las web clonadas (take down [lookup.icann.org/es/lookup](https://lookup.icann.org/es/lookup))
- Y web falsas que nunca envían productos:

<https://maestro-h.com>



Comprado con mayor frecuencia:



Aspirador escoba - CECOTEC Conga  
ThunderBrush 560, 600 W, 100 min, Grey  
Original  
Aspirador  
€34.00



Aspirador sin bolsa - CECOTEC Conga 3000  
Carpet Clean L, 400 W, Grey Original  
Aspirador  
€83.30



AÑADIR AL CARRITO  
Aspirador escoba - CECOTEC Conga  
Rockstar 1500 Ray Pure, 215 W, Black Original  
Aspirador  
€68.00



Aspirador de trineo Cecotec Conga Rockstar  
Multicyclonic Compact X-Treme 800W 20kPa  
2L Negro Original  
Aspirador  
€42.50

- Comprobar si la web es de fiar:  
➤ <https://es.trustpilot.com>



# SI DESARROLLAS APLICACIONES

- Es habitual que en el código desarrollado haya vulnerabilidades si los desarrolladores no han recibido la formación adecuada para evitarlo o no han seguido unas buenas prácticas de desarrollo seguro debido a la presión por la entrega de los programas.
- Si se hacen desarrollos internos, se debe escanear el código con alguna herramienta de análisis de código estático o subcontratarlo a un tercero. Si se hacen desarrollos para terceros, se deberían entregar a los clientes libres de vulnerabilidades.

➤ <https://www.sonarsource.com/open-source-editions>

- Algunas herramientas comerciales de análisis de código estático SAST y análisis de código dinámico DAST son: Veracode, Fortify, Checkmarx, etc.
- Los desarrolladores deben conocer las vulnerabilidades más comunes y los estándares OWASP, CWE <https://cwe.mitre.org>. CVE <https://cve.mitre.org/>

# SEGURIDAD POR DISEÑO



# SEGURIDAD EN EL SOFTWARE?



This screenshot shows the VirusTotal analysis results for a URL. At the top left, a circular progress indicator shows a score of 5 out of 95. Below it is a 'Community Score' slider. A notification banner at the top right says '5/95 security vendors flagged this URL as malicious'. The URL being analyzed is 'http://citeceramica.com/citeceramica.com'. The content type is 'text/html'. Below this are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY' (4). A green banner encourages joining the community. Below that is a table titled 'Security vendors' analysis'.

Vendor	Detection	Vendor	Detection
Antiy-AVL	Malicious	CyRadat	Malicious
Fortinet	Malware	Seclookup	Malicious
Trustwave	Phishing	Abusix	Clean

This screenshot shows the VirusTotal analysis results for a clean URL. At the top left, a circular progress indicator shows a score of 0 out of 95. Below it is a 'Community Score' slider. A notification banner at the top right says 'No security vendors flagged this URL as malicious'. The URL being analyzed is 'http://newvetec.com/newvetec.com'. The content types are 'text/html' and 'base64-embedded'. Below this are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'.

1. **Reconocer** el entorno: configuración de equipos, software, análisis de vulnerabilidades, privilegios administrativos, correo, navegadores, antivirus, puertos, protocolos, servicios, wifi, etc.
2. **Auditoría Interna** de Ciberseguridad (usuario interno autorizado)
3. **Auditoría Externa** de intrusión (web)
4. Análisis de exposición digital (huella digital)
5. Plan de acción para remediar las vulnerabilidades encontradas
6. Monitorización continua (opcional)

# RESPUESTA A INCIDENTES

- Crear un sencillo plan de respuesta ante incidentes como un ciberataque de Ransomware en el que se documente en un procedimiento sencillo las pautas básicas sobre cómo actuar en dicho escenario.
- Algunas herramientas para ayudar a crearlo y ensayarlo/entrenarlo:
  - Cuestionario inicial de respuesta a incidentes como documento de apoyo para analizar y resolver un incidente.
  - Juego de rol para ensayar respuesta con 5 escenarios: Ransomware, phishing, fuga de información, ataque de ingeniería social, botnet.  
[https://www.incibe.es/sites/default/files/contenidos/JuegoRol/juegorol\\_manual.pdf](https://www.incibe.es/sites/default/files/contenidos/JuegoRol/juegorol_manual.pdf)



# RESPUESTA A INCIDENTES

- En caso de incidente de seguridad, contactar de forma gratuita con INCIBE:
  - Por teléfono en el 017 (horario de 8:00 a 23:00, los 365 días del año)
  - Por WhatsApp (900 116 117) o Telegram (@INCIBE017)
  - Atención presencial (solo en León)
  - Formulario web: <https://www.incibe.es/incibe-cert/incidentes/notificaciones>

Servicio gratuito y confidencial, disponible de 08:00 am a 11:00 pm los 365 días del año.



## TU AYUDA EN CIBERSEGURIDAD

- 017  
Teléfono 017
- WhatsApp 900 116 117
- Telegram @INCIBE017
- Formulario web
- Atención presencial

## Notificación

Correo \*

Incidente

Asunto \*

Descripción \*

# ¡Ahora te toca!



¿Tienes una idea de negocio en ciberseguridad, tu proyecto necesita de ciberseguridad?

**¡Te ayudamos a emprender!**



¡Apúntate a los próximos talleres de emprendimiento!



¡O solicita plaza en el programa de Incubación de INCIBE Emprende!

# Ediciones anteriores



# INCIBE Emprende

¡Te estamos esperando!



[proyectos@clubdeemprendimiento.com](mailto:proyectos@clubdeemprendimiento.com)



[www.clubdeemprendimiento.com](http://www.clubdeemprendimiento.com)





## Programa de Impulso a la Industria de la Ciberseguridad Nacional

#INCIBEemprende