Acelera *pyme*

Ciberseguridad para pymes y autónomos: protege tu negocio en el mundo digital y ve un paso por delante

Abril 2023

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

Acelera pyme

Contenidos

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

1. Introducción

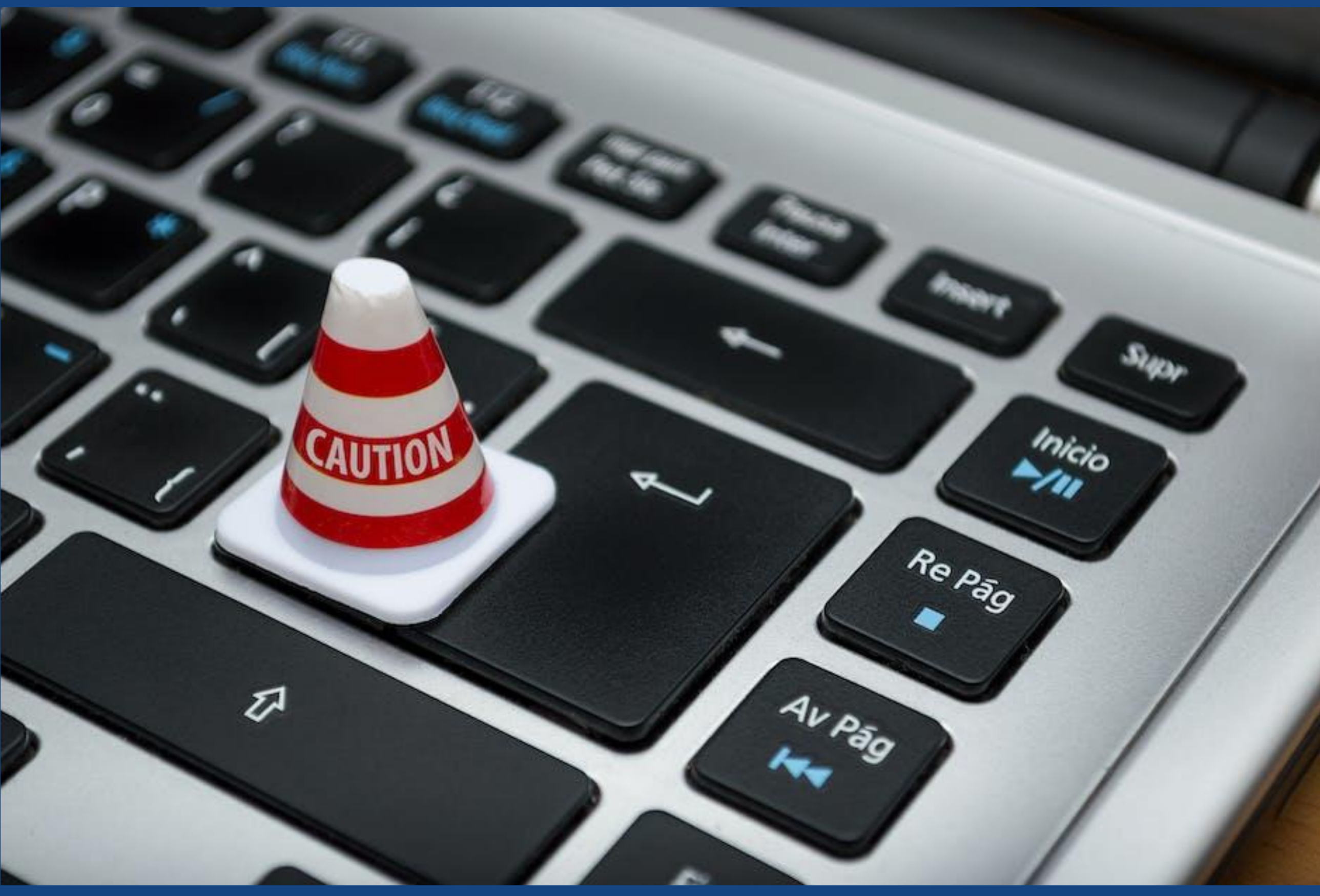
En el ámbito de la ciberseguridad, el **riesgo de sufrir ataques informáticos** es una realidad cada vez **más presente** en el mundo empresarial y de la ciudadanía en su conjunto. Estos ataques no solo pueden **poner en peligro la seguridad de los datos y la información confidencial de la pyme**, sino que también pueden **afectar a la imagen y reputación** de la misma, así como **generar pérdidas económicas** significativas. Además, con la aceleración de la digitalización en todos los sectores, la exposición a este tipo de amenazas también ha aumentado. Por lo tanto, es **imprescindible** que las pymes y **autónomos estén preparados para hacer frente a estos ataques** y contar con medidas y herramientas de ciberseguridad adecuadas para minimizar los riesgos.

