Acelera pyme

Ciberseguridad

Documento de referencia

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

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

Índice

Índice

1. Resumen ejecutivo

Resumen ejecutivo

La Ciberseguridad

En un mundo en el que la tecnología avanza rápidamente, **la seguridad es uno de los principales retos de todas las personas y empresas** que disponen de diferentes recursos informáticos conectados a la red.

Los nuevos medios tecnológicos han permitido que el mundo se mantenga conectado a todos los niveles, tanto personal como profesional. Estos cambios en la sociedad han aumentado la eficiencia y mejorado la calidad de vida de todas las personas, aunque existen ciertos riesgos y amenazas que se deben tener en cuenta para la protección de todos y todas.

De este nuevo reto, surge la necesidad de **aumentar el nivel de compromiso público y privado para lograr un espacio digital más seguro.** Esto no solo reside en la creación de herramientas disruptivas en materia de seguridad informática, sino que también se deben complementar con la creación de productos, procesos y sistemas de Tecnologías de la Información (TIC).

La situación derivada de la Covid-19 ha acelerado la transformación digital, obligando a modificar las infraestructuras tecnológicas de las empresas, incrementando el riesgo de ataques por parte de los ciberdelincuentes.

Este documento tratará todas las cuestiones relacionadas con la evolución de la ciberseguridad y el panorama actual en los diferentes sectores, destacando: **el origen de la cibercriminalidad**, **principales amenazas** (*Malware, p*rotección de las contraseñas, ingeniería social, ataques a las conexiones) y **medidas de protección.**

En definitiva, las tecnologías en materia de ciberseguridad ayudan a todas las personas y empresas a prepararse ante las posibles crisis que puedan surgir a raíz de los ciberataques, garantizando la protección de la información y, de las propias personas usuarias de Internet, aunque cabe destacar que la mejor protección es la concienciación de los usuarios sobre los riesgos derivados del uso de internet.

Cabe mencionar que la elaboración del libro cuenta con la colaboración de **Marc Martínez Marce**, **socio de Ciberseguridad y Technology Risk en KPMG**, con amplia **experiencia en numerosas organizaciones internacionales y nacionales** en la mayoría de los sectores de la industria, como servicios financieros, seguros, gestión de activos y organizaciones de terceros, y es considerado uno de los **líderes en su campo de especialización**. Compagina esta actividad con la docencia en el Máster en Gestión de la Seguridad de la Información de Asimelec y de la Universidad Politécnica de Madrid.

2. Introducción

Introducción

El panorama actual de la Ciberseguridad

El proceso de transformación digital, conocido como la ***"era de la información"*** comenzó al mismo tiempo que la revolución digital, entre los años 50 y 70. Este periodo está asociado al momento en el que se desarrollaron las tecnologías digitales de la información y comunicación (TIC), las cuales surgieron a raíz de la importancia en la rapidez de la comunicación.

En estos últimos años la tecnología ha avanzado sin precedentes, convirtiendo las herramientas informáticas en recursos esenciales para la optimización de las actividades llevadas a cabo en las empresas y aumentando la productividad de los trabajadores y de la propia compañía.

Debido a la exposición de la información por medio de este tipo de tecnologías de la información, surge el concepto de ciberseguridad. La seguridad informática o digital se crea a causa de la necesidad de proteger todos los dispositivos informáticos conectados a la red de aquellos "ataques" que puedan ocasionar daños o pérdidas de la mencionada información, tanto a nivel personal como laboral.

> *"La ciberseguridad es el conjunto de actuaciones orientadas a asegurar, en la medida de lo posible, las redes y sistemas de que constituyen el ciberespacio: detectando y enfrentándose a intrusiones; detectando, reaccionando y recuperándose de incidentes; preservando la confidencialidad, disponibilidad e integridad de la información".*
>
> **Centro Criptológico Nacional de España**

El objetivo principal de los programas o de las estrategias de seguridad informática, además de la protección de la información, es **proporcionar a los usuarios unos conocimientos básicos** para la detección de posibles amenazas.

Para combatir los posibles riesgos es necesario que las empresas dispongan de una estrategia de ciberseguridad que incluya los siguientes aspectos:

- Políticas y procedimientos de actuación.
- Planificación de la seguridad de la empresa.
- Fomento de la cultura de la ciberseguridad.

Por todo esto, la ciberseguridad se emplea como herramienta para luchar contra los posibles ataques informáticos que atentan contra cada usuario de Internet.

Introducción

Conceptos clave

Algunos de los conceptos que se deben conocer en el campo de la ciberseguridad y que se emplearán en este documento, se explican a continuación y todos ellos están definidos por el **Instituto Nacional de Ciberseguridad (INCIBE)** en su glosario de términos de ciberseguridad.

Ciberataque

*"Intento deliberado de un ciberdelincuente de **obtener acceso a un sistema** informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema".*

Ciberdelincuente

*"Persona que realiza **actividades delictivas en la red** contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos".*

Cifrado

*"Proceso de **codificación de información** para poder evitar que esta llegue a personas no autorizadas. Solo quien posea la clave podrá acceder al contenido".*

Confidencialidad

*"**Confidencialidad** es la **propiedad de la información**, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información".*

Copia de seguridad

*"Proceso mediante el cual se **duplica la información** existente de un soporte a otro, con el fin de poder recuperar los datos contenidos en caso de fallo del primer soporte de alojamiento".*

Cortafuegos o firewall

*"**Sistema de seguridad** compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios".*

3. Ciberseguridad

3.1. Qué es y en qué consiste

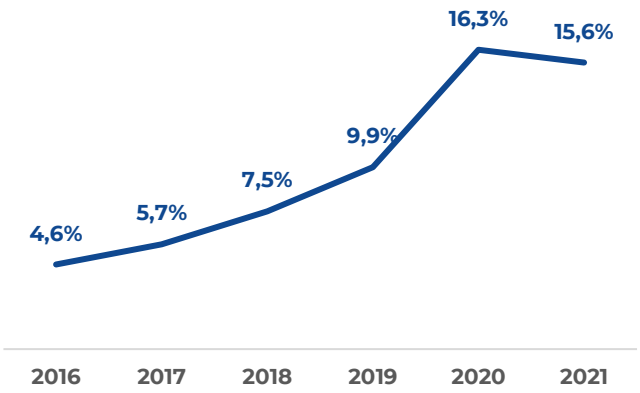
Ciberseguridad

Evolución de la cibercriminalidad

La ciberdelincuencia es un fenómeno mundial y complejo que requiere un conjunto de técnicas específicas para su lucha pero, para ello, es necesario conocer la situación actual y evolución de la misma. En el gráfico de la derecha se recopilan los datos de los delitos informáticos sobre el total de las infracciones penales cometidas en España. En este gráfico observamos cómo la ciberdelincuencia **ha aumentado cada año desde 2016, hasta 2020, siendo el año más afectado de todos** y el que mayor peso presenta frente a la totalidad de la criminalidad del país.

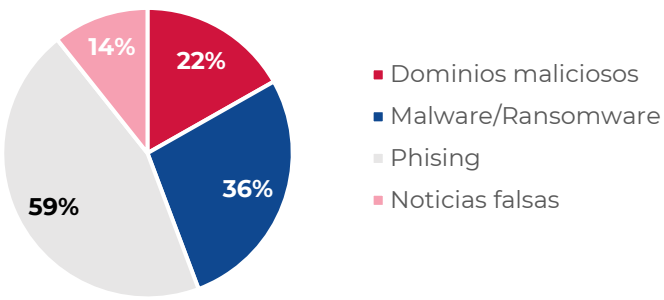
Tal y como se comentó anteriormente, la situación ocasionada por la **Covid-19 ha disparado los delitos informáticos**, destacando el *Phishing* y el *malware*, como se puede observar en el gráfico.

Delitos informáticos sobre el total de las infracciones penales cometidas en España



Fuente: Ministerio del Interior

Ciberamenazas relacionadas con la Covid-19



Fuente: Ministerio del Interior

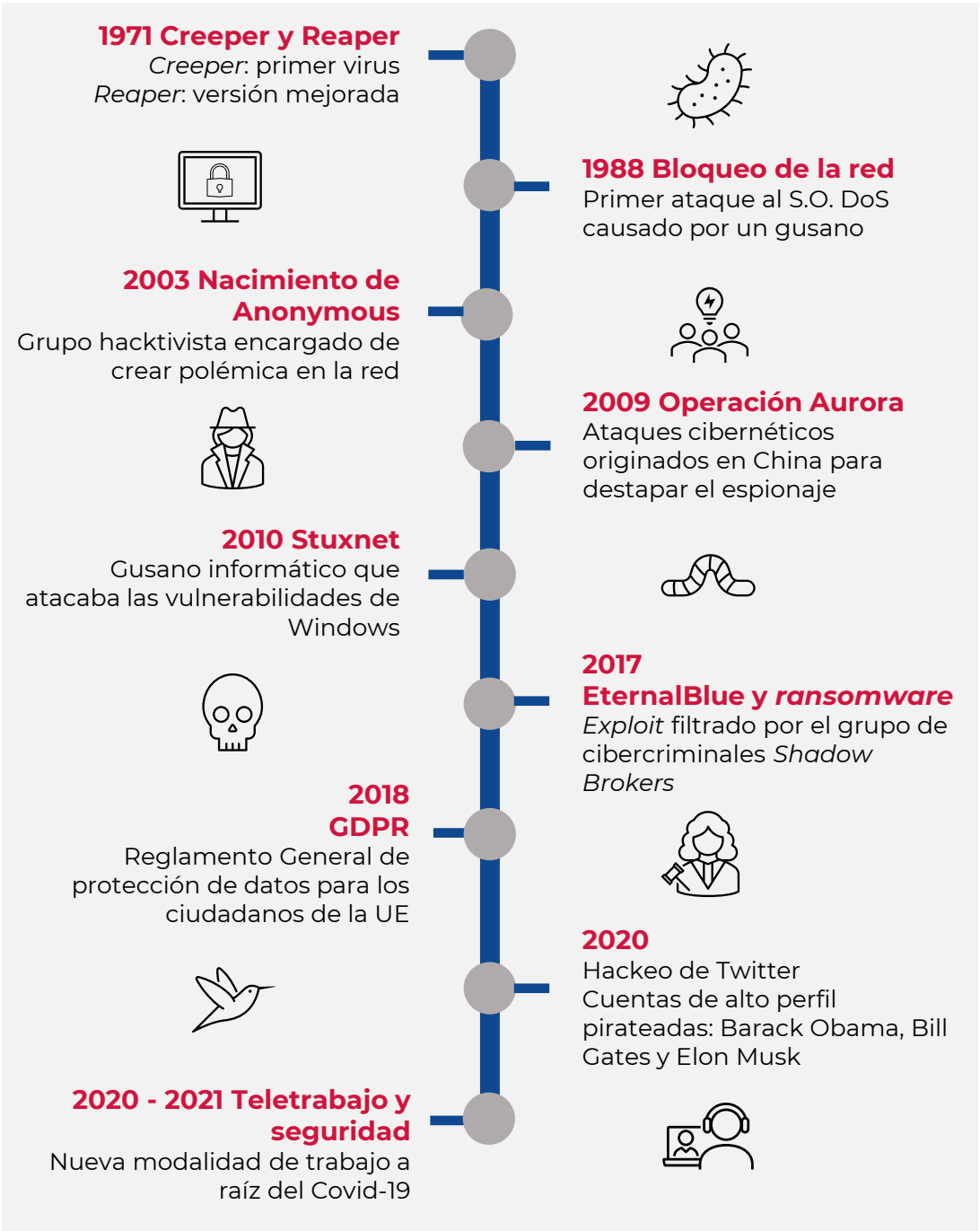
Según el Informe de Evaluación de la Amenaza del Crimen organizado en Internet (IOCTA) de 2021, el aumento de mercado online lleva emparejado ciertas actividades intrusivas informáticas y ha proliferado la venta de productos médicos falsificados generados por la COVID-19, entre otros casos. La mayoría de los ciberataques se aprovechan del contexto mediante las siguientes amenazas informáticas:

- ***Ransomware:*** encriptación de archivos para la solicitud de un determinado rescate debido al aumento de la modalidad del teletrabajo y las compras *online*.
- **Troyanos bancarios:** tipo de *malware* cuyo propósito es robar los datos bancarios de sus víctimas utilizando mecanismos de ingeniería social.
- **Ataques de denegación de servicio distribuido:** ataque a un sistema o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- **Captación de menores:** debido al incremento de menores conectados a la red.

