Guía para la Ciberseguridad en las PYMES

Guía de preguntas y respuestas

universidad de león

Global Digital Foundation
The Digital Policy Network

eit Digital

Entidad cofinanciada por la Unión Europea

HUAWEI

PRÓLOGO DE LA UNIVERSIDAD DE LEÓN

En el contexto de la era digital, la transformación tecnológica ha revolucionado la manera en que interactuamos, trabajamos y nos comunicamos. El proceso de digitalización se extiende a todas las esferas de la sociedad, impulsando la conectividad global. La llegada e implantación de la tecnología 5G en los próximos años supondrá una nueva revolución en esta conectividad. Permitirá la implementación de aplicaciones innovadoras como el Internet de las cosas (IoT), los vehículos autónomos o las ciudades inteligentes, y supondrá una oportunidad de negocio para todo tipo de organizaciones, incluyendo las pequeñas y medianas empresas.

Este avance tecnológico trae consigo nuevos desafíos, y la ciberseguridad emerge como una cuestión crítica que es imprescindible abordar.

La ciudad de León es un polo de investigación y desarrollo de tecnologías relacionadas con la ciberseguridad, en torno a la sede del Instituto Nacional de Ciberseguridad (INCIBE), que se encuentra en esta localidad. Desde la Universidad de León tenemos el compromiso de apoyar y contribuir a estas iniciativas, habiendo creado la Cátedra Institucional en Ciberseguridad, que tiene como objetivos el análisis, investigación, docencia y difusión sobre ciberseguridad, así como la generación, retención y atracción del talento joven. En el ámbito docente, también hemos diseñado e implementado diferentes itinerarios formativos directamente relacionados con la ciberseguridad, abordándola tanto desde el punto de vista técnico como del derecho[1].

La colaboración con el tejido empresarial es prioritaria para la Universidad de León, promoviendo la firma de convenios de colaboración y procesos de transferencia de conocimiento con todo tipo de organizaciones. En este contexto se enmarca la firma del convenio entre nuestra universidad y Huawei, a la que agradecemos su iniciativa. Fruto de esta colaboración surge la adaptación de esta guía enfocada en promover la ciberseguridad en las pequeñas y medianas empresas en España, que esperamos sirva para concienciar y fomentar la implantación de prácticas y actitudes dirigidas a mejorar la ciberseguridad en estas organizaciones, tan relevantes para el desarrollo económico de nuestro país.

Fdo. Juan Francisco García Marín
Rector de la Universidad de León

[1] Al final de esta guía, encontrará más información sobre la cátedra y títulos en Ciberseguridad.

00 ÍNDICE

CAPÍTULO

01 POR QUÉ LAS PYMES SON IMPORTANTES

¿POR QUÉ LAS PYMES SON TAN IMPORTANTES PARA ESPAÑA Y EUROPA?

Las pymes contribuyen a la economía de la UE mediante la creación de puestos de trabajo de alta calidad. El fomento y la protección de las pymes en Europa es una prioridad política clave para los responsables de la UE.

25mill

En Europa hay 25 millones de pymes, casi 3 millones de ellas en España.

99%

Las pymes representan más del 99% de las empresas europeas.

100mill

Las pymes emplean más de 10 millones de personas en España, 100 millones de personas en toda Europa.

+50%

Las pymes contribuyen a más de la mitad del PIB de la UE.

Las pymes apuntalan la construcción de una sociedad más innovadora.

Las pymes son motores de la transformación digital y el crecimiento económico.

¿POR QUÉ LAS PYMES DEBEN TENER NIVELES DE CIBERSEGURIDAD ROBUSTOS?

Las recientes restricciones de la pandemia Covid-19 aceleraron la necesidad de que las pymes digitalizaran aún más sus operaciones y servicios. La digitalización de una gran parte de las pymes europeas se produjo muy rápidamente. Lamentablemente, este crecimiento de la digitalización estuvo marcado por un aumento de los ataques a la ciberseguridad. Según el Foro Económico Mundial (FEM), se produjo un aumento del 667% en los ataques de phishing durante los primeros meses de Covid-19 en 2020. Varias de estas pymes no estaban preparadas para los ciberataques y muchos empleados desconocían cómo mitigar los riesgos cibernéticos. No es correcto suponer que los ciberataques se dirigen únicamente a las grandes empresas. Hay pruebas claras de que el sector de la pymes también es objetivo sistemático de los ciberdelincuentes.