De acuerdo con el Balance de Ciberseguridad 2022 [REF-01] publicado por el Instituto Nacional de Ciberseguridad (INCIBE), las consultas de las empresas se originan principalmente a través de técnicas de phishing, smishing o extorsión (20,8%), de fraude del CEO o Business Email Compromise, BEC (15,3%) y de la concienciación de los empleados y las buenas prácticas de ciberseguridad (12,5%). Cabe destacar que, en el **año 2022**, el INCIBE ha gestionado un total de **118.820 incidentes**, lo que supone un incremento del 8,8% con respecto a 2021. **Diversos motivos pueden haber influido en ello**, como por ejemplo el **aumento del grado de digitalización** en el país tanto por parte de ciudadanos como de empresas, lo que ha generado un mayor número de incidentes cibernéticos, y el conflicto Rusia-Ucrania, que ha permitido a los ciberdelincuentes perpetrar más delitos informáticos [REF-02] . Según S21sec, España se sitúa en el séptimo lugar en la clasificación de los países más ciberatacados por ransomware en 2022 [REF-03] . Como indica el resultado del DESI 2022 [REF-04] aunque España no es el país con mayor grado de digitalización, figura en el top 10 de países que más ataques de ransomware han recibido este año. Por tanto, es fundamental que tanto ciudadanos como empresas, la administración pública y formadores **otorguen a la ciberseguridad la importancia que merece**, ya que sufrir un ataque de este tipo puede acarrear graves consecuencias.

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

Acelera pyme

Los **objetivos de este monográfico** son **proporcionar** a las pymes y autónomos una **visión clara y concisa de los principales riesgos y amenazas** en el ámbito de la ciberseguridad, así como **ofrecer pautas y consejos prácticos** para reducir los riesgos y proteger sus datos e información. Se centra en la situación actual de la ciberseguridad en el entorno empresarial, y está dirigido a aquellas empresas que no cuentan con recursos suficientes en materia de ciberseguridad o que tienen un conocimiento limitado en esta materia. Se abordarán temas como la protección de datos, las amenazas más comunes, la **importancia de la concienciación** y las **buenas prácticas**, así como la descripción de herramientas y tecnologías de ciberseguridad accesibles y más efectivas para que las pymes y los autónomos puedan protegerse de los riesgos y amenazas.



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

2. La concienciación en el ámbito de la ciberseguridad

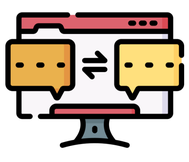
Ahora, y cada vez más, es **fundamental concienciar** sobre la importancia de la ciberseguridad a todos los usuarios. La ciberseguridad no es algo que solo debería **concernir** a las grandes empresas, si no **a todo tipo de empresas**, grandes o pequeñas. Para todos los negocios debería ser crucial proteger los datos personales de la empresa, clientes y proveedores, evitar pérdidas económicas, asegurar la reputación del negocio a la vez que se cumple con las normativas. Nadie está a salvo del todo de sufrir un ataque cibernético, sin embargo, sí **que se pueden implementar distintas medidas para minimizar los riesgos lo máximo posible**. Por ejemplo, han sufrido ataques instituciones y empresas [REF-05] tan conocidas como el Servicio Público de Empleo Estatal (SEPE), paralizando todo el sistema informático, y, en consecuencia, provocando demoras en la gestión de citas y retrasando los pagos de las prestaciones por desempleo. La empresa española de reparto a domicilio, Glovo, también sufrió un ataque de ciberseguridad, en el que pudieron acceder a los datos de las cuentas de los clientes y los repartidores. De forma similar, unos ciberdelincuentes consiguieron acceder a datos sensibles de clientes de la cadena. Todo esto supuso un **daño reputacional** para estas empresas, lo cual **puede afectar** también seriamente **a sus ingresos**. Más recientemente, en marzo de 2023, el Hospital Clínic de Barcelona sufrió un ciberataque de “ransomware” en el que robaron los datos de pacientes y trabajadores y pidieron un rescate a cambio de no publicar los datos [REF-06]. Actualmente la Autoritat Catalana de Protecció de Dades (Apdcat) ha iniciado una investigación preliminar con el propósito de determinar si se han implementado medidas apropiadas para salvaguardar la seguridad de los datos que tenían [REF-07] .

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

El **proceso de concienciación** en el ámbito de la ciberseguridad es algo que puede comenzar llevando a cabo **diversas acciones** como, por ejemplo, las que se enumeran a continuación:

Formar y capacitar a los empleados de la pyme con el objetivo de que conozcan los riesgos más comunes y cómo evitarlos.

Establecer políticas de ciberseguridad claramente establecidas y comunicarlas de forma eficaz y regular.



Intercambiar información con otros organismos y asociaciones para prevenir los ataques más comunes o más recientes. Esto también es muy importante, ya que hay constantemente nuevas amenazas y cada vez más ingeniosas.

Informar de los riesgos con casos reales para ilustrar las consecuencias de la falta de concienciación y conocimiento de ciberseguridad.

Fondo Europeo de Desarrollo Regional

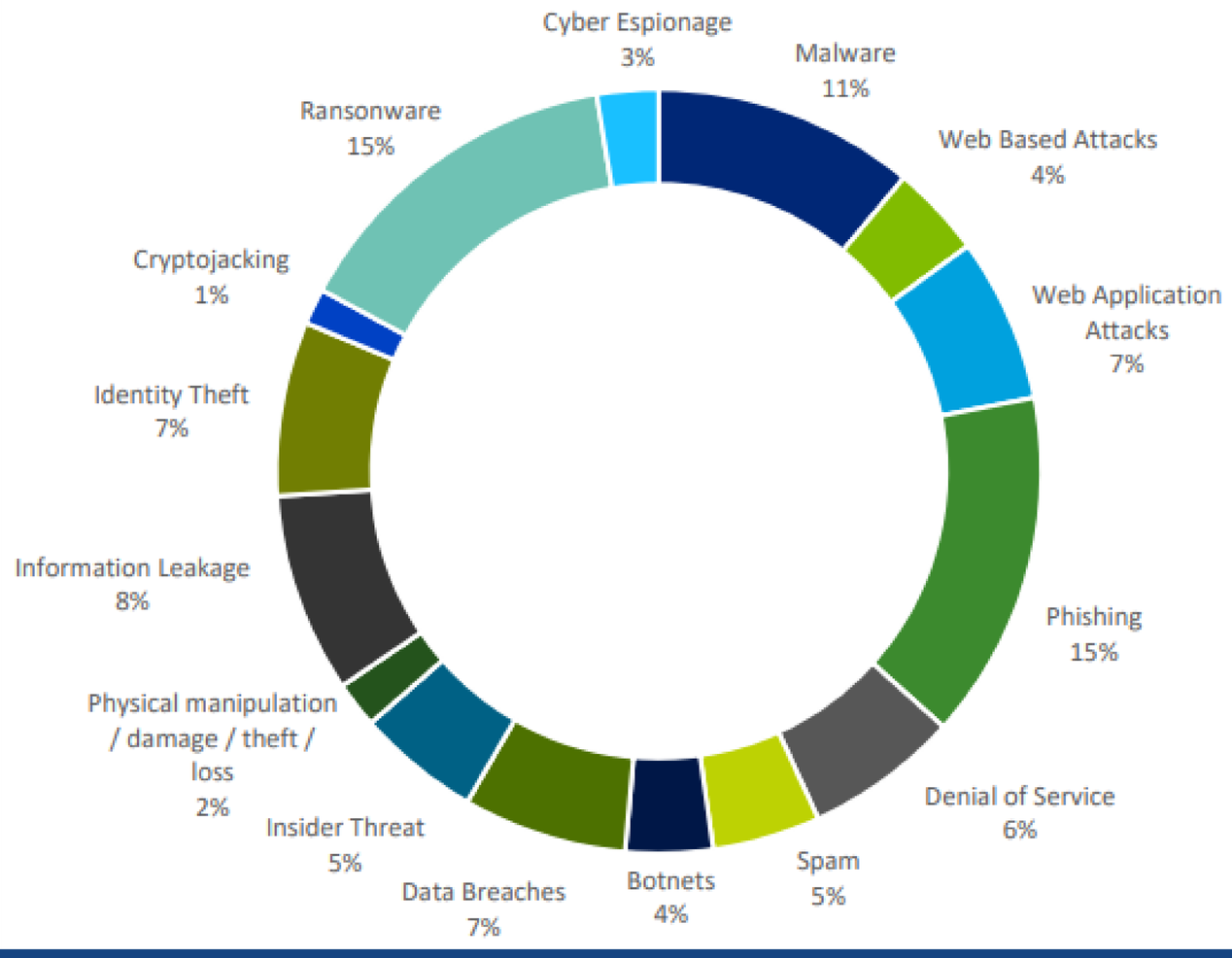
"Una manera de hacer Europa"

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

3. Amenazas más comunes en ciberseguridad:

Después de establecer las acciones para promover la concienciación en ciberseguridad, es importante comprender las **amenazas comunes a las que se enfrentan las pymes y autónomos**. Un estudio de Deloitte titulado “El estado de la ciberseguridad en España 2023” [REF-08], indica que las tres amenazas más habituales son ransomware (15%), phishing (15%) y malware (11%). Además de estas tres amenazas hay muchos más tipos de ciberamenazas que pueden sufrir pymes y autónomos. Por ello, es fundamental que **estén familiarizados** con los diferentes tipos de amenazas existentes para que puedan **tomar las medidas oportunas** para prevenir posibles ataques de los ciberdelincuentes.

Porcentaje de ocurrencia de ciberamenazas en 2022



El estado de la ciberseguridad en España. Deloitte España. https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

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

Por su parte, el **INCIBE** pone a disposición de cualquier interesado de **forma gratuita** en su web diferentes guías para **prevenir a diferentes ataques** y **cómo actuar** en caso de sufrir uno. En este respecto, hay una guía publicada titulada "Ciberamenazas contra entornos empresariales – Una guía de aproximación para el empresario" [REF-09]. En esta guía se incluyen los **principales tipos de amenazas** que existen y lo que significan:

1. **Fugas de información:** se refiere a la divulgación no autorizada o accidental de datos confidenciales de una empresa, lo que puede resultar en la pérdida de la privacidad de los datos, daños a la reputación y posibles consecuencias legales.

2. **Ataques de tipo phishing:** estos ataquen pretenden engañar a los usuarios para que revelen información personal, como, por ejemplo: contraseñas, datos de tarjetas de crédito o de cuentas bancarias, a través de comunicaciones falsificadas que parecen provenir de una fuente conocida y legítima, como un banco o una empresa conocida.

3. **Fraude del CEO (spear phishing):** como su nombre apunta, este fraude consiste en la suplantación de identidad adecuadamente planificada de un alto cargo con el fin de sustraer fondos a las empresas.

4. **Fraude de RR.HH.:** de forma similar al fraude del CEO, se trata de la suplantación de identidad, pero esta vez de un empleado, siendo la victima el departamento de recursos humanos de una empresa.

5. **Sextorsión:** esta amenaza es más conocida, y radica en amenazar a la víctima con compartir con su entorno unas imágenes comprometidas de la víctima a no ser que reciba un pago.

6. **Ataques contra la página web corporativa:** consiste en atacar la web de una empresa por dañar la imagen de la misma, obtener beneficios económicos o robar datos personales, por ejemplo.

Acelera pyme

7. **Ransomware:** este ataque bloquea la información en un dispositivo electrónico, rápidamente propagables y se solicita un rescate económico con el fin de liberar la información.

8. **Fraude del falso soporte de Microsoft:** comienza por una llamada de un supuesto empleado de Microsoft informando de errores de seguridad de los dispositivos con el objetivo de acceder a información confidencial de la empresa.

9. **Campañas de correos electrónicos con malware:** incluyen ficheros o enlaces con software malicioso oculto para introducir distintos tipos de malware en los dispositivos.

10. **Ataques de denegación de servicio (DoS):** son ataques cibernéticos que buscan interrumpir o bloquear el acceso a un sistema, servicio o red al abrumarlo con una gran cantidad de solicitudes o tráfico, agotando sus recursos y provocando su inaccesibilidad. Pueden acabar generando pérdidas económicas y daños a la reputación de la organización afectada. Los métodos utilizados incluyen el envío masivo de solicitudes, la inundación de tráfico de red y la explotación de vulnerabilidades en el software objetivo.

11. **Ataques de adware:** como su nombre señala, se trata de ataques mostrando anuncios publicitarios de forma intrusiva con el fin de generar ingresos.

12. **Ataque de suplantación de proveedores:** en este caso también es una suplantación de identidad, no obstante, a un proveedor de un servicio, consiguiendo que las victimas transfieran el dinero a los ciberdelincuentes en vez de al proveedor real.

Además, explica en mayor detalle en qué consisten estas amenazas, cómo identificarlas y cómo actuar en caso de sufrir cualquiera de estos ataques.

Acelera pyme

4. Protección de datos y consejos prácticos para la implementación de la ciberseguridad:

A la hora de hablar de ciberseguridad, mucha gente no es plenamente consciente de qué datos pueden ser objeto de ataque por parte de los **ciberdelincuentes,** sin embargo, es **crucial conocerlos**, para poder protegerse adecuadamente. A continuación, se indican una serie de **datos que son susceptibles de ser robados por estos**:

Información corporativa confidencial o privilegiada

Información de clientes (datos de contacto, historial de pedidos y preferencias de compra, datos de cuentas bancarias, etc.)

Información de proveedores (información de la empresa, detalles de transacciones comerciales, información financiera, contratos y acuerdos comerciales confidenciales, etc.)

Información de empleados (información personal de los mismos, vidas laborales, datos de la seguridad social, nóminas, etc.)

Contraseñas

Ahora bien, conociendo esta información, ¿qué medidas pueden llevar a cabo pymes y autónomos para proteger dichos datos? En este sentido, hay una **serie de pautas** básicas que propone Panda Security, una empresa especializada en ofrecer productos y servicios de ciberseguridad, y **que debería seguir cualquier pyme o autónomo** cómo, por ejemplo [REF-10] :

Acelera pyme

1. Utilizar **contraseñas únicas** (de al menos 12 caracteres, que contengan mayúsculas, minúsculas, números y caracteres especiales (%&$#) y que no contengan información personal o de la empresa en la misma) para cada tipo de cuenta e intentar modificarla con una periodicidad recomendable de al menos 45 días.

2. En los casos que sea posible, utilizar la **autenticación multi-factor** con el fin de asegurar una verificación de identidad avanzada.

3. **Emplear un firewall** (cortafuegos) con el objetivo de impedir accesos no deseados a los dispositivos de la pyme.

4. Asegurarse de tener el **sistema operativo actualizado en todo momento**, así como los navegadores y el software que empleemos con el fin de reducir el riesgo de sufrir ataques cibernéticos.

5. Si es posible, **evitar conectarse a Wi-Fi público, y activar la VPN** (hay muchas gratuitas y disponibles) con el fin de tener una conexión segura en todo momento y minimizar riesgos.

6. Revisar que los enlaces a los que se accede en la web tienen siempre el "**https**" al inicio del enlace en vez del "http".

7. En todos los programas instalados que lo permitan, **habilitar la configuración de privacidad o aumentarla** en los que sea posible.

8. Tener **precaución con la información personal que se comparte y dónde**, puesto que puede otorgar pistas a los ciberdelincuentes para adivinar contraseñas.

9. Por supuesto, **solo descargarse software verificado y de fuentes fiables**, ya que los programas piratas suelen contener malware, además de no ser legal.

10. Asegurarse de **llevar a cabo de forma regular copias de seguridad** en la nube o en unidades externas para poder prevenir el ransomware y la pérdida de datos.

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

Independientemente de lo indicado anteriormente, comenzar a aplicar medidas de ciberseguridad tiene que venir acompañado de una implementación organizada y medida con el fin de asegurar que se lleva a cabo de forma correcta. Es por ello, que se proponen las **siguientes estrategias**:

- **Desarrollar un plan de ciberseguridad:** Preferiblemente se debería crear un plan integral que aborde políticas, procedimientos y acciones para proteger los sistemas y datos de la empresa.

- **Establecer una respuesta a incidentes:** De forma similar al plan de ciberseguridad, se debería preparar y practicar un plan de respuesta a incidentes para abordar de manera rápida y efectiva cualquier incidente de seguridad que pueda ocurrir.

- **Establecer políticas de seguridad:** Definir y comunicar claramente las políticas de seguridad de la pyme, como el uso adecuado de dispositivos y recursos, la privacidad de la información y las responsabilidades del personal en términos de seguridad.

- **Implementar medidas de seguridad técnicas:** Establecer protocolos y medidas de seguridad, como la autenticación de doble factor/multi-factor, cifrado de datos, actualizaciones regulares de software y sistemas operativos, y copias de seguridad periódicas de los datos relevantes.

- **Capacitar y concienciar a los empleados:** Informar a los empleados sobre buenas prácticas de ciberseguridad, como la correcta identificación de ataques de phishing, el uso seguro de contraseñas y la identificación de posibles amenazas.

- **Mantener el software actualizado:** Asegurarse de que todos los sistemas, aplicaciones y dispositivos utilizados estén actualizados con los últimos parches de seguridad y actualizaciones proporcionadas por los proveedores de estos softwares.

- **Realizar copias de seguridad regulares:** Hacer copias de seguridad periódicas de los datos importantes y almacenar las copias de seguridad en ubicaciones seguras fuera de la red principal del negocio.

Dentro de estas medidas, es fundamental **reducir la huella digital** lo máximo posible, limitando así la información personal del autónomo o la pyme compartida en Internet, y controlando bien la información que se comparte (consciente o inconscientemente) en Internet y redes sociales. Esto ayuda a **mitigar el riesgo de exposición de datos sensibles** y contribuye a **fortalecer la ciberseguridad** en pymes y autónomos. Si bien es cierto que no es posible eliminar la huella digital por completo, INCIBE recomienda seguir una **serie de pasos que ayuden a minimizarla lo máximo posible** [REF-11] **:**

1. **No subir imágenes de lugares comprometidos** en la oficina (salas de servidores, accesos de seguridad, etc.).

2. **Evitar tomar fotografías del puesto de trabajo** y menos de la pantalla del ordenador encendida.

3. **Eliminar datos de los documentos antes de subirlos a la red**.

4. **Emplear navegadores** [REF-12] **que cuenten con funcionalidades para minimizar la huella digital** en la medida de lo posible (por ejemplo: Firefox, Brave, DuckDuckGo, Tor).

5. **Emplear** una **VPN para proteger mejor la información**.

6. **Concienciar a los empleados** para evitar fugas de información (son la principal fuente de las fugas por malas praxis y desconocimiento).

Adicionalmente, el INCIBE también pone a disposición de los usuarios información, pautas y consejos específicos [REF-13] según el tipo de sector al que se pertenezca (desde educación, salud, turismo y ocio hasta comercio minorista, por ejemplo).

En resumen, la **protección de datos y la implementación de medidas de ciberseguridad son cuestiones fundamentales** para las pymes y los autónomos en estos momentos. Aspectos como reducir la huella digital, aumentar la conciencia de los empleados y adoptar herramientas de seguridad como las VPN son acciones esenciales para salvaguardar la información confidencial y fortalecer la ciberseguridad de una pyme. **Siguiendo** estos **consejos** y **aprovechando** los **recursos disponibles**, las pymes y los autónomos van **a estar mejor preparados para enfrentar las amenazas de ciberseguridad existentes** y podrán **proteger mejor los datos de su negocio y de sus clientes.**

5. Herramientas y tecnologías de seguridad

Hay diferentes opciones a disposición de las empresas y autónomos que INCIBE publica de forma totalmente gratuita como por ejemplo el *Glosario de términos de ciberseguridad – Una guía de aproximación* [REF-14] para el empresario que incluye una definición de todos los términos de la materia.

Por un lado, en la página web de INCIBE, hay una prueba de análisis de riesgos [REF-15] que puede hacer cualquier persona que les va a ayudar a evaluar su estado de ciberseguridad. Por otro lado, en la propia **plataforma de Acelera *pyme***, tras iniciar sesión, **cualquier usuario puede llevar a cabo una autoevaluación de ciberseguridad** [REF-16] para conocer el estado de madurez de la ciberseguridad en su empresa.

En cuanto a **herramientas concretas**, a continuación de indican diferentes softwares para firewall, antivirus, etc. gratuitos o de bajo coste:

Antivirus [REF-17]**:**

- **Bitdefender Antivirus Free** [REF-18]**:** Permite una protección antimalware destacada, con una alta detección de amenazas y bloqueo eficiente de páginas web maliciosas. Además, ofrece una sólida protección antiphishing, bloqueando un alto porcentaje de páginas ilegítimas. Es un antivirus gratuito, fácil de usar y que no ralentiza el rendimiento del ordenador.

- **Avast Free Antivirus** [REF-19]**:** Destaca por su alta detección de virus y páginas web maliciosas, alcanzando el 99,96% y 99,67% respectivamente. También ofrece una gran protección contra el phishing, bloqueando el 93% de los intentos. Sin embargo, tiene mucha publicidad y carece de funciones adicionales como control parental, VPN, gestor de contraseñas y protección bancaria. No obstante, se puede combinar con otras herramientas que se enumeran en este apartado.

Firewall [REF-20]**:**

- **Windows Defender:** este cortafuegos viene por defecto instalado en el sistema operativo de Windows 10, por lo cual ya cuenta con muchas ventajas de base.

- **ZoneAlarm** [REF-21]**:** es compatible con sistemas Windows y es una solución gratuita que controla la actividad de los programas en los ordenadores. Protege la identidad de los usuarios frente a hackers y ofrece herramientas de seguridad para navegación en redes poco seguras. Destaca su función Web Secure, que garantiza una protección adicional mientras se navega por Internet.

- **Comodo Free Firewall** [REF-22]**:** permite controlar el tráfico, detectar conexiones sospechosas y desinfectar el PC en caso necesario. Además, ofrece características como servidores DNS personalizados, bloqueador de anuncios y protección contra actividades sospechosas. Cuenta con una interfaz sencilla y tiene la capacidad de ocultar puertos y bloquear software sospechoso.

VPN [REF-23]**:**

- **Hotspot Shield** [REF-24]**:** uno de los VPN gratuitos más recomendados y populares, que permite utilizar el servicio en hasta cinco dispositivos con una sola cuenta y ofrece hasta 500 MB al día. Destaca por su facilidad de uso y cifrado de datos seguro. Sin embargo, la versión gratuita tiene anuncios y no permite seleccionar la ubicación del servidor, ya que se conecta de forma aleatoria.

- **ProtonVPN Free** [REF-25]**:** este VPN es indicado para aquellos casos en los que se prime la cantidad de datos, ya que está tiene datos ilimitados en su versión gratuita, sin embargo, solo se puede utilizar en un dispositivo a la vez y sólo tiene tres ubicaciones para sus servidores. Por el contrario, no es necesario iniciar sesión para utilizarlo, pudiendo minimizar así más aún la huella digital.

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

Gestor de contraseñas [REF-26]**:**

- **1Password:** un gestor de contraseñas seguro y sencillo de utilizar, que cuenta con una amplia gama de funciones y ofrece una prueba gratuita de 14 días. Proporciona planes accesibles tanto para usuarios individuales como para familias. Además, ofrece una versión diseñada específicamente para empresas, la cual tiene un precio de 7,99 USD al mes. Esta versión para empresas no solo tiene una gestión segura de contraseñas, sino también una integración sin problemas con otras herramientas utilizadas en entornos corporativos.

- **LastPass** [REF-27]**:** cuenta con una prueba gratuita de 14 días y su versión de pago básica para empresas tiene un precio de 3,90€ por usuario al mes e incluye una serie de funcionalidades adicionales, como la posibilidad de tener hasta 50 usuarios, inicio de sesión sin contraseñas, carpetas compartidas, autenticación multifactor (MFA), un panel de seguridad y la capacidad de supervisar intentos de hackeo.

6. Conclusiones

En conclusión, en este monográfico se ha explicado la **importancia de la ciberseguridad** para pymes y autónomos, se han **ofrecido indicaciones de cómo promover la concienciación** en el ámbito de la ciberseguridad, dando ejemplos reales de ataques al Servicio Público de Empleo Estatal (SEPE) y a la empresa española de reparto a domicilio, Glovo. Además, se ha hecho hincapié en la importancia de **conocer los diferentes tipos de amenazas** existentes **y sus consecuencias**, como el ransomware, phishing y malware.

Más adelante, se han especificado **qué datos pueden ser objeto de robo** por los ciberdelincuentes como por ejemplo la información personal, financiera y comercial que puede tener graves repercusiones tanto para la empresa como para los individuos afectados. En términos de medidas a efectuar, se han **proporcionado consejos específicos para pymes y autónomos**. Estos incluyen la implementación de un plan de ciberseguridad, el uso de contraseñas seguras, la realización de copias de seguridad regulares, la actualización de software o incluso reducir de la huella digital. Además, se ha destacado la **importancia de contar con herramientas de ciberseguridad** como antivirus, firewalls y VPNs, y se han mencionado algunas opciones gratuitas o de bajo coste que pueden utilizar pymes y autónomos.

Las pymes y autónomos tienen que ser conscientes de que la **ciberseguridad** es un aspecto crítico que **no puede ser ignorado**. Implementar medidas de protección, concienciar a los empleados, proteger los datos y mantenerse actualizado sobre las últimas amenazas son pasos fundamentales para salvaguardar la información y garantizar la continuidad del negocio para evitar graves consecuencias. En este sentido, cabe resaltar que la ciberseguridad debe ser **considerada como una inversión**, no como un gasto, ya que los costes asociados a una brecha de seguridad pueden ser mucho mayores. Contando con una estrategia sólida de ciberseguridad, las pymes y autónomos van a estar mejor preparados para hacer frente a los desafíos y proteger su negocio en la era digital.

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

7. Referencias

[REF-01] – INCIBE. +118.820 incidentes gestionados fraude online. https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

[REF-02] – CSO España. El cibercrimen crece en España y se profesionaliza en 2022. (1 noviembre, 2022). https://cso.computerworld.es/reportajes/el-cibercrimen-crece-en-espana-y-se-profesionaliza-en-2022

[REF-03] – Group, I. D. M. España es el séptimo país más ciberatacado por ransomware en 2022. (7 diciembre, 2022). https://www.itreseller.es/seguridad/2022/12/espana-es-el-septimo-pais-mas-ciberatacado-por-ransomware-en-2022

[REF-04] – Índice de la Economía y la Sociedad Digitales (DESI). (2022) https://espanadigital.gob.es/sites/espanadigital/files/2022-08/DESI%202022%20Espa%C3%B1a.pdf

[REF-05] – Unión Alcoyana Seguros. Ejemplos de ciberataques en empresas españolas y consecuencias. (13 julio 2022). https://unionalcoyana.com/consecuencias-ciberataques-en-empresas-espanolas/

[REF-06] – Fontserè, C. B., Sara. El ciberataque que sufre el Hospital Clínic de Barcelona procede del extranjero y obliga a anular 3.000 visitas. El País. (6 marzo, 2023). https://elpais.com/espana/catalunya/2023-03-06/el-ciberataque-que-sufre-el-hospital-clinic-de-barcelona-procede-del-extranjero.html

[REF-07] – Press, E. La Apdcat abre un expediente por el ciberataque al Hospital Clínic y sus entidades. Www.europapress.es. (22 junio, 2023). https://www.europapress.es/catalunya/noticia-apdcat-abre-expediente-ciberataque-hospital-clinic-entidades-20230622141451.html

[REF-08] – El estado de la ciberseguridad en España. Deloitte España. https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

[REF-09] – Ciberamenazas contra entornos empresariales. https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf

[REF-10] – Panda Security Mediacenter. 10 consejos de seguridad en el Mes de la Concienciación sobre la Ciberseguridad. (10 octubre, 2018) https://www.pandasecurity.com/es/mediacenter/panda-security/consejos-mes-ciberseguridad/

[REF-11] – INCIBE. Como Evitar Que La Huella Digital Afecte Nuestras Empresas | Empresas https://www.incibe.es/empresas/blog/como-evitar-que-la-huella-digital-afecte-nuestras-empresas

[REF-12] – AndroidTR. *Cómo minimizar tu huella digital*. (9 marzo, 2023). https://androidtr.es/como-minimizar-tu-huella-digital/

[REF-13] – INCIBE. Sectoriza2 | Empresas (https://www.incibe.es/empresas/sectoriza2

[REF-14] – Glosario de términos de ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[REF-15] –INCIBE. Instituto Nacional de Ciberseguridad. Adl.incibe.es. Autodiagnóstico ligero, https://adl.incibe.es/

[REF-16] – Acelera pyme. ¿Quieres conocer el grado de digitalizacion de tu pyme? https://www.acelerapyme.es/quieres-conocer-el-grado-de-digitalizacion-de-tu-pyme

[REF-17] – Proteger el ordenador con antivirus gratuitos. https://www.ocu.org/tecnologia/antivirus/consejos/antivirus-gratuitos

[REF-18] – Bitdefender. Líder mundial en software de seguridad informática. https://www.bitdefender.es/

[REF-19] – Avast. Descargar Free Antivirus y VPN | 100 % gratis y sencillo. https://www.avast.com/es-es/index

[REF-20] – ADSLZone. Los mejores cortafuegos para tu ordenador Windows 10. https://www.adslzone.net/listas/mejores-programas/cortafuegos-firewall/

[REF-21] – ZoneAlarm. *PC and Mobile Security Software*. https://www.zonealarm.com/

[REF-22] – Comodo. Free Firewall | Get Award Winning Comodo Firewall Today. https://www.comodo.com/home/internet-security/firewall.php

[REF-23] – Fernández, Y. Xataka. VPN gratis: las 7 mejores con las que conectarte ocultando tu IP o desde otro país. (28 junio, 2022). https://www.xataka.com/basics/vpn-gratis-mejores-que-conectarte-ocultando-tu-ip-otro-pais

[REF-24] – Hotspotshield. Descargue ya la VPN de Hotspot Shield para navegar por Internet de forma privada y segura, acceder a sitios web bloqueados y mucho más. https://www.hotspotshield.com/es/

[REF-25] – Proton VPN. VPN gratuita sin anuncios ni límites de velocidad. https://protonvpn.com/es/free-vpn

[REF-26] – SafetyDetectives. Los 7 mejores gestores de contraseñas (GRATIS) en 2023. (12 abril, 2021). https://es.safetydetectives.com/blog/the-best-free-password-managers-es/

[REF-27] – LastPass. Precios por plan. https://www.lastpass.com/es/pricing?pill=business

Acelera pyme

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