Ciberseguridad

Evolución de la cibercriminalidad: breve cronología

La evolución de las nuevas tecnologías ha hecho que se desarrollen **herramientas informáticas destinadas a la detección y lucha contra los ataques cibernéticos**. A continuación, se destacan algunos de los hitos más críticos en materia de seguridad de la información.



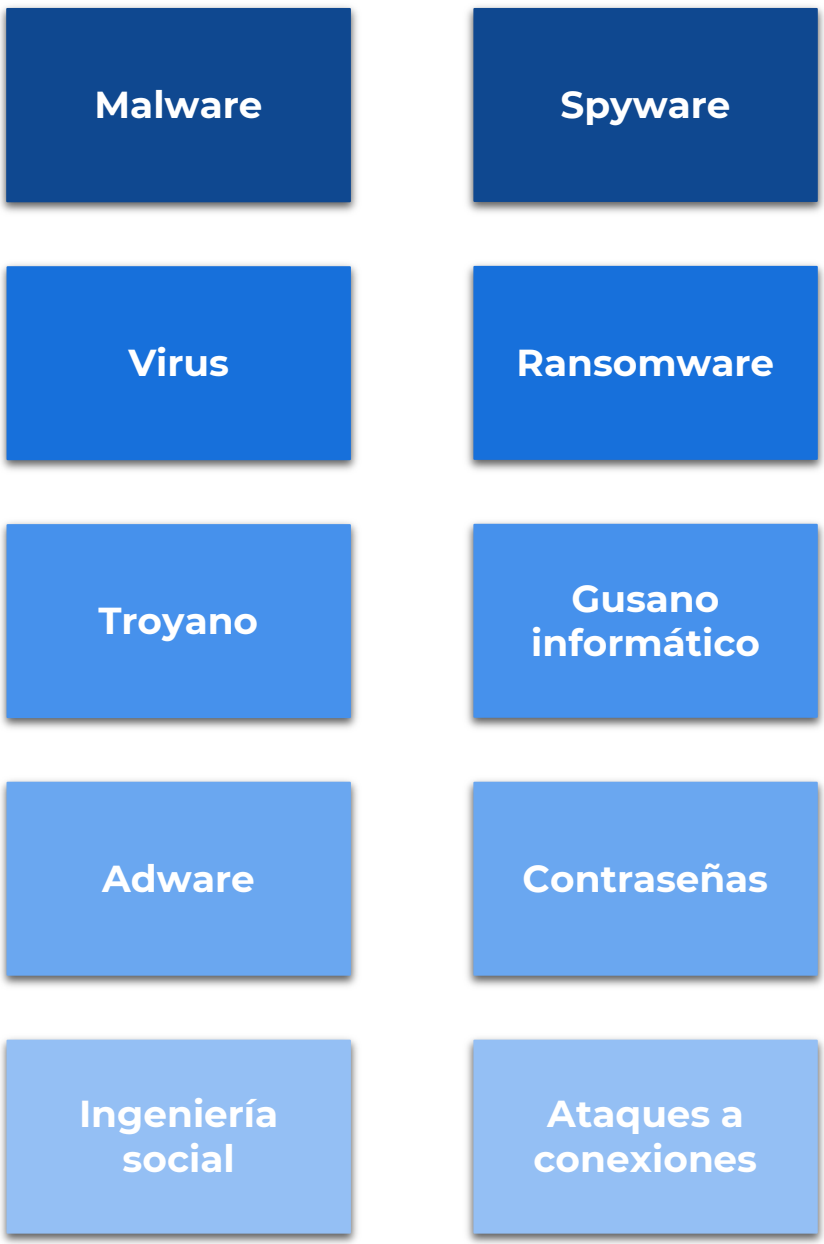
Fuente: Elaboración propia a partir de ManageEngine

3.2. Principales amenazas para las pymes

Ciberseguridad

Principales amenazas de la ciberseguridad para las pymes

Es necesario que todas las entidades, tanto públicas como privadas, protejan de forma completa la información de la que disponen. Por ello, deben tener una buena estructura de seguridad, de forma general o individual (para todos los usuarios de la misma). Las **principales amenazas**, que se explicarán a lo largo de esta sección, son las siguientes:



Ciberseguridad

El ***malware*** se trata de un *software* malicioso que daña los diferentes sistemas. La principal función de este *software* cibercriminal es apropiarse de datos personales, invadir el ordenador de forma que determinadas funciones queden deshabilitadas e incluso espiar la actividad del usuario.

Señales para la detección de un malware

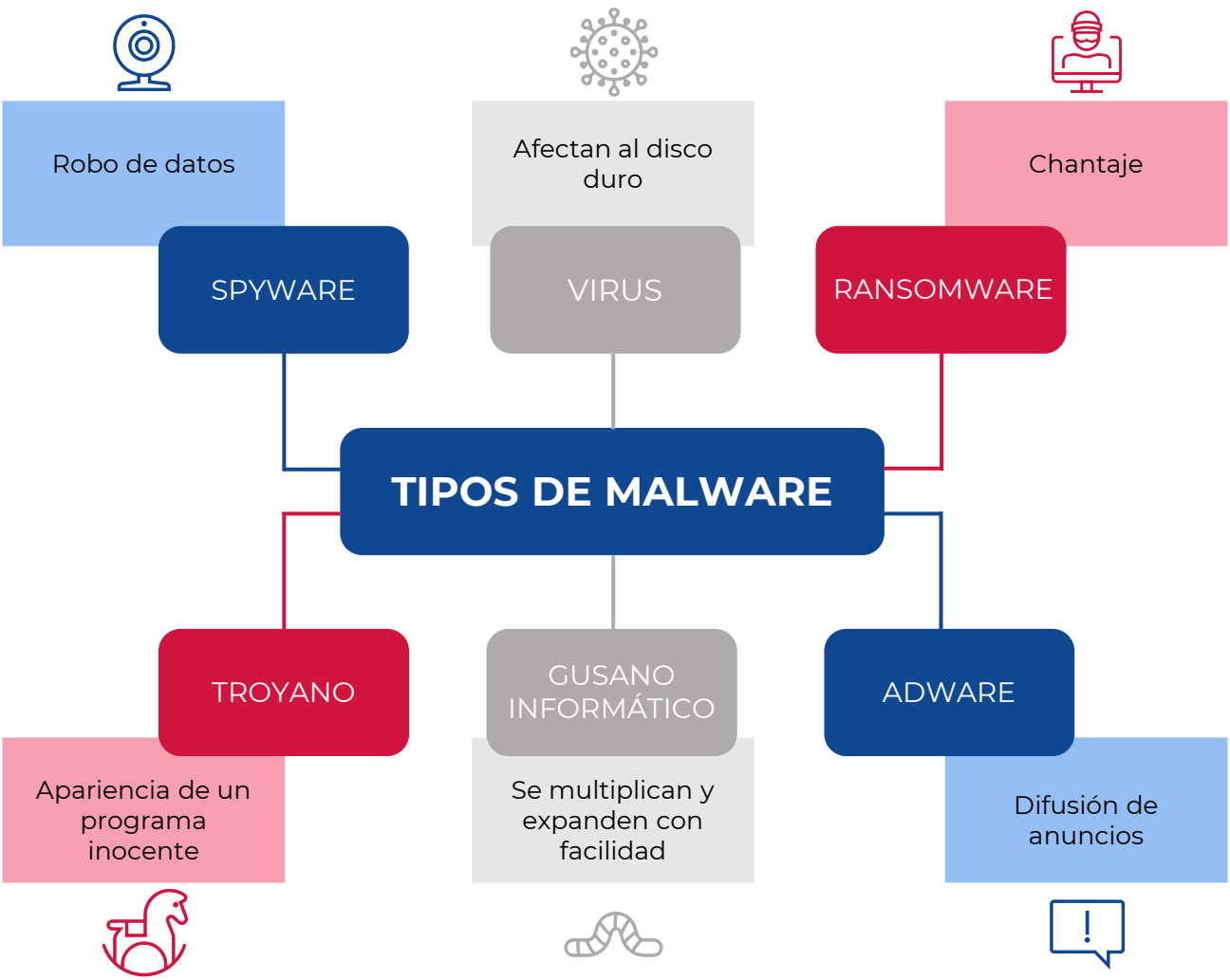
- La velocidad del equipo se ve afectada por este tipo de amenazas, se ralentiza.
- *Blue Screen of Death (BSOD),* es una pantalla azul que no permite realizar ninguna acción sobre tu equipo. Bloqueo del sistema.
- Publicidad constante en la pantalla *(adware).* Los más comunes son los anuncios engañosos que garantizan un premio.
- Advertencia del robo de datos que incluya un mensaje de recuperación mediante un rescate *(ransomware).*
- Nuevos elementos, complementos o barras de herramientas en el navegador y cambios en el mismo.
- Pérdida de espacio en el disco de almacenamiento.
- Funcionamiento de aplicaciones en un segundo plano y aumento de la actividad del ventilador.

Ciberseguridad

El ***malware*** puede acceder al sistema a través de la conexión a Internet del usuario. Lo más común es que el usuario sea atacado mediante búsquedas en el navegador o el correo electrónico.

Hay que prestar especial atención al contenido de Internet, ya que estos *software* pueden encontrarse en archivos de música infectados, barras de herramientas de un proveedor inusual, mensajes maliciosos del correo electrónico, páginas web pirateadas, descarga de aplicaciones de sitios webs desconocidos, juegos *online*, etc.

Sus creadores están involucrados en el vandalismo informático, robo, cibercrimen y negocios oscuros. A continuación, se muestran los principales tipos de *malware*:



Fuente: Elaboración propia a partir de vti

Ciberseguridad

El ***spyware*** se trata de un *software* malicioso cuya finalidad es espiar al usuario infectando dispositivos electrónicos conectados a Internet. Se instala sin permiso a través de archivos, aplicaciones y programas descargados intencionadamente en el equipo. También existen webs maliciosas, enlaces y archivos del correo electrónico que contienen algún tipo de *spyware*.

Su finalidad es, como bien indica su nombre, **espiar cualquier tipo de actividad del propietario del dispositivo**. A través de este *software* se pretenden grabar y robar datos de navegación, páginas web visitadas, compras *online*, contraseñas, datos de las tarjetas de crédito, etc. El creador del *spyware* se apropia de toda esta información y la emplea para su propio beneficio. En la siguiente ilustración se especifica en qué consisten cada una de las posibles actividades de *spyware*.

ROBO DE INFORMACIÓN

- Robo de todo tipo de información personal.

ROBO DE CONTRASEÑAS

- Diseñado para el robo de credenciales de registro.

KEYLOGGERS

- Control del sistema (capturas de pantalla, pulsaciones, etc.)

TROYANOS BANCARIOS

- Acceso y registro de información de la banca electrónica.

SECUESTRO DE MÓDEM

- Desconexión de la línea de teléfono local a una internacional.

Ciberseguridad

Un **virus** es un tipo de *malware* cuyo propósito es alterar el funcionamiento del dispositivo electrónico. Según su actividad pueden dividirse en:

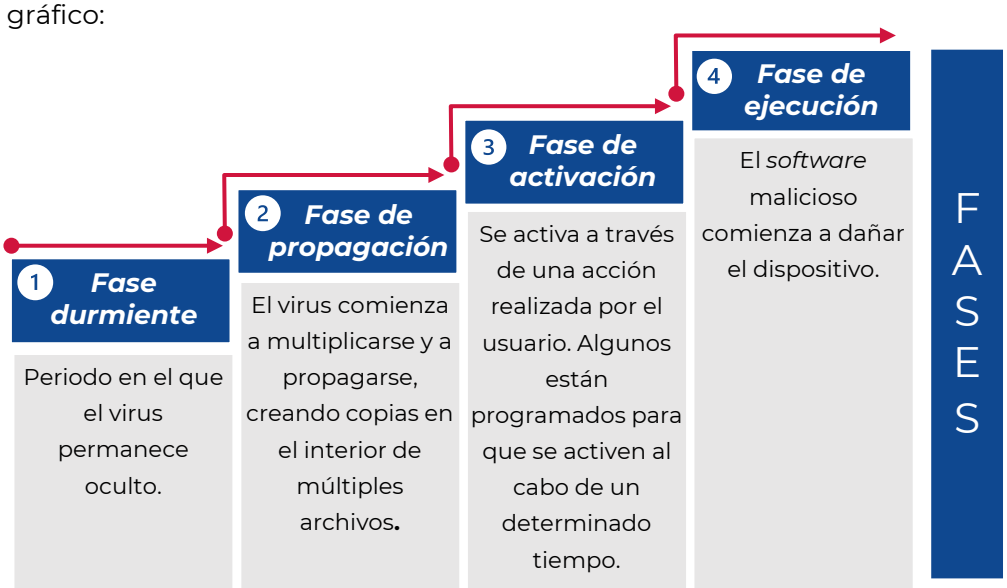
- **Virus informáticos activos:** aquellos que empiezan a funcionar y propagarse en cuanto llegan al equipo.
- **Virus informáticos inactivos:** empiezan a funcionar una vez el usuario los activa inconscientemente.

Propagación del virus informático

Los virus pueden infectar al equipo informático mediante:

1. **Correo electrónico:** los correos electrónicos pueden contener enlaces engañosos, archivos adjuntos ejecutables dañinos (.EXE o .ZIP) e incluso, cuerpos del mensaje infectados.
2. **Descargas:** virus ocultos en aplicaciones, complementos, archivos, en definitiva, todo aquel contenido que se pueda descargar.
3. **Mensajes:** infección a través de servicios de mensajería como Facebook, WhatsApp, Instagram, SMS, etc.
4. ***Software* no actualizado:** el usuario que tenga un dispositivo con el sistema operativo antiguo, puede ser víctima de ciberataques.
5. ***Malvertising*:** virus presentes en anuncios de todo tipo de webs.

Las distintas **fases de actuación** de un virus informático en un equipo aparecen en el siguiente gráfico:



Ciberseguridad

El ***ransomware*** es un tipo de *software que* roba información privilegiada de los usuarios y después amenaza con difundirla en caso de que no se realice un pago. Existen tres tipos de *ransomware*:

- ***Ransomware* de cifrado:** se encarga de cifrar los archivos para que el usuario no pueda tener acceso a ellos. Es el más efectivo de todos ya que una vez se produce el ciberataque es imposible recuperar los archivos secuestrados con la ayuda de *software* de seguridad, por lo que es necesario pagar el rescate. Aun pagando la cantidad indicada por el ciberdelincuente, no hay garantía de se recupere la información robada. Normalmente, el ataque se produce en archivos de ofimática, bases de datos, multimedia o cualquier tipo de archivo de interés o unidad externa al equipo.

  ⚠ **Síntomas**: extensión de archivos desconocida e imposibilidad para abrirlos.

- **Bloqueadores de pantalla:** inhabilita el acceso a los dispositivos bloqueando la pantalla hasta que el usuario pague el rescate. En la actualidad, es fácil de detectar, suele atacar a dispositivos móviles o tabletas. Estos fueron las primeras clases de *ransomware* que empleaban métodos sencillos para tener el control de la pantalla.

  ⚠ **Síntomas**: bloqueo del equipo nada más encenderlo.

- ***Scareware*:** esta variedad de *ransomware* es la más fácil de detectar y evitar. Se trata de un *software* malicioso que engaña a los usuarios para que visiten sitios infestados de *malware*. También se conoce como *software* de engaño, *software* de escaneo fraudulento o *fraudware*.

  ⚠ **Síntomas**: pantalla emergente anuncia la detección de un virus.

Los diferentes tipos de *ransomware* se crearon para atacar a equipos particulares. Con el paso de los años, estos ciberataques empezaron a ser comunes entre las empresas, ya que los ciberdelincuentes eran conocedores del daño que podían causar a los grandes negocios mediante el robo de información privilegiada. Los daños por parte de estos *malwares* han crecido exponencialmente desde su creación. Los ataques a empresas globales empezaron a extenderse a pequeñas y medianas empresas poniendo en peligro todos los negocios.

La forma más común de que un dispositivo sea atacado por un *malware* de esta categoría es mediante los correos de *phishing*, aquellos correos fraudulentos que parecen provenir de una fuente segura y que piden información confidencial, o bien mediante sitios web, descargas y/o conexiones remotas que se aprovechan de las contraseñas débiles, etc.

Ciberseguridad

El **troyano** se trata de un código malicioso que tiene apariencia de un archivo fiable. El usuario ejecuta el *software* nada más iniciar su descarga en el dispositivo informático correspondiente.

Los *troyanos* suelen presentar una serie de características fundamentales:

- **Empleo de *exploits*:** programa informático, parte de un *software* o código que se aprovecha de las deficiencias de seguridad para causar daños en un *software*, *hardware* o cualquier dispositivo electrónico.
- **Presencia en forma de *rootkits*:** extensión del *software* malicioso cuya finalidad es ocultarse en el dispositivo para el acceso y control del mismo.
- **Creación de una *botnet*:** conjunto de dispositivos infectados que reciben órdenes por parte de los creadores.

El *malware* troyano presenta múltiples variaciones, entre las cuales destacan:

- **Troyano de puerta trasera:** un ciberdelincuente toma el control remoto del dispositivo, engañando al propietario del mismo, crea una puerta trasera virtual para acceder al equipo. Así, se descarga información personal y puede llevar a la instalación de otro tipo de *malware*.
- **Troyano de descarga:** se encarga de instalar un programa que lleva a cabo acciones maliciosas en dispositivos infectados.
- **Troyanos de denegación de servicio distribuido (DDoS):** ataque a una red o servidor determinado para la inhabilitación del sistema mediante el envío masivo de información. El servidor web colapsa al no poder procesar todos los datos.
- **Troyanos bancarios:** son los troyanos más comunes, roban información bancaria y se suelen esconder como un programa legítimo.

A pesar de que existan más troyanos, todos tienen unos objetivos comunes que causan daños al equipo invadido.

OBJETIVOS COMUNES DE LOS TROYANOS

- **Bloqueo e inhabilitación del equipo informático.**
- **Eliminación y modificación de información.**
- **Robo de datos para el beneficio del delincuente.**
- **Obstaculizar el rendimiento del servidor y/o red atacada.**

Ciberseguridad

El **gusano informático** se trata de una subclase de virus que se reproduce para infectar y esconderse en diferentes ubicaciones del mayor número de dispositivos informáticos posible. La función principal de los gusanos informáticos o ***worms***, es impedir el acceso a los propietarios de los equipo o usuarios de ciertos servidores mediante su colapso. Se aprovechan de las vulnerabilidades del sistema operativo para llevar a cabo su actividad.

Se puede decir que son *malwares* autónomos ya que no necesitan que alguien los active para que lleven a cabo sus acciones (como sucede con muchos *malwares*). Aunque se puedan relacionar los virus y los gusanos informáticos es necesario conocer sus diferencias:

GUSANO	VS	VIRUS
Programa capaz de multiplicarse e infectar múltiples dispositivos	**Función**	*Software* adherido a archivos ejecutables
Malware autónomo	**Activación**	Requiere acción humana para su activación
Rápido	**Propagación**	Más lento que el gusano
Formatear el equipo o herramienta específica para su eliminación	**Eliminación**	Formatear el equipo o herramienta específica para su eliminación
Firewall, *software* antivirus	**Protección**	*Software* antivirus

Los tipos de gusanos informáticos existentes son los siguientes:

- **Gusanos de correo electrónico:** controlan el correo electrónico del usuario atacado y envían correos no deseados a sus contactos.
- **Gusanos de mensajería instantánea:** envían mensajes no deseados a todos los contactos a través de plataformas de mensajería como WhatsApp o Skype.
- **Gusanos de intercambio de archivos:** gusanos presentes en las plataformas de intercambios de archivos multimedia, suelen ser sitios webs no regulados.
- **Gusanos de red:** son aquellos que se aprovechan de las vulnerabilidades de los sistemas operativos y se propagan a otros equipos que presente las mismas características.

Ciberseguridad

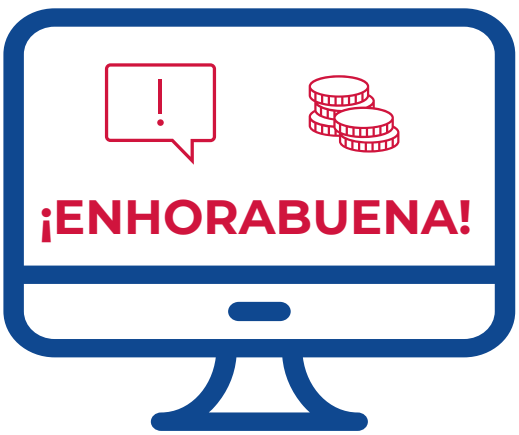
El ***adware*** se trata de un *software* malicioso encargado de bombardear al usuario con anuncios en la pantalla del dispositivo electrónico. Se encarga de recopilar información de la actividad del usuario para mostrar anuncios dirigidos. Además de suponer una molestia, pueden ocasionar el mal funcionamiento del equipo.

Existen dos formas de que un usuario sea víctima de algún tipo de *adware*:

1. **Instalación de un programa (gratuito o compartido):** este tipo de programas pueden contener *adware* debido a un acuerdo entre el creador del *software* y del programa para obtener beneficios. Esta publicidad hace posible que su descarga sea gratuita. Cabe destacar que algunos programas de pago también contienen *adware*.
2. **Descarga involuntaria de un sitio web:** el *adware* se aprovecha de algún tipo de vulnerabilidad en el explorador mientras el usuario navega por diferentes sitios webs, una vez infecta el equipo deseado, recopila datos personales, lanza anuncios maliciosos, etc.

Algunas señales que indican la presencia de un *adware* en los equipos informáticos son:

- Anuncios recurrentes inusuales.
- Cambios sospechosos en la página de inicio del navegador como nuevas barras de herramientas o extensiones.
- Sitios webs con aspectos diferentes.
- Ralentización o bloqueo del explorador.
- Enlaces que redirigen a sitios webs diferentes.



SOLUCIONES DE PROTECCIÓN

Evitar la descarga de aplicaciones o sitios webs desconocidos. Se recomienda estudiar detalladamente los pasos de instalación de los programas y aplicaciones para verificar que no se descarguen elementos maliciosos. Se recomienda hacer clic en "*Opciones de instalación*" o "*Instalación Avanzada*".

Ciberseguridad

Las **contraseñas** son uno de los **principales objetivos** de los ciberdelincuentes. Muchas veces, los usuarios les facilitan su robo mediante actos que comprometen la seguridad informática de sus dispositivos electrónicos:

- ✖ Uso de contraseñas débiles (emplear nombres comunes, fechas de nacimiento, etc.).
- ✖ Utilizar la misma contraseña en múltiples sitios web.
- ✖ Emplear contraseñas tipo (incluir solamente una letra mayúscula, 4-5 minúsculas y un número o un carácter especial).
- ✖ Guardar las contraseñas en notas o archivos sin cifrar.

Para descubrir las contraseñas, los ciberdelincuentes pueden realizarlo de dos maneras, las cuales se explican a continuación:

Ataques por fuerza bruta

Los delincuentes consiguen descifrar la contraseña a base de ***prueba y error***. Combinan múltiples caracteres relacionados con datos personales del usuario hasta que consiguen descifrar el patrón.

OBJETIVO: contraseñas vulnerables

Ataques por diccionario

Los cibercriminales descubren las credenciales mediante el uso de un *software* especializado. Este programa realiza combinaciones de forma automática, empezando por las más sencillas hasta las más complejas.

Ciberseguridad

La **Ingeniería social** es un método muy común entre los ciberdelincuentes basado en la manipulación. Los atacantes tratan de ganarse la confianza de la víctima para que revele información personal y así, tomar el control de sus dispositivos informáticos. Los tipos de ataques por medio de la ingeniería social son los siguientes:

- ***Phishing, Vishing y Smishing*:** el cibercriminal envía un mensaje de carácter urgente a través de redes sociales, llamadas telefónicas o servicios de mensajería, haciéndose pasar por una entidad legítima, es decir, un banco, soporte técnico, entidad pública o cualquiera que parezca de confianza para poder engañar al usuario.
- **Fraudes *online*:** se tratan de estafas *online* con las que el atacante se apropia de datos o solicita un pago para devolver cierta información sensible.
- ***Spam*:** envío de una gran cantidad de anuncios publicitarios no deseados, algunos de ellos pueden contener *malware*. La principal fuente de difusión suele ser el correo electrónico.
- ***Dumpster Diving*:** este método se conoce como *"buscar en la papelera"*. Suele ser un ataque dirigido a usuarios concretos o a grandes empresas en el que el delincuente informático accede a datos a través de los documentos de la papelera.
- **Gancho o *Baiting*:** los dispositivos se infectan mediante el uso de un medio físico, este puede ser un USB o disco duro, colocado en un sitio estratégico para que el usuario lo encuentre y lo conecte a su equipo. Esta técnica también es conocida con el nombre de cebo.
- ***Shoulder surfing*:** el robo de información se consigue en espacios públicos, *"mirando por encima del hombro"* sin que el usuario pueda darse cuenta de que alguien le está espiando.

SOLUCIONES DE PROTECCIÓN

- **¡Prestar atención!** Leer todos los mensajes detenidamente, sobre todo aquellos mensajes que sean demasiado atractivos.
- Configuración del filtro antispam y no emplear jamás el correo corporativo para el registro de promociones *online*.
- Eliminar la información de forma segura y permanente.
- Evitar la conexión de dispositivos físicos desconocidos.
- Asegurar los equipos electrónicos en espacios públicos (filtros anti-espía, verificar que no hay terceros pendientes de los dispositivos, etc.).

Ciberseguridad

Otras de las amenazas más frecuentes en este ámbito son los **ataques a las conexiones** mediante ciertas herramientas o *software* destinados a infectar los dispositivos. En este tipo de ataques, lo normal es que el delincuente se interponga entre la información suministrada por el usuario y el sitio web de destino. Dentro de los ataques a las conexiones podemos incluir:

- **Redes trampa:** creación de una red wifi falsa con el mismo nombre (o muy parecido) que una legítima, suele encontrarse en lugares que presenten una red wifi abierta para engañar al mayor número de usuarios posible.
- **Ataques a *cookies*:** robo o alteración de la información presente en los ficheros web relacionada con la navegación del usuario.
- **Ataques DDoS:** ataques simultáneos a un determinado equipo para colapsarlo y que el propietario no pueda acceder a él.
- **Inyección SQL:** ataque a las bases de datos que presentan el lenguaje de programación SQL mediante la introducción de códigos maliciosos.
- ***Spoofing*:** conjunto de técnicas de *hacking* para la suplantación de identidad, se distinguen varias categorías:
    - *IP Spoofing*: falsificación de la dirección IP para introducir un *software* malicioso en varios dispositivos y robar información.
    - *Web Spoofing*: sustitución de una página web segura por una copia falsa que emplea una URL y una apariencia muy similar.
    - *Email Spoofing*: suplantación del correo electrónico para enviar información masiva, Spam, bulos o fraudes.
    - *DNS Spoofing*: redirección de sitios webs debido a una suplantación de la DNS, Domain Name System, es decir, los cibercriminales consiguen infectar el router de las víctimas.
- **Escaneo de puertos:** programa destinado a la inspección de los puertos de un equipo para averiguar vulnerabilidades y robar información.
- ***Man in the middle*:** el ciberdelincuente se entromete entre la actividad del usuario y el servidor a través de redes wifi falsas o públicas.
- ***Sniffing*:** instalación de un programa de escucha para controlar la actividad de una web. En esta práctica se emplean herramientas de *hacking* conocidas como *sniffers*.

3.3. Cómo proteger mi pyme

Ciberseguridad

Procedimientos para garantizar la seguridad informática

Según Marc Martínez, experto en Ciberseguridad, **la mayor parte de los ataques cibernéticos son causados por error o desconocimiento humano**. En muchos casos, los piratas informáticos se aprovechan de las **vulnerabilidades** provocadas por los propios usuarios. Por ello, es necesario que cada una de las personas que poseen un equipo electrónico presten atención y tomen precauciones para evitar las amenazas que atentan contra seguridad informática.

- ✓ **Instalación de un programa de seguridad:** cada equipo debe tener instalado un antivirus para la detección de posibles ciberataques y control de los archivos almacenados en el ordenador.
- ✓ **Actualización de *software*:** las actualizaciones suelen incluir correcciones que subsanan vulnerabilidades detectadas en versiones anteriores.
- ✓ **Desactivación de la reproducción automática de medios extraíbles:** se recomienda desactivar esta opción del dispositivo para evitar la reproducción automática de ciertos tipos de *malware*.
- ✓ **Inspección de los archivos recibidos:** revisión de la información recibida (correos electrónicos, archivos, etc.).
- ✓ **Navegación segura en la web:** navegar por sitios web seguros, bajo el protocolo HTTPS.
- ✓ **Uso de navegadores seguros:** empleo de navegadores como Google Chrome, Safari o Firefox Mozilla.
- ✓ **Herramientas informáticas adicionales:** acceso a la web a través de una red VPN (red virtual privada) e instalación de un cortafuegos o *firewall*.
- ✓ **Formación sobre la ciberseguridad:** las empresas deben de proporcionar un protocolo para el tratamiento de la información confidencial y la manera de actuar ante la existencia de un peligro.
- ✓ **Cifrar sistemas:** encriptación de la información a través de herramientas como PGP *(Pretty Good Privacy)*.

> *"Lo primero que deberían hacer las pymes es analizar en qué nivel de madurez en ciberseguridad se encuentran e identificar los activos que pueden proteger, dando prioridad a las llamadas "joyas de la corona", es decir, aquellos activos críticos para sus negocios. Este análisis de madurez es un buen punto de partida para establecer, en un plazo de uno o dos años, los controles que permitan reducir el nivel de riesgo hasta un nivel razonable".*
>
> **Marc Martínez, Socio de Ciberseguridad y Technology Risk en KPMG**

Ciberseguridad

Recomendaciones de ciberseguridad para pymes y autónomos

Los ciberataques aumentan todos los años, afectando a usuarios individuales y a diferentes empresas. Uno de los mitos más comunes, relacionado con este tipo de delitos, es que solamente perjudican a grandes empresas. Sin embargo, en 2021 el 44% de las pymes españolas sufrió al menos un ciberataque, según Hiscox. Por ello, es necesario tener en cuenta las siguientes recomendaciones relacionadas con la seguridad informática para pymes y autónomos.

¿Cómo hacer mi pyme más segura?

Políticas de seguridad: es importante mantener actualizadas las políticas de ciberseguridad para empleados que cuenten con protocolos de actuación correspondientes y la formación adecuada.

Instalación de cortafuegos y antivirus: el cortafuegos y antivirus son los primeros elementos que debe adquirir una empresa para la detección y bloqueo de accesos no autorizados.

Uso exclusivo de equipos corporativos: la información debe ser tratada exclusivamente por medio de los dispositivos electrónicos de empresa, con la configuración predeterminada.

Protección de las credenciales: mantener los datos del usuario y contraseña privados.

Evitar la difusión de información: no se deben mantener conversaciones confidenciales delante de terceros, mantener el puesto de trabajo libre de información sensible (bloqueo de ordenador), etc.

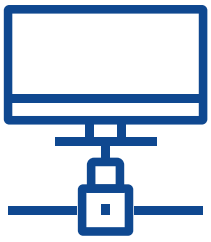
Cifrar y asegurar la información: realizar copias de seguridad de los archivos y encriptar la información y dispositivos extraíbles que proceda.

Ciberseguridad

Recomendaciones de ciberseguridad para pymes y autónomos

Las nuevas tecnologías permiten mantener conectados a todos los empleados y empleadas, permitiendo que continúen su trabajo desde casa o desde cualquier parte del mundo. El objetivo del teletrabajo es ofrecer una mayor flexibilidad a la persona trabajadora, pero **¿cuáles son las precauciones que se deberían tomar para no sufrir un ataque cibernético?**

Seguridad fuera de mi pyme: Teletrabajo



1. En el momento en el que los trabajadores y trabajadores no estén en la oficina, además de proteger tus equipos empleando medidas de seguridad como:
   - Pantallas de protección
   - Contraseñas seguras
   - Sistemas de seguridad antivirus
   - Encriptación de archivos

   La mejor forma de proteger una empresa es conectarse a ella a través de **una red privada virtual (VPN)** así, la información quedará completamente cifrada a través de Internet.

2. Evitar la conexión de otros dispositivos electrónicos (televisión, relojes inteligentes, asistentes virtuales como, etc.) a los equipos corporativos para protegerse de los ataques de los ciberdelincuentes que puedan tener acceso a ellos.

3. Configuración correcta y segura de la red wifi de casa y evitar en todo momento la conexión a redes wifi públicas.

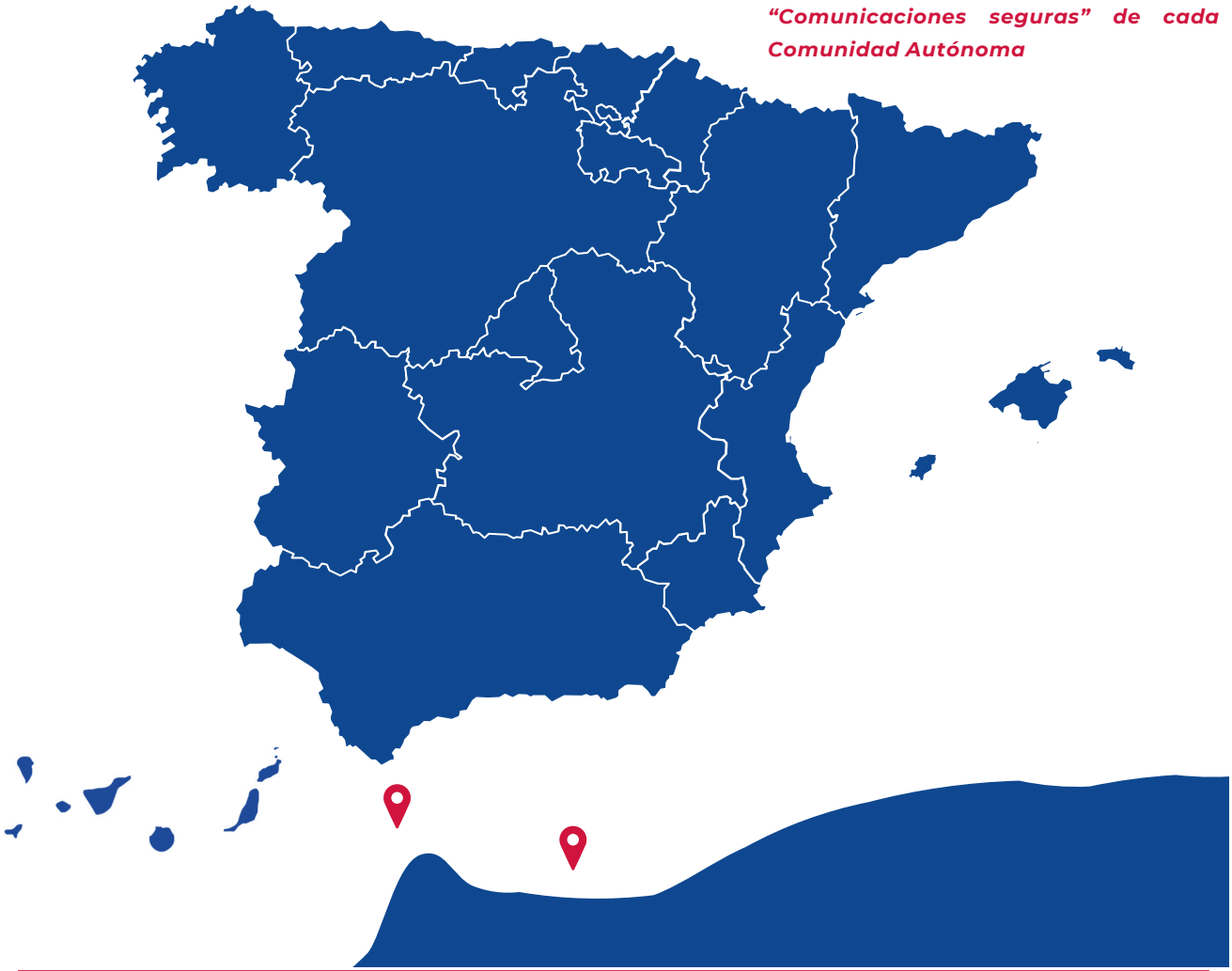
Ciberseguridad

Recursos y digitalizadores para mi pyme

En el mapa que aparece a continuación se presenta un Catálogo de digitalizadores con una serie de soluciones para promover la digitalización de pymes y autónomos. El Catálogo se ha desarrollado en el marco del Programa Kit Digital, iniciativa del Gobierno de España.

Así, el Catálogo de digitalizadores incluye una serie de Agentes Digitalizadores, tanto públicos como privados, que ofrecen las diferentes soluciones digitales del Kit Digital. Así, dos de las soluciones son "Ciberseguridad" y "Comunicaciones seguras", enfocadas a proporcionar seguridad básica y avanzada para los dispositivos y en las conexiones de los empleados. **Haz *click* en el mapa y accede al catálogo de agentes que ofrecen las soluciones "Ciberseguridad" y "Comunicaciones seguras" en tu Comunidad Autónoma.**

Haz clic para acceder al catálogo de digitalizadores que ofrecen las soluciones "Ciberseguridad" y "Comunicaciones seguras" de cada Comunidad Autónoma



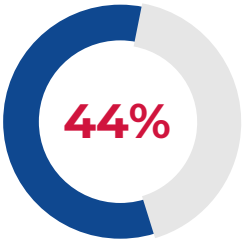
3.4. Situación presente y escenarios futuros

Ciberseguridad

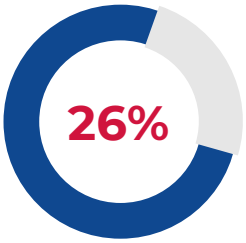
La Ciberseguridad en la actualidad

En 2021 se incrementaron considerablemente los ciberataques en empresas españolas y, entre ellas, **las pymes son las que son más vulnerables ante ellos**. Al no tener la suficiente seguridad para hacer frente a estos ataques, las pymes suelen ser el objetivo de las ciberbandas, debido a que son más vulnerables.

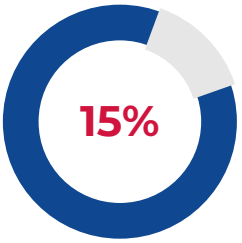
Los **ciberataques más comunes** suelen ser los que buscan la suplantación de identidad, explotando el fenómeno del phishing. Otros como el *ransomware* o *malware* también están a la orden del día. Por lo tanto, ante tanta posible amenaza, **es vital incrementar la ciberseguridad en las pymes**, primero analizando los factores que favorecen su aparición y, en segundo lugar, buscando la manera de detenerlos. En las gráficas que se muestran a continuación se ofrecen unos datos relevantes acerca de cómo ha afectado la ciberdelincuencia a las pymes en el último año.



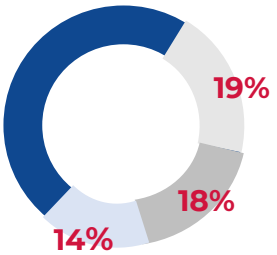
El 44% de las pymes españolas *han sufrido al menos un ciberataque grave en 2021*



La ***media de incidentes*** *ha* ***aumentado un 26%*** *con respecto a 2020*



Las empresas que imparten ***más de 20 horas de formación a sus empleados*** *han recibido únicamente el* ***15% de los ataques*** *en 2021*



El phishing ***19%,*** *el ransomware* ***18%*** *y malware* ***14%*** *son las* ***amenazas más importantes***

Fuente: Elaboración propia. Datos a partir de Europapress.

> *Según un estudio de* ***Europapress****, el* ***66% de los comités de dirección considera a la ciberseguridad un tema relevante*** *que es tratado periódicamente, experimentando un incremento del 25% respecto a 2020.*

Ciberseguridad

Escenarios futuros de desarrollo

Debido al aumento de los ciberataques, las empresas han optado por invertir en sistemas de ciberseguridad cada vez más **sofisticados**. Se prevé que un 70% de las empresas españolas (frente al 50% del año 2021), habrá incrementado su presupuesto en materia de seguridad informática en 2022.

La lucha contra los ataques causados por las diferentes **ciberamenazas** que inhabilitan el funcionamiento de los dispositivos electrónicos, roban información o infectan el ordenador con diferentes tipos de *malwares*, resulta ser una de las principales preocupaciones de, prácticamente, todas las entidades. Por ello, cada año surgen nuevas herramientas para combatir los daños causados por ciberdelincuentes.

Las **tendencias futuras de la ciberseguridad** avanzan hacia los siguientes recursos:

Centro de Operaciones de Seguridad (SOC)

La mayoría de las compañías apostarán por la creación de un SOC. Estos centros son **unidades centralizadas encargadas de la prevención, control y resolución de ataques cibernéticos**, con la ayuda del personal y la tecnología adecuada.

Las compañías tendrán que optar por un servicio externo o interno.

Biometría conductual

Gracias a la Inteligencia Artificial, la biometría conductual estará más presente en las empresas para garantizar la seguridad efectiva de los dispositivos electrónicos.

Consiste en la **medición del comportamiento,** así como el **reconocimiento de los rasgos fisiológicos** para la detección de intrusos.

Ciberseguridad

Escenarios futuros de desarrollo (cont.)

Proveedores

A partir del año 2022, **los acuerdos entre entidades y proveedores tendrán que realizarse en base a los sistemas de seguridad informática** que tengan estrategia clave para garantizar la seguridad informática.

Es decir, que un proveedor tenga un determinado protocolo de ciberseguridad será determinante para su contratación.

Next-Gen SWG

Solución innovadora para la protección de todo el contenido almacenado en la nube.

Se encargará de la **prevención de ataques causados por *malware*, detección de ataques sofisticados, protección de datos y control del uso de aplicaciones** por parte de cualquier usuario, dispositivo o localización.

Teletrabajo

Como ya se ha mencionado a lo largo de este documento, el teletrabajo ha aumentado desde la crisis sanitaria producida por a Covid-19.

Esta nueva forma de trabajo seguirá desempeñándose en el futuro, las diferentes entidades seguirán incluyendo sistemas de protección como VPNs o firewalls.

4. Impacto en sectores y empresas

Impacto en empresas y sectores

Beneficios de la ciberseguridad para las empresas

Las empresas son las entidades más vulnerables frente a las actividades cibernéticas delictivas. Esto se debe a la cantidad de información privilegiada que almacenan en sus dispositivos electrónicos.

La seguridad informática aporta una serie de ventajas para la mejora de la actividad de las compañías y de toda persona que posea un equipo informático.

- *Protección de dispositivos electrónicos*
- *Privacidad de la información*
- *Cultura de la seguridad informática*
- *Mejora de la imagen corporativa*
- *Ayuda en la toma de decisiones*
- *Índices de seguridad controlados*

1. Uno de los objetivos principales de la práctica de esta actividad en las empresas, es **proteger los equipos** de cualquier tipo de ataque físico (robos, incendios o cualquier tipo de destrucción de los dispositivos).
2. Mantener **privada la información** de los equipos y los datos disponibles en la red mediante la instalación de ciertos sistemas: antivirus, claves de acceso complejas, cortafuegos, acceso restringido de ciertos archivos, etc.
3. Crear una serie de pautas para la **implementación de la seguridad informática.**
4. Mejorar la **imagen de las empresas**, con el objetivo de que los clientes estén seguros de confiarles información sensible.
5. Ayudar a los usuarios a **tomar un mayor número de decisiones** positivas, ya que es posible detectar los posibles peligros del manejo de cierta información a través de Internet.
6. Permite **mantener un control** para la prevención de determinadas amenazas en base a los ataques cibernéticos más comunes.

Impacto en empresas y sectores

Casos de ataques cibernéticos en España

Según el **Instituto de Ciberseguridad (INCIBE)**, en 2021 en España se produjeron una media de 40.000 ciberataques al día, de los cuales el 75% van dirigidos a pymes. Esto supone un incremento del 125% con respecto al 2020. Algunos de los ataques más importantes producidos en los últimos años han sido:

Casos de ciberataques

Mercado Libre

Pirata informático

En 2022, esta multinacional argentina dedicada al comercio electrónico sufrió la filtración de datos de más de 300.000 usuarios. Además, los ciberdelincuentes accedieron a parte del código fuente de la organización.

Según el comunicado oficial, este ciberataque no significó la pérdida de información como contraseñas de usuarios, balances de cuenta, inversiones, datos financieros o tarjetas de pago.

Uber

Ingeniería social

En 2022, sufrió un ciberataque de alto nivel en el cual los ciberdelincuentes consiguieron acceder a sus sistemas, en primer lugar, engañando a través de ingeniería social a un empleado y logrando el acceso a su VPN y, seguidamente, escaneando la Intranet. Con ello, consiguieron acceder a los datos de millones de usuarios.

Otros de los sistemas vulnerados fueron la consola de Amazon Web Services de Uber, el panel de administración de correo electrónico de Google Workspace, el servidor Slack y las máquinas virtuales VMware ESXi.

Impacto en empresas y sectores

Casos de ataques cibernéticos en España

Casos de ciberataques

Glovo

Pirata informático

La *startup* española de reparto a domicilio fue víctima de un ciberataque a través del cual se pudo acceder a información sobre clientes y trabajadores de la compañía.

Glovo asegura que no se difundió ningún tipo de información confidencial ya que, Alex Holden, fundador de Hold Security identificó el problema a tiempo. El *hacker* fue capaz de tener acceso a la empresa debido a una interfaz de panel de administración antigua.

MediaMarkt

Bloqueo de los servidores

La multinacional MediaMarkt sufrió un ataque por *ransomware* que bloqueó múltiples servidores en plena campaña del Black Friday. Las tiendas afectadas se encontraban en España, Holanda, Bélgica y Alemania. Como medida de prevención los sistemas de venta, devolución y gestión on-line se paralizaron ya que hubo unos 3.000 dispositivos involucrados en este acontecimiento.

Facebook

Difusión de datos sensibles

Los datos de unos 533 millones de usuarios de Facebook fueron publicados en la web. En España se compartió información personal (nombres completos, números de teléfono, etc.) de 11 millones de cuentas.

Impacto en empresas y sectores

La importancia de la ciberseguridad en diferentes sectores

Sector de la salud

El sector de la salud ha experimentado un gran cambio desde la pandemia causada por el Covid-19. La medicina ha avanzado hacia la telemedicina y la salud digital a través de herramientas informáticas apropiadas para la asistencia médica. Según INCIBE, con esta digitalización del sector han aumentado los ciberataques en un 48%, por lo que es necesario incrementar la ciberseguridad para combatir contra la exposición y vulnerabilidad de los equipos conectados a la red para la protección de todos los ciudadanos.

Sector turismo

En España, el sector turístico ha evolucionado de acuerdo con las tecnologías, cambiando la forma de interacción entre los turistas: *check-in* virtual, tarjetas de habitaciones virtuales, reseñas en internet por parte de los clientes, etc. Este avance tecnológico ha hecho que viajar sea más sencillo, pero también ha convertido a este sector en un objetivo muy atractivo para los ciberdelincuentes. Es necesario que dicho crecimiento esté acompañado de la seguridad informática apropiada y así, mantener protegidos a todos los clientes y trabajadores tal y como indica el Instituto Tecnológico Hotelero.

Sector financiero

Las tácticas para cometer delitos y fraudes financieros se han adaptado al mundo digital consiguiendo atacar a miles de clientes y entidades financieras. La mayoría de los ataques por parte de los ciberdelincuentes son por *malware*, fraude, ingeniería social y de denegación de servicio distribuido, para conseguir beneficio económico. Además de perder dinero, las compañías y sus clientes se exponen al riesgo de que se compartan todo tipo de datos de carácter sensible. Las entidades financieras deben invertir sus recursos en reforzar su ciberseguridad.

Impacto en empresas y sectores

La importancia de la ciberseguridad en diferentes sectores

Sector industrial

La ciberseguridad de la Industria 4.0 juega un papel esencial en su desarrollo y trata conceptos relacionados con la seguridad de las instalaciones y su optimización, protección de los procesos de producción y de la información confidencial relativa a dicha producción. Cabe destacar que la seguridad física y virtual de una industria está interconectada:

- Medidas de protección en el diseño y uso de la maquinaria.
- Asegurar todos los dispositivos para cumplir los protocolos de seguridad.

Sector agroalimentario

La evolución global hacia las nuevas tecnologías ha causado un impacto en el sector agroalimentario, ayudando a aumentar su rentabilidad y llevar a cabo una digitalización del mundo rural. Esta transformación favorece a la ecologización y al cambio climático, pero es necesario tener en cuenta las posibles amenazas cibernéticas que atentan contra las fases de la cadena agroalimentaria (producción, industrialización, distribución y venta).

Sector telecomunicaciones

Las Tecnologías de la Información y la Comunicación (TIC) son parte de la cultura tecnológica de todas las empresas, administraciones y ciudadanos. Por lo que es lógico que la ciberseguridad se haya convertido en un factor clave para todos los sectores. Muchas empresas de telecomunicaciones se dedican exclusivamente a ofrecer sistemas de seguridad que garantizan la protección, seguridad y disponibilidad de la información de las compañías, trabajadores y usuarios.

Impacto en empresas y sectores

La importancia de la ciberseguridad en diferentes sectores

Sector del transporte

En la actualidad, la mayoría de los transportes presentan nuevos servicios de conectividad, debido a las tecnologías inalámbricas y de red. Es por esto, que la mayoría de los vehículos, particulares o profesionales, incluyen todo tipo de dispositivos electrónicos conectados a Internet (asistentes virtuales, GPS, etc.).

Estas nuevas incorporaciones tecnológicas resultan ser nuevas líneas de ataque para los ciberdelincuentes, lo que supone un peligro para la economía (empresas de transporte de mercancías) y para la sociedad.

Sector de la energía

La energía es necesaria para el desarrollo de la economía de un país. Por ello, el suministro de energía debe ser continuo, sin ningún tipo de interrupción, garantizando un buen funcionamiento de las entidades encargadas de realizar esta actividad. La posible falta de alguna de las fuentes de energía (electricidad, gas y petróleo) impactaría directamente en la sociedad, causando desperfectos en prácticamente todos los sectores. Para evitar cualquier daño de distribución de energía en el país, a causa de un ciberataque, se necesitan los sistemas de seguridad informática.

Sector químico y farmacéutico

Sector atractivo para los delincuentes de Internet debido a la información sensible que manejan las industrias químicas. Todas las plantas de producción de este sector emplean las tecnologías de la información para optimizar sus procesos. La protección es necesaria tanto a nivel interno como externo, ya que la información compartida sobre la cadena de producción puede ser muy valiosa y perjudicial para el negocio, en caso de que fuese pública.

Impacto en empresas y sectores

La importancia de la ciberseguridad en diferentes sectores

Sector de servicios de emergencia

Los sistemas de seguridad son imprescindibles para garantizar el funcionamiento de los servicios de emergencias, así como de sus infraestructuras, las cuales incluyen la gestión y coordinación de dichos servicios.

La Comunidad de Madrid ha impulsado un modelo de seguridad para reforzar los instrumentos encargados de detectar y eliminar los ciberataques. Garantizando así, la seguridad informática durante la gestión de crisis.

Sector del deporte

Las empresas de ciberseguridad aportan, cada vez más, soluciones de seguridad a las grandes compañías del deporte. Este sector, ha avanzado mucho tecnológicamente, empleando diferentes herramientas para la gestión de su servicio.

Un ejemplo de esto son los clubes de fútbol y sus jugadores, que suelen ser personalidades públicas, sus dispositivos electrónicos contienen información personal que no debería ser expuesta públicamente.

Sector público

La importancia de la ciberseguridad en el sector púbico se considera de carácter primordial en la sociedad. Las tecnologías ofrecen numerosas oportunidades a todos los ciudadanos y ciudadanas y, la dependencia de la sociedad es innegable.

Mantener el ciberespacio seguro es uno de los principales retos del sector público, procurando la privacidad y libertad de todas las personas. Para ello, todas las administraciones públicas deben colaborar conjuntamente.

Impacto en empresas y sectores

Citas de autoridad

Marc Martínez — ***Socio de Ciberseguridad y Technology Risk en KPMG***

"En la actualidad, todas las empresas están en el ojo del huracán. Las grandes empresas son muy atractivas porque la superficie de ataque es mayor y por tanto hay más posibilidades de realizar fraudes y lucrarse con ellos. En las Pymes, aunque el botín suele ser más pequeño, suelen estar muy poco protegidas, por lo que el atacante tiene que esforzarse menos para conseguir su objetivo".

Gabriela Ratti — **Directora General de Ciberseguridad y Protección de la Información del Ministerio de Tecnologías de la Información y la Comunicación.**

"El COVID-19 fue utilizado por muchos criminales como "gancho" en múltiples engaños o fraudes digitales (phishing, scam, estafas mediante ingeniería social y otros.)".

"Muchas personas y organizaciones aumentaron su dependencia de las tecnologías y digitalización, por lo cual tomaron mayor conciencia de su importancia y reportaron los ataques que antes, muchas veces, eran ignorados".

Marcos Gómez — **Subdirector de Servicios de INCIBE-CERT**

"Se han registrado 4.000 dominios '.es' maliciosos relacionados con el COVID-19. Aunque muchos de ellos no han llegado a ver la luz gracias a INCIBE y Red.es. Solo el tres por ciento lo han hecho y han podido tener un posible perjuicio para ciudadanos y empresas".

Rosa Kariger — **Global CISO de Iberdrola, Copresidenta de los Sistemas de Resiliencia Cibernética: grupo de trabajo de electricidad.**

"Solo uniendo esfuerzos podremos hacer frente a los retos de la ciberseguridad introducido por el aumento de la digitalización y la hiperconectividad".

"La ciberseguridad tiene que formar parte de la toma de decisión de los negocios".

5. Casos de éxito

Casos de éxito

Casos de éxito en pymes y autónomos

Por último, desarrollamos casos de éxito de pymes y autónomos, que gracias a sus estrategias de ciberseguridad han conseguido grandes beneficios en sus empresas. Estas empresas **han sabido proporcionar y garantizar la seguridad en su empresa y en los dispositivos de sus empleados.**

Las estrategias de ciberseguridad han ayudado a estas empresas a **protegerse** en una época **totalmente tecnológica**, donde la mayoría de la **información** se encuentra en **formato digital**. En ocasiones, las pymes no tienen en cuenta la ciberseguridad al pensar que, dado el volumen de su negocio, la información generada de la empresa no contiene valor para los ciberdelincuentes. Sin embargo, al no proteger los datos o no destinar los recursos necesarios, la intrusión de los ciberdelincuentes resulta mucho más fácil.

Por ello, estos **casos de éxito** suponen un **referente** en el ámbito de la ciberseguridad, ya que a través de diferentes herramientas y/o métodos, han **protegido sus datos y los de sus clientes**, **evitando** cualquier **amenaza a la integración de la información**. Además, las empresas han logrado proteger la información de sus clientes, que los empleados trabajen con seguridad, proteger la proactividad, proteger sus sitios web y plataformas de redes sociales, prevenir ciberataques y, así, inspirar mayor confianza a sus clientes.

A continuación, se presentan **casos de éxito de pymes y autónomos** que han sabido aprovechar las estrategias de ciberseguridad para, entre otros, proteger los activos digitales de su empresa, identificar vulnerabilidades y aplicar sistemas, métodos y herramientas que garanticen la integridad de los datos.

Adicionalmente, de cara a entender en mayor profundidad casos de éxito destacables, **se han realizado una serie de entrevistas a pymes y autónomos en relación con sus estrategias de ciberseguridad**. Entre otros, se les entrevistó acerca de los objetivos de su estrategia, los métodos de ciberseguridad empleados, los ciberataques recibidos y las soluciones implementadas, las tendencias futuras, etc.

Casos de éxito

Entrevistas a pymes y autónomos

Atalanta Madera

Atalanta madera es una empresa dedicada a la **tornería artesanal en madera** formada por Isabel y Ana Neira, la 7ª generación de la familia Neira dedicada a este sector. Ana e Isabel se dedican al diseño, torneado y acabado de los objetos artesanales que crean, además del ideado de los diferentes tipos de *packaging*. Atalanta Madera cuenta actualmente con un **sitio web con información de la empresa**, además de un ***e-commerce*** donde venden artículos de cocina, baño, juguetes y más artículos elaborados **artesanalmente en madera,** a ser posible, **de proximidad.** Así, Atalanta Madera, con el apoyo del programa Smart Peme de la Diputación de Pontevedra, ha implementado en su empresa una serie de **herramientas y métodos para proteger su información y la de sus clientes.**

¿Qué papel juega la ciberseguridad en vuestra empresa?

Para nosotras **siempre ha sido importante proteger los datos**, a pesar de ser una empresa pequeña. En 2018, a través del programa Smart Peme, creamos nuestra propia página web y, con esto, nos dimos cuenta de la necesidad de contar con seguridad de la información. Éramos conscientes de que, como cualquier usuario de internet, éramos un **blanco fácil para los ciberdelincuentes**, por lo que es **indispensable** para nosotras ser **precavidas**.

¿Qué tipos de herramientas o métodos disponéis para proteger la seguridad de vuestra información y activos?

Con el fin de proteger los dispositivos que tenemos en la empresa, decidimos instalar **sistemas de protección en los dispositivos**, que a su vez se encuentran constantemente conectados a una VPN. Todas las comunicaciones que se realizan se procesan a través de la VPN. Además, **analizamos las comunicaciones y correos electrónicos** que reciben para asegurar que no se trata de ciberataques.

¿Qué tipo de amenazas afectan más a las pymes?

En el caso de nuestra empresa, hemos recibido en diferentes ocasiones correos falsos y ataques de ***phishing***, que hemos sabido **identificar de manera previa analizando los correos y verificando en cada caso la autenticidad de los mismos**. A veces, es tan sencillo como ponerse en contacto con las personas correspondientes para verificar que los datos son reales. Además, en este tipo de correos, es importante analizar elementos básicos: el dominio del remitente, los archivos adjuntos y sus formatos, falta de concordancia, si el correo solicita información personal, etc.

"Al contar con un sitio web o e-commerce, se configura como fundamental proteger la página web para evitar ciberataques, además de proteger la información de los usuarios y garantizar la integridad de sus datos, aportando así confianza a los clientes".

Ciberseguridad

Otros casos de éxito de pymes y autónomos

2. Galletas BIRBA

Birba es una empresa fundada en 1893 destinada a la **producción de galletas**, con ingredientes siempre naturales y de alta calidad. Ante el aumento de casos de ciberdelincuencia en pymes, la compañía decidió llevar a cabo una estrategia para protegerse ante posibles ataques mediante la **implementación de un sistema de seguridad integral**, donde destacan: email seguro, firewall UTM y antivirus, conexión VPN y copias de seguridad. Desde el grupo Birba, aseguran que una buena protección pasa por la combinación de tecnologías y medidas preventivas.

Si la empresa no está preparada para un plan de envergadura, hay que empezar por crear copias de seguridad de los datos y aplicaciones críticas, para garantizar que tu empresa siga adelante en caso de desastre informático.

3. Digiotouch

Digiotouch es una pyme de Estonia, a la vanguardia de las innovaciones y servicios TIC a través de su participación en los proyectos EU Horizon 2020. La empresa tiene experiencia en el **desarrollo de aplicaciones de IoT, Web of Things y transformación digital**. Actualmente, la empresa genera fuertes impactos comerciales en las industrias y los consumidores europeos e internacionales. Digiotouch, con el objetivo de proteger su empresa y probar la resistencia de la plataforma, lanzó una serie de ciberataques simulados y conocidos (DDoS, autenticación insuficiente y servicios web en la nube inseguros). Esta simulación permitió a la empresa actualizar su plataforma basada en la nube, pudiendo **combatir de manera óptima los ataques DDoS**, y garantizando la seguridad del diseño de su web.

La compañía, a través del proyecto llevado a cabo, ha logrado optimizar su plataforma en la nube, aportando sistemas de seguridad adaptados a su empresa y garantizando la seguridad de la información.

> *"Los ciberataques pueden afectar a cualquier empresa de cualquier sector y de cualquier tamaña, ya que por ejemplo ante los casos de ransomware, cualquiera está expuesto a sufrir un secuestro de sus datos y sistemas y verse extorsionado."*
>
> **Marc Martínez, Socio de Ciberseguridad y Technology Risk en KPMG**

6. Anexo I. Recursos de las Oficinas Acelera Pyme

Recursos de las Oficinas Acelera *pyme*

El **Programa Acelera *pyme*** es la iniciativa del Ministerio de Asuntos Económicos y Transformación Digital destinada a construir el ecosistema de referencia de la transformación digital de las pymes. El programa se enmarca en el Plan de Digitalización de Pymes 2021 – 2025, que cuenta con más de 4.000 millones de euros de presupuesto.

Más información sobre el proyecto Acelera pyme: https://www.acelerapyme.gob.es/

Bajo este programa, se ha creado una **red de Oficinas Acelera *pyme* ("OAPs")** la cual es el punto de encuentro físico y virtual para el apoyo de todas las pymes, autónomos y emprendedores del país, cuyo objetivo es impulsar la transformación digital de las pequeñas y medianas empresas (incluidas las de nueva creación), autónomos y emprendedores. Actualmente hay **27 Oficinas Acelera *pyme* y 62 Cámaras de Comercio** ubicadas en todas las Comunidades Autónomas de España.

Localiza tu Oficina: https://www.acelerapyme.gob.es/localizador-de-oficinas

Estas oficinas, realizan labores de sensibilización sobre las ventajas y metodologías innovadoras para optimizar el funcionamiento de sus negocios, mediante la incorporación de las TIC. Además, la iniciativa Acelera *pyme* se complementa con un **servicio de apoyo y asesoramiento**, a través del cual se realizan **actividades de soporte técnico y especializado** para los programas de transformación digital de pymes de Red.es. También están programadas **actividades de dinamización** entre las que se incluyen seminarios y talleres en todo el territorio español sobre temáticas relacionadas con la transformación digital de las pymes.

Accede al calendario de actividades: https://www.acelerapyme.gob.es/agenda

Estas OAPs, a día de hoy, han impactado a más de **40.000 pymes y autónomos** a través de la realización de las diferentes actividades, talleres, eventos, etc. que desarrollan. Estas actividades se llevan a cabo entorno a las **soluciones del Kit Digital**. En este sentido, a continuación, se presentan **recursos y enlaces** de estas actividades en relación con la **Ciberseguridad.**

Acelera *pyme*

Recursos de las Oficinas Acelera *pyme*

- **Micro píldoras**

AECIM. La importancia de la Ciberseguridad en la empresa

En esta píldora informativa, Rocío Pastor, Coordinadora BPO en Verne Technology Group, explica por qué es importante la ciberseguridad para las empresas.

Enlace al vídeo: https://www.youtube.com/watch?v=QJuyZ8zapc4&list=PLznoG4y55z-mHDksj6I39uILRaNqMaUka&index=9

- **Jornadas y sesiones**

Ciberseguridad

INEO. La importancia de la ciberseguridad en la agenda de las PYMEs

En este taller se explica de la mano de Roberto Heker (Cofundador y CEO de Next Vision) la importancia de la ciberseguridad en una empresa y cómo gestionarla.

Enlace al evento: https://www.youtube.com/watch?v=TrUg5wGRKbE

INGENIERIAK. ¿Cómo adoptar medidas de ciberseguridad en las empresas

María Pinilla, Directora Técnica de ZIUR, cuenta en este webinar la forma de adaptar las medidas de ciberseguridad necesarias para las empresas.

Enlace al evento: https://www.youtube.com/watch?v=lWXXoXpAcUA

FAEBURGOS. Webinar. Gestiona los datos de tu negocio de forma cibersegura

Webinar destinado a la gestión óptima de la información del negocio de una manera segura.

Enlace al evento: https://www.youtube.com/watch?v=AS8q45eM_38

FAEBURGOS. Protege tu negocio de los ciberdelincuentes empresariales de hoy

Webinar que explicará distintas amenazas a las que una empresa está expuesta, como *phishing* o *ransomware*, así como las formas para protegerse ante ellas.

Enlace al evento: https://www.youtube.com/watch?v=3OkHxB34mXU

FEMEVAL. La importancia de la ciberseguridad en entornos industriales

Este webinar tiene como objetivo conocer la importancia de la Ciberseguridad Industrial, cómo protegerse de ciberataques y ver casos reales.

Enlace al evento: https://youtu.be/Zm2ft_k8Lyc

Recursos de las Oficinas Acelera *pyme*

- **Jornadas y sesiones (cont.)**

INEO. La importancia de la ciberseguridad en la agenda de las PYMEs

En este taller se explica de la mano de Roberto Heker (Cofundador y CEO de Next Vision) la importancia de la ciberseguridad en una empresa y cómo gestionarla sin un grupo de especialistas en nómina. Se cuenta también con la presencia de Juan Carlos Suárez (CIO del grupo Nortempo) como caso de éxito.

Enlace al evento: https://www.youtube.com/watch?v=TrUg5wGRKbE

INGENIERIAK. ¿Cómo adoptar medidas de ciberseguridad en las empresas

María Pinilla, Directora Técnica de ZIUR, cuenta en este webinar la forma de adaptar las medidas de ciberseguridad necesarias para las empresas.

Enlace al evento: https://www.youtube.com/watch?v=lWXXoXpAcUA

FAEBURGOS. Webinar. Gestiona los datos de tu negocio de forma cibersegura

Webinar destinado a la gestión óptima de la información del negocio de una manera segura.

Enlace al evento: https://www.youtube.com/watch?v=AS8q45eM_38

FAEBURGOS. Protege tu negocio de los ciberdelincuentes empresariales de hoy

Webinar que explicará distintas amenazas a las que una empresa está expuesta, como *phishing* o *ransomware*, así como las formas para protegerse ante ellas.

Enlace al evento: https://www.youtube.com/watch?v=3OkHxB34mXU

FEMEVAL. La importancia de la ciberseguridad en entornos industriales

Este webinar tiene como objetivo conocer la importancia de la Ciberseguridad Industrial, cómo protegerse de ciberataques y ver casos reales.

Enlace al evento: https://youtu.be/Zm2ft_k8Lyc

ASHOTEL. El uso responsable del RGPD y los datos personales

El webinar destaca la importancia de conocer la normativa e implementar políticas de seguridad a través del personal, para evitar ser sancionados y realizar un tratamiento de los datos responsable. Se cuenta con la participación de Daiana Lamela e Iván Afonso, fundadores de I+D Abogados.

Enlace al evento: https://www.youtube.com/watch?v=ymUwlMAQHCU

Recursos de las Oficinas Acelera *pyme*

- **Jornadas y sesiones (cont.)**

ASHOTEL. Requisitos legales y fiscales de las *e-commerce*

En este webinar se habla sobre las responsabilidades y sanciones, el contenido de contratos electrónicos, la tributación en el comercio electrónico y los aranceles y aduanas entre otros temas. Se cuenta con la colaboración de Daiana Lamela e Iván Afonso de I+D Abogados.

Enlace al evento: https://www.youtube.com/watch?v=VomIP7p-kNQ

ASHOTEL. Cómo explotar el dato de forma responsable para aumentar ventas

Seminario que habla sobre el *marketing* digital y la explotación de datos eficiente, I+D Abogados y, por otro lado, sobre cómo el uso del machine learning puede hacer que se consigan ventas de forma segura.

Enlace al evento: https://www.youtube.com/watch?v=vxLAIw5H_L8

COIIAS. Top 10 errores de ciberseguridad en las pymes y cómo prevenirlos

El objetivo del webinar es concienciar sobre los riesgos de ciberseguridad, los errores más habituales, y técnicas de supervivencia para combatirlos.

Enlace al evento: https://www.youtube.com/watch?v=mXh_1o1W3Fw

CIDAUT. La protección de datos personales y la ciberseguridad como factores para la mejora de la competitividad

Webinar que explica factores para mejorar la competitividad, como puede ser la protección de datos personales y la ciberseguridad de la empresa.

Enlace al evento: https://attendee.gotowebinar.com/recording/7219076008511376897

CIDAUT. IA & Industria 4.0. De la eficiencia energética a la detección de amenazas

El objetivo es presentar soluciones de Inteligencia Artificial, aplicadas en entornos industriales, desde un punto de vista metodológico con ejemplos reales y resultados obtenidos. Se divide en una parte más investigadora apoyada en la tecnología y otra más práctica de su aplicación.

Enlace al evento: https://www.youtube.com/watch?v=Yceo3VhAiLA

FREMM. Protección de la Información en la Empresa

Jornada centrada en cómo proteger la información estratégica de la empresa mediante una serie de medidas y controles de seguridad.

Enlace al evento: https://www.youtube.com/watch?v=VomIP7p-kNQ

Recursos de las Oficinas Acelera *pyme*

- **Jornadas y sesiones (cont.)**

FREMM. Ciberseguridad: Retos y Soluciones

Webinar para conocer la problemática de los riesgos actuales estudiados en Ciberseguridad, el concepto y el impacto que puede tener en nuestro negocio, cómo analizarlos, cómo prevenirlos e incluso si podemos asegurarnos ante ellos.

Enlace al evento:
https://www.youtube.com/watch?v=YlaZ9wYZMrs&list=PLU4KpWXjCCye9dPDz0XksbO0d07JVpL_h&index=43

Principales amenazas

AEDHE. Webinar Problemas informáticos que te hacen perder dinero en tu empresa, ¿Cómo solucionarlos?

Este webinar hace ver qué ocurre si se pierde toda la información de los clientes, así como ver la manera de minimizar la posibilidad de que esto ocurra.

Enlace al vídeo: https://www.youtube.com/watch?v=pkM4OU9co6E

AEDHE. La ciberseguridad en el tejido empresarial del Corredor del Henares

Webinar enfocado a ver cómo está afectando la ciberdelincuencia en las empresas.

Enlace al evento: https://www.youtube.com/watch?v=jxc9wchgIec

INGENIERIAK. Cómo evitar ataques de phishing

En este webinar se hará un análisis de cómo se produce un ataque de phishing y medidas a adoptar para evitarlos.

Enlace al evento: https://www.youtube.com/watch?v=mI0aj1bDmt4

Tecnologías de ciberseguridad

AEDHE. Webinar Soluciones de Digitalización del Programa Kit Digital (III)

En este webinar, el agente digitalizador Incopyme ofrece más detalles de la firma electrónica y las soluciones de digitalización: Ciberseguridad y Gestión de redes sociales.

Enlace al vídeo: https://www.youtube.com/watch?v=h-VHF4PJ4pk&t=1s

Recursos de las Oficinas Acelera *pyme*

- **Jornadas y sesiones (cont.)**

INEO. *Cómo hacer tu email más seguro. Normas básicas de protección*

En este taller, Eduardo Díaz (CIO de Ultreia) explica que acciones se deben llevar a cabo para proteger a una empresa de posibles ataques que pueda sufrir a través de correo electrónico.

Enlace al evento: https://www.youtube.com/watch?v=kGjF1JNLjHQ

INGENIERIAK. Cómo securizar el acceso a mi red: teletrabajo y acceso remoto de proveedores

Webinar destinado a cómo securizar el acceso a la red desde el punto de vista del teletrabajo y el acceso remoto de proveedores de la empresa.

Enlace al evento: https://www.youtube.com/watch?v=8qeCv98YEu8

CTIC. Mecanismos de protección en ciberseguridad

Jornada divulgativa sobre mecanismos de Ciberseguridad organizada en colaboración con ASEMPOSIL.

Enlace al evento: https://www.youtube.com/watch?v=94xLGTGBYHg

FREMM. Cómo proteger a tu empresa del fraude del CEO: Elaboración de un plan de seguridad informática

Jornada informativa sobre cómo proteger a una empresa del fraude del CEO y la elaboración de un plan de seguridad informática.

Enlace al evento:

https://www.youtube.com/watch?v=gOj6ZQh5_qg&list=PLU4KpWXjCCye9dPDz0XksbO0d07JVpL_h&index=18

7. Anexo II. Bibliografía y enlaces de interés

Eventos de presentación del Programa de Kit Digital

El Programa Kit Digital celebra una serie de eventos para pymes, autónomos y empresas, en diferentes ciudades de España. En el evento realizan su ponencia profesionales relacionados con la transformación digital y pymes. Otra iniciativa del Gobierno de España, que tiene como objetivo subvencionar la implantación de soluciones digitales disponibles en el mercado para conseguir un avance significativo en el nivel de madurez digital. A continuación, adjuntamos los enlaces para la visualización de los eventos, que se han emitido en vivo durante la realización de los mismos:

Lista con todos los eventos de presentación

Enlace al canal de YouTube: Roadshow Kit Digital
https://youtube.com/playlist?list=PLntgnlTyDYQNlblqlj9DM2HgHVs1UkHk0

Enlace al canal de YouTube: Kit Digital
https://youtube.com/playlist?list=PLntgnlTyDYQP1pe4n6Ifyu-o5Uuya83XF

Bibliografía y enlaces de interés

Qué es la ciberseguridad

- *Ciber-Pyme*. (2021, December 13). INCIBE. https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/ciber-pyme
- *Glosario de términos de ciberseguridad*. (n.d.). https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
- *Principios y recomendaciones básicas en Ciberseguridad*. (n.d.). https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-principios-y-recomendaciones-basicas-en-ciberseguridad/file.html
- *¿Qué es la ciberseguridad?* (n.d.). Cisco. https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~how-cybersecurity-works

La ciberseguridad en la actualidad

- *Ciberseguridad en la actualidad*. (2021, May 26). Santalucia Impulsa. https://www.santaluciaimpulsa.es/ciberseguridad-en-la-actualidad/
- *Destacamos la importancia de la ciberseguridad en la gestión de crisis*. (2020, May 29). Comunidad de Madrid. https://www.comunidad.madrid/noticias/2020/05/29/destacamos-importancia-ciberseguridad-gestion-crisis
- *Infografía: Evolución de la Ciberseguridad | Software de gestión de logs y seguridad de red - ManageEngine Log360*. (n.d.). Www.manageengine.com. https://www.manageengine.com/latam/log-management/infografia-evolucion-ciberseguridad.html

Tipos de ciberataques

- *Malware Threat Report: Q2 2020 Statistics and Trends*. (2020, September 29). Avira Blog. https://www.avira.com/en/blog/malware-threat-report-q2-2020-statistics-and-trends
- Mundaca, R. (n.d.). *Malware y otros "ware" que te hacen sufrir y cómo debes cuidarte*. VTI Universidad de Chile. https://vti.uchile.cl/malware-y-otros-ware/
- *¿Qué es spyware? La definición y los 5 ejemplos principales*. (n.d.). https://softwarelab.org/es/que-es-spyware/
- *10 mejores antispyware [2022]: eliminación y protección*. (2021, August 4). SafetyDetectives. https://es.safetydetectives.com/blog/mejores-herramientas-anti-spyware-probadas/

Bibliografía y enlaces de interés

Formas de protección

- *Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse*. (2019, September 5). INCIBE. https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse
- *La biometría como clave para la seguridad*. (2011, December 15). INCIBE. https://www.incibe.es/protege-tu-empresa/blog/post-biometria
- *Pautas para realizar un teletrabajo ciberseguro*. (2022, February 18). INCIBE. https://www.incibe.es/sala-prensa/notas-prensa/pautas-realizar-teletrabajo-ciberseguro
- *Respondiendo a incidentes industriales, SOC OT*. (2018, December 13). INCIBE-CERT. https://www.incibe-cert.es/blog/respondiendo-incidentes-industriales-soc-ot
- *Trojans, backdoors and droppers top the list of most-searched malware according to Kaspersky security analysts : @VMblog*. (n.d.). Vmblog.com. https://vmblog.com/archive/2020/07/02/trojans-backdoors-and-droppers-top-the-list-of-most-searched-malware-according-to-kaspersky-security-analysts.aspx#.Yd6ef_7MI2w
- *5 Best Anti-Malware Software [2020]: Removal & Protection*. (2020, July 1). SafetyDetectives. https://www.safetydetectives.com/blog/best-malware-removal-software/

Impacto en empresas y sectores

- *Conoce los 5 sectores en los que más se valora la formación en Ciberseguridad*. (n.d.). LISA Institute. https://www.lisainstitute.com/blogs/blog/salidas-profesionales-formacion-ciberseguridad
- *Los 16 sectores de ciberseguridad de infraestructura crítica*. (2021, April 3). https://pcweb.info/los-16-sectores-de-ciberseguridad-de-infraestructura-critica/#El_sector_de_sistemas_de_agua_y_aguas_residuales
- *Retos y oportunidades para el sector público y privado Panorama actual de la Ciberseguridad en España*. (n.d.). https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
- Toca, G. (2016, November 7). *» Los cinco sectores que más están exprimiendo el big data - Esglobal - Política, economía e ideas sobre el mundo en español. ¿Cuáles son los sectores más apetecibles para el cibercrimen?* (2019, July 18). Blog Sarenet. https://blog.sarenet.es/sectores-apetecibles-cibercrimen/

Bibliografía y enlaces de interés

Casos de éxito

- *Dotnetsafer - Focus 100% on Development and Forget about Security (We take care of it for you)*. (n.d.). https://www.dotnetsafer.com/
- *Iberbox Almacenamiento Seguro - Ciberseguridad - Nº 1*. (n.d.). https://www.iberbox.com/
- *Smart Protection - Keeping your online assets safe*. (n.d.). Smart Protection. https://smartprotection.com/

Otros enlaces de interés

- Administrador. (n.d.). *Ciberataque, una amenaza creciente y sin fronteras*. https://www.clubdeejecutivos.org.py/revista/ciberataque-una-amenaza-creciente-y-sin-fronteras
- Agudo, S. (2017, March 10). *Guía de compras de VPN: nueve servicios a considerar para navegar de forma más segura*. Xataka. https://www.xataka.com/seguridad/guia-de-compras-de-vpn-nueve-servicios-a-considerar-para-navegar-de-forma-mas-segura
- *Las 5 tendencias en ciberseguridad de las que se hablarán en 2022*. (n.d.). Cloud & Cyber Security Expo Madrid 2020. https://www.cybersecurityworld.es/noticias/5-tendencias-ciberseguridad-2022
- *Solo el 2% de los ciberincidentes están asociados al coronavirus*. (2020, May 9). Redseguridad. https://www.redseguridad.com/actualidad/solo-el-2-de-los-ciberincidentes-gestionados-por-incibe-cert-estan-asociados-al-coronavirus_20200509.html

Acelera pyme

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

red.es