- En una encuesta realizada por ENISA en 2021[1], el 57% de las pymes creen que sus empresas quebrarían como consecuencia de un ciberataque. Los incidentes de ciberseguridad también socavan la confianza empresarial y perturban el proceso de transformación digital en toda Europa. Los ciberataques contra las pymes pueden tener un efecto perturbador en la economía de la UE.
- La ciberseguridad de las pymes es fundamental para asegurar la cadena de suministro en Europa. La ciberseguridad de la cadena de suministro puede definirse como la resistencia de cada empresa, producto y servicio que interviene en la entrega de un producto o solución al usuario final. El número de ataques a la cadena de suministro está aumentando exponencialmente. El informe sobre el panorama de las amenazas 2022 de ENISA[2] ha descubierto que los ataques a la cadena de suministro representan el 17% de todos los ciberataques en 2022, en comparación con solo el 1% en 2021. Muchos ataques en los que las redes o la información de los clientes se ven comprometidas están relacionados con una violación de la seguridad de un proveedor.
- Unos mayores niveles de ciberseguridad para las pymes protegerán aún más la ciberresiliencia de la UE. Las pymes sirven a sectores críticos de la economía europea, aportando servicios y productos a proveedores de TI o a operadores de servicios públicos. Como forma de penetrar en redes de infraestructuras críticas que, de otro modo, serían seguras, los ciberdelincuentes atacan a los proveedores de las pymes para acceder a redes y datos clave.
- La ciberseguridad de las pymes es un componente esencial para preservar la seguridad de los ciudadanos europeos. Si la tecnología no es segura y las pymes la utilizan, esto genera claramente vulnerabilidades y plantea mayores riesgos para los usuarios.

2021

1,0%

Los ataques a la cadena de suministro representan solo el 1% de todos los ciberataques.

2022

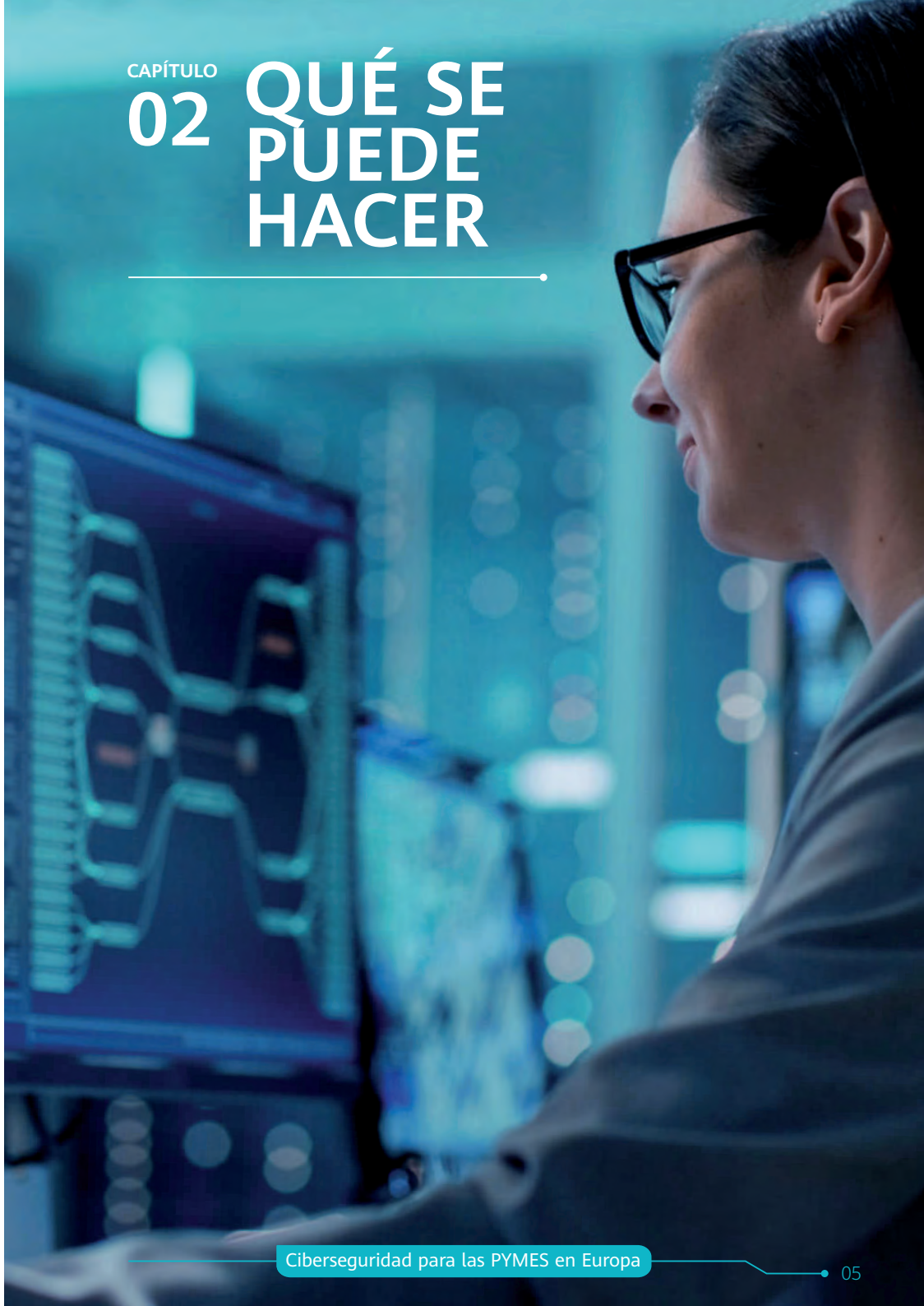
17,0%

Los ataques a la cadena de suministro representan el 17% de todos los ciberataques.

[1] https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes
[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

CAPÍTULO 02

QUÉ SE PUEDE HACER



¿CUÁLES SON LOS DESAFÍOS CLAVE PARA LAS PYMES EN LA PROMOCIÓN DE ESTÁNDARES Y COMPETENCIAS EN CIBERSEGURIDAD?

Una de las principales preocupaciones de las pymes es mantener o ampliar sus oportunidades de negocio y hacerlo de forma segura. Para lograr este objetivo, las pymes deben tener en cuenta la evolución del panorama de las ciberamenazas. Entre los principales retos relacionados con la ciberseguridad de las pymes figuran los siguientes:

El factor humano:

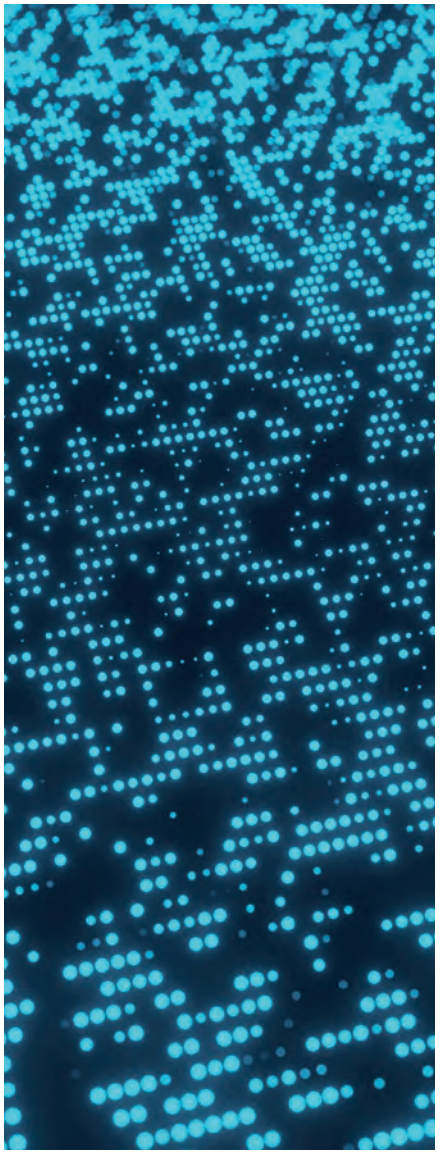
Según el informe 2023 Data Breaches Investigations de Verizon[3], el 74% de las brechas de datos implican un factor humano. Esto está relacionado con la falta de concienciación sobre ciberseguridad de algunos empleados y usuarios. Resulta difícil abordar este problema subyacente: el comportamiento y los hábitos humanos. Asegurar los datos sensibles y protegerlos contra el robo debería ser un elemento esencial de la formación en capacidades en materia de ciberseguridad de los empleados.

Inversión:

El 93% de las pymes son microempresas, con menos de 10 empleados y sin personal dedicado a las TI o la seguridad[4]. Al igual que los seguros contra incendios o de hogar, la inversión en ciberseguridad es de vital importancia para proteger los productos y servicios de las pymes. Evaluar el riesgo en ciberseguridad e identificar los procesos y activos críticos que deben protegerse puede llevar tiempo y conocimientos especializados. Tenemos que poner fin a las situaciones en las que las empresas se dan cuenta de la necesidad de la ciberseguridad sólo después de un incidente importante, evidentemente cuando ya es demasiado tarde.

Falta de cualificación y competencia

Las pymes se enfrentan a dificultades para acceder a profesionales de la seguridad capacitados para un asesoramiento a medida sobre la integración de la ciberseguridad en sus operaciones. Según un estudio del ISC2 Cybersecurity Workforce Study 2022[5], en Europa faltaban más de 300.000 especialistas en ciberseguridad (60.000 de ellos en España). Todo ello conlleva una mayor responsabilidad para los directivos y empleados de las pymes de mantenerse al día en un panorama de ciberseguridad en constante cambio. El Informe Fortinet Cybersecurity Skills Gap Report 2022[6] reveló que el 80% de las organizaciones han sufrido una o más brechas que podrían atribuirse a la falta de habilidades de ciberseguridad y/o a la falta de concienciación sobre ciberseguridad en el entorno laboral. ENISA publicó en abril de 2022 el Marco Europeo de Competencias en Ciberseguridad[7]. Este marco identifica el conjunto de habilidades críticas de ciberseguridad que se requieren para el entorno laboral. También proporciona las herramientas adecuadas para que el personal de RRHH comprenda mejor qué se necesita exactamente para contratar personal de ciberseguridad.



¿QUÉ MEDIDAS PRÁCTICAS HAY QUE ADOPTAR PARA AYUDAR A MEJORAR LA CIBERSEGURIDAD DE LAS PYMES EN ESPAÑA Y EUROPA?

Hay cuatro medidas clave que deben tenerse en cuenta a la hora de crear una estrategia de seguridad y que nos ayudan a minimizar el riesgo:

- Identificar los procesos y recursos críticos de la empresa, las amenazas a la seguridad, las vulnerabilidades y los riesgos.
- Implantar medidas de seguridad, como un estricto control de acceso, concienciación y formación, gestión de vulnerabilidades y parches, y procesos de copia de seguridad y recuperación de datos.
- Utilización de procedimientos actualizados antimalware, de detección de incidentes de seguridad y de notificación al personal y a los usuarios.
- Mantener los planes de recuperación ante incidentes y catástrofes y establecer las estructuras de comunicación adecuadas para interactuar con las partes interesadas.

[3] https://www.verizon.com/business/resources/reports/dbir/

[4] Se ajusta a los últimos datos españoles del informe "Cifras pyme" de junio de 2023: https://industria.gob.es/es-es/estadisticas/Cifras_PYME/CifrasPYME-junio2023.pdf

[5] Pese a haberse generado más puestos de trabajo en ciberseguridad, la demanda ha crecido todavía más, por lo que la falta de especialistas es todavía mayor ahora. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196

[6] https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

[7] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

¿QUÉ DEBEN HACER LAS PYMES PARA REDUCIR LOS TIPOS DE CIBERAMENAZAS?

Los tipos más comunes de ataques a las pymes incluyen malware, phishing, ataques basados en web, ransomware y denegación de servicio distribuido (DDoS).

Control de acceso estricto: gestión segura de contraseñas

- Más del 60% de las violaciones de la ciberseguridad afectan a las credenciales de los usuarios. Las prácticas deficientes y débiles en materia de contraseñas suponen un riesgo real para la ciberseguridad.
- Utilizar una contraseña fuerte y única con al menos 12 caracteres y letras, números y símbolos. Se recomienda encarecidamente utilizar un gestor de contraseñas para generarlas, gestionarlas y almacenarlas de forma cifrada.
- Aplicar/activar la autenticación multi-factor (AMF) para las aplicaciones y sistemas que las pymes utilizan o ponen a su disposición. La AMF actúa como una capa más de protección de la seguridad para las pymes.

Gestión de vulnerabilidades

- Corresponde a las pymes garantizar que se identifican y mitigan las vulnerabilidades de sus productos. Los parches para vulnerabilidades y las medidas de mitigación para los productos/servicios que utilizan (señalados por los proveedores o las autoridades nacionales) deben aplicarse oportunamente.
- La instalación y el mantenimiento de sistemas antivirus es un paso esencial para proteger los sistemas operativos y las aplicaciones de las pymes de otras amenazas.

Copia de seguridad de datos

- Copia de seguridad de los datos esenciales para las actividades empresariales en al menos 2 ubicaciones fuera de la red corporativa.
- Utilizar el cifrado completo de disco para garantizar que, en caso de pérdida o robo de un disco duro, los datos permanezcan seguros. Las claves de cifrado deben protegerse de forma segura.

Instalación y mantenimiento de cortafuegos

- Instalar un cortafuegos para mejorar la seguridad aislando una red confiable de otra que no lo es. Parchear y reforzar el cortafuegos. Utilizar un enfoque de listas blancas (denegación por defecto) para permitir únicamente el tráfico específico que requieren los servicios utilizados por la empresa. Actualizar periódicamente el software del cortafuegos y, en la medida de lo posible, automatizar el proceso.

Inalámbrico / Acceso Wi-Fi protegido (WPA)

- Utilizar WPA3 siempre que sea posible y una contraseña única y segura con cifrado de red Wi-Fi que contenga al menos 20 letras, números y caracteres especiales.

Red privada virtual (VPN) para acceder fuera de una red corporativa

- Una VPN robusta puede proporcionar un acceso remoto seguro a una red y sus aplicaciones.

Mantener un Plan de Recuperación de Incidentes y Catástrofes

- Definir y mantener un plan de recuperación ante incidentes y catástrofes para responder a las violaciones de seguridad, de modo que las pymes puedan recuperar el control de sus operaciones y datos empresariales.

¿POR QUÉ ES TAN IMPORTANTE QUE LA DIRECCIÓN DE LAS PYMES COMUNIQUE DE MANERA CLARA LAS RESPONSABILIDADES Y NECESIDADES EN CONEXIÓN CON LA CIBERSEGURIDAD?

- Los directivos de las pymes deben comunicar muy claramente a sus equipos y explicar de forma concisa lo que se espera de ellos para mitigar los ciberataques en el entorno laboral.
- Debe impartirse una formación adecuada en ciberseguridad sobre gestión de contraseñas, copias de seguridad de datos y sobre cómo responder a un ciberataque. La formación puede hacer hincapié en que el 82% de las brechas de datos se producen como consecuencia de un error humano.
- Se aconseja elaborar un plan sobre cómo comunicarse con las partes involucradas y afectadas en caso de incidente de ciberseguridad.

La importancia de la formación se debe a que el 82% de las brechas ocurren como resultado de un error humano.

82%
Consecuencia de errores humanos

¿QUÉ PUEDEN HACER LAS PYMES PARA IMPEDIR QUE SE INSERTE MALWARE EN SUS SISTEMAS?

Los principales objetivos de los códigos maliciosos son los siguientes:

01
Cifrado, robo o modificación de la información, por ejemplo, para pedir un rescate o revender los datos.

02
Supervisión de los flujos de datos, por ejemplo, en beneficio del atacante.

03
Tomar el control de un dispositivo, por ejemplo, para provocar un incidente.

Medidas clave para que las pymes se protejan contra el malware:

- Instalación y mantenimiento de software antimalware especializado. Estos programas pueden instalarse en dispositivos móviles, sistemas operativos y redes. El software escanea los datos entrantes en busca de malware y bloquea o pone en cuarentena el código identificado como sospechoso antes de su uso. Existen muchos tipos de software antimalware a la venta en el mercado.
- Los usuarios/empleados deben permanecer alerta y abstenerse de hacer clic en enlaces sospechosos de correos electrónicos o abrir archivos adjuntos sospechosos.
- Es necesario realizar copias de seguridad de los datos.

¿CÓMO PUEDEN LOS CORTAFUEGOS MEJORAR LA SEGURIDAD DE LAS PYMES?

Un cortafuegos intenta mejorar la seguridad aislando los sistemas, aplicaciones y datos internos de una red no confiable como Internet.

- Las normas que definen el acceso a la red deben ser específicas. Deben definirse directrices de seguridad para la empresa.
- Deben realizarse auditorías periódicas de los cortafuegos. Por ejemplo, cualquier cambio no autorizado en la configuración del cortafuegos debe ser detectado e identificado.

¿CÓMO PUEDEN LAS PYMES RECONOCER LOS ATAQUES DE PHISHING?

Los ataques de phishing son un tipo de ataque de ingeniería social, es decir, dirigido a las personas y no a las vulnerabilidades del sistema. Es, en esencia, análogo a los tipos tradicionales de fraude. Por defecto, el phishing no es un ataque técnico complejo. Sólo requiere una buena razón, como un escenario de fraude, para hacer que el usuario haga clic en un enlace malicioso, abra un archivo con malware o escriba/proporcione información confidencial.

Reconocer los tipos habituales de fraude puede evitar que las pymes sean víctimas de muchos ataques de phishing. Comprender los distintos tipos de ataques de phishing ayudará a los directivos y empleados de las pymes a desarrollar el instinto de revisar cuidadosamente el correo electrónico y otros mensajes antes de hacer clic en los enlaces o archivos adjuntos que contengan.

Preguntas que las personas que trabajan en pymes deberían plantearse para detener un ataque de phishing:

¿El mensaje es solicitado o esperado? Si no es así, hay que responder a todas las preguntas siguientes para identificar un intento de phishing.

¿Es legítimo el remitente, es decir, utiliza el correo electrónico, el perfil o el número de teléfono corporativos correctos? Si no es así, podría tratarse de un intento de phishing.

¿Hay una sensación de urgencia en el mensaje, una consecuencia aterradora o una gran recompensa? En caso afirmativo, podría tratarse de un intento de phishing.

¿La solicitud afirma proceder de un banco, de los servicios postales, de la administración tributaria o de un organismo policial? En caso afirmativo, podría tratarse de un intento de suplantación de identidad y provenir de un ataque muy extendido de este tipo. Este tipo de organizaciones suelen utilizar canales de comunicación seguros (por ejemplo, aplicaciones). En caso de duda, hay que ir directamente a la aplicación/página web del remitente e iniciar sesión para comprobar si aparece algún mensaje.

¿El mensaje parece extraño, con errores tipográficos o es muy genérico? Entonces podría tratarse de un intento de phishing.

¿QUÉ PUEDEN HACER LAS PYMES EN CASO DE ATAQUE DE PHISHING?

Los ataques de phishing son una realidad para las pymes. Se deben tener en cuenta las siguientes respuestas:

- Nunca hacer clic en un enlace en caso de sospecha de ataque de phishing.
- Detectar e identificar el mensaje como posible phishing a su departamento informático o a la plataforma utilizada o a la organización suplantada.
- Borrar el mensaje.
- En caso de ataque de phishing, informar al equipo de seguridad/IT y cambiar las contraseñas y PIN de todas las cuentas importantes (correo electrónico, banco, servicios de autenticación, sistemas operativos y servicios en la nube).
- Si el ataque de phishing tiene éxito, los sistemas y los datos pueden verse comprometidos y quedar inaccesibles, pudiendo incluso recibirse un mensaje de ransomware. En tal caso existen algunos recursos útiles con consejos sobre cómo actuar en caso de un incidente de ransomware, como el proyecto "No More Ransom" de Europol, y en todo caso la colaboración con el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) de referencia.

¿QUÉ PUEDEN HACER LAS PYMES PARA EVITAR UN ATAQUE WEB?

Un ataque basado en la web aprovecha las debilidades de seguridad de la infraestructura de Internet para llevar a cabo un ciberataque contra, por ejemplo, el sitio web de una empresa, un sitio de comercio electrónico, un blog o un motor de búsqueda. Algunos ejemplos de ataque basado en la web son la instalación de código malicioso para extraer información sensible, como una base de datos de consumidores o un detalle de pago, una modificación de los datos del sitio web, el borrado de datos y el sabotaje del acceso al sitio web.

- Para protegerse contra los ataques basados en la web, las pymes deben tener en cuenta lo siguiente:
- Mantener actualizados los sistemas operativos. Las últimas actualizaciones de seguridad disponibles deben instalarse en cuanto estén disponibles.
- Habilitar opciones de seguridad, como la autenticación robusta para el acceso con privilegios de administración, el cifrado y las copias de seguridad.
- Control y supervisión de sitios web para detectar y prevenir vulnerabilidades y la distribución de código malicioso.

CAPÍTULO 03

APOYO A NIVEL EUROPEO

¿CUÁL ES LA POLÍTICA DE LA UE Y DE ESPAÑA EN MATERIA DE APOYO A LAS PYMES DESDE EL PUNTO DE VISTA DE LA CIBERSEGURIDAD?

La UE aborda la mejora de la ciberseguridad de las pymes de dos maneras: inversión y regulación.

Cyber Security Act (2019)

- Un instrumento político que promueve y apoya la ciberseguridad de las pymes en la UE es la Ley de Ciberseguridad de 2019, también conocido como Ley de Ciberseguridad. Esta regulación sienta las bases para un mayor desarrollo de los sistemas de certificación de la ciberseguridad en toda la UE.
- Estos sistemas de certificación pueden beneficiar a las pymes que buscan garantías de ciberseguridad de sus proveedores, así como actuar como instrumento para promover y dar una ventaja competitiva a las pymes que invierten en ciberseguridad. En la UE se están elaborando tres importantes sistemas de certificación de ciberseguridad centrados en los servicios en la nube (EUCS), la tecnología 5G, y la creación de un "Common Criteria" europeo (EUCC) para los productos TIC de confianza en la UE. La nube y la tecnología 5G son pilares estructurales que permiten una mayor digitalización de las pymes y el desarrollo de nuevos servicios. El esquema de "Common Criteria" certifica las características de seguridad de los productos y esto, a su vez, puede ser utilizado por algunas pymes como parte de su oferta de productos y servicios.

Directiva NIS2 y Ley de Ciberresiliencia (CRA)

- La nueva Directiva NIS2, publicada en diciembre de 2022 (Directiva 2022/2555) introduce una serie de medidas que obligarán a los operadores de determinados servicios esenciales dentro de la UE a aplicar medidas de seguridad y realizar una evaluación del riesgo de ciberseguridad de sus proveedores. En algunos casos, estos requisitos podrán también afectar a algunas pymes de los Estados miembros.
- Desde 2022, la Comisión Europea trabaja en la Ley de Ciberresiliencia (CRA), centrada en mejorar la ciberseguridad de los productos con un elemento digital (por ejemplo, los fabricantes de productos digitales). Según esta propuesta de CRA, dichos productos deben cumplir estrictos requisitos de ciberseguridad, gestión de incidentes y vulnerabilidades, análisis de riesgos y notificación antes de su comercialización en la UE. La gobernanza y el planteamiento legislativo de la CRA se basan en el proceso NLF (Nuevo Marco Legislativo) que existe actualmente para certificar la seguridad de los productos destinados al mercado de la UE.

Horizonte Europa / Europa Digital

- En cuanto a la inversión, la UE ha asignado 10000 millones de euros a acciones de colaboración en materia de ciberseguridad en el marco del programa de investigación, innovación y ciencia Horizonte Europa 2021-2027. También existen fondos disponibles del programa Europa Digital para que las pymes promuevan niveles más altos de ciberseguridad en Europa. Estas iniciativas ofrecen a las pymes más oportunidades de ampliar su presencia en Europa desarrollando productos y servicios nuevos e innovadores relacionados con la ciberseguridad.

La UE ha asignado 10.000 millones de euros para acciones de colaboración en materia de ciberseguridad dentro del programa de investigación, innovación y ciencia Horizonte Europa 2021-2027.

InvestEU / Mecanismo de recuperación y resiliencia de la UE

- La ciberseguridad también forma parte de InvestEU, un instrumento financiero que apoyará el refuerzo de las cadenas de valor de la ciberseguridad en Europa. En el marco del Mecanismo de Recuperación y Recuperación de la UE, muchos países de la UE están adoptando planes que contienen una serie de inversiones adicionales en ciberseguridad.

Año Europeo de las Capacidades 2023

- La Comisión Europea y los Estados miembros de la UE desarrollarán una serie de nuevas iniciativas relacionadas con la ciberseguridad en el ámbito de las capacidades en ciberseguridad en el contexto del despliegue de actividades en el marco del Año Europeo de las Capacidades 2023.

España Digital 2026

- En España, la iniciativa "España Digital 2026", que se enmarca dentro del Plan de Recuperación, Transformación y Resiliencia, como instrumento de despliegue de los fondos europeos de recuperación Next Generation UE, ha creado ocho planes de digitalización específicos, dos de los cuales inciden especialmente en el ámbito de la ciberseguridad en las pymes: el Plan Nacional de Ciberseguridad, aprobado en marzo de 2022, y el Plan de Digitalización de pymes 2021-2025.
- El Plan de Digitalización de pymes incluye el programa "Protege tu empresa" cuyo objetivo es la "sensibilización, concienciación, educación y formación en ciberseguridad dirigido específicamente a empresas, y en especial a todas aquellas del ámbito pymes y micro-empresa. En este mismo plan, la iniciativa "Activa Ciberseguridad" es un programa piloto de Innovación en Ciberseguridad de la pymes impulsado por la Secretaría General de Industria y de la PYMES en el marco de la Estrategia de Industria Conectada 4.0. Adicionalmente, en el marco de digitalización de pymes, se llevó a cabo el lanzamiento del denominado "Kit Digital", una iniciativa orientada a fomentar la transformación digital de las pymes mediante una serie de ayudas que incluyen partidas para la adopción de soluciones digitales básicas en las que pueden incluirse la mejora de la ciberseguridad en las empresas.

¿CÓMO PUEDE EL EIT DIGITAL APOYAR A LAS PYMES EN LA OBTENCIÓN DE NIVELES SUPERIORES DE CIBERSEGURIDAD?

El EIT Digital encarna el futuro de la innovación mediante la movilización de un ecosistema paneuropeo de innovación abierta en el que participan las principales empresas, pymes, start-ups, universidades e institutos de investigación europeos. Estudiantes, investigadores, ingenieros, creadores de empresas e inversores pueden abordar las necesidades tecnológicas, de talento, competencias, negocio y capital del emprendimiento digital.

El EIT Digital crea la próxima generación de empresas, productos y servicios digitales. Esto genera talento empresarial digital, ayudando a las empresas y a los emprendedores a estar en la frontera de la innovación digital proporcionándoles tecnología, talento y apoyo al crecimiento.

El EIT Digital responde a necesidades específicas de innovación, por ejemplo, encontrando los socios adecuados para llevar la tecnología al mercado, apoyando la ampliación de empresas de tecnología digital, atrayendo talento y desarrollando conocimientos y competencias digitales.

En su calidad de mayor ecosistema de innovación digital de Europa, **EIT Digital** contribuye de diversas maneras a elevar el nivel de ciberseguridad de las pymes. Con ello se pretende aumentar el número de productos y servicios europeos de ciberseguridad, que actualmente se sitúa en torno al 16% del mercado mundial de la ciberseguridad. EIT Digital lleva a cabo una serie de iniciativas para apoyar tanto a las empresas de nueva creación como a la ampliación de las pymes:

EU
Los productos y servicios de ciberseguridad europeos

constituyen el

16%
del mercado mundial de ciberseguridad

- A través de su acelerador, EIT Digital identifica y apoya el crecimiento de nuevas empresas europeas de ciberseguridad. Esto contribuye aún más a la diversidad y disponibilidad de soluciones de ciberseguridad para pymes.
- El programa Digital DeepHack del EIT reúne a innovadores digitales y emprendedores para resolver retos empresariales críticos, también en el ámbito de la ciberseguridad.
- La iniciativa Factoría Digital de Innovación del EIT reúne a socios europeos para crear la próxima generación de empresas, productos y servicios digitales.
- El Programa Digital Venture del EIT ofrece ayuda financiera y formación a empresarios europeos para poner en marcha nuevas empresas de alta tecnología.
- El programa de ciberseguridad Digital Masters del EIT ayuda a compensar el déficit de personal cualificado. Esta iniciativa ya se está llevando a cabo en varios países de Europa, como los Países Bajos, Italia, Francia, Hungría, Rumanía y Finlandia. Los temas que se abordan en estos cursos están relacionados con la escasez de competencias en seguridad de la computación en nube, seguridad de las aplicaciones, gestión de riesgos en ciberseguridad, análisis de seguridad, criptografía, seguridad de las infraestructuras de red, validación de sistemas y gestión segura de datos.

¿CÓMO PUEDEN EL CENTRO Y LA RED EUROPEOS DE COMPETENCIA EN CIBERSEGURIDAD ELEVAR LOS NIVELES DE CIBERSEGURIDAD DE LAS PYMES?

- Una de las funciones del Centro Europeo de Competencia en Ciberseguridad (ECCC) es apoyar y coordinar una serie de proyectos de investigación e innovación relacionados con cuestiones de ciberseguridad en Europa. Este es un ejemplo de esfuerzo coordinado en toda la UE para ayudar a garantizar que las pymes puedan traducir las actividades de investigación sobre ciberseguridad en productos y soluciones innovadores para el mercado.
- Las prioridades de trabajo anuales en materia de ciberseguridad del ECCC pueden suponer un fuerte apoyo adicional para que las pymes participen en las iniciativas Horizonte Europa y Europa Digital.
- El ECCC colabora estrechamente con la Red de Centros Nacionales de Coordinación (NCC) de los 27 Estados miembros de la UE. Esta colaboración puede ampliar los programas de apoyo a la ciberseguridad de las pymes en los distintos Estados miembros de la UE y de manera uniforme en toda la UE.
- Apoyar el desarrollo de capacidades en los 27 Estados miembros de la UE para promover normas más estrictas de ciberseguridad y un mayor uso de la certificación de ciberseguridad.

¿QUÉ ORGANISMO DE REFERENCIA TIENEN LAS PYMES EN ESPAÑA?

- En España, el Instituto Nacional de Ciberseguridad (INCIBE) ha sido designado como Centro de Coordinación Nacional (NCC-ES) del Centro Europeo de Competencia en Ciberseguridad.
- INCIBE cuenta con una sólida experiencia en el sector y posee conocimientos especializados en tecnología, investigación e innovación. Además, es una entidad destacada en el desarrollo de la ciberseguridad y en el fomento de la confianza digital entre ciudadanos, instituciones académicas y de investigación, profesionales, empresas y sectores estratégicos. Su Centro de Respuesta a Incidentes INCIBE-CERT es el centro de respuesta de referencia designado en España para entidades privadas. De este modo, INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.
- En el siguiente epígrafe de esta guía, con información y recursos útiles para pymes, se incluyen referencias a los materiales y recomendaciones de INCIBE para las pymes, así como del programa ACTIVA Ciberseguridad, del que INCIBE es colaborador, cuyo objetivo es proporcionar a las pymes un análisis de la situación actual de la empresa en materia de ciberseguridad para conocer su nivel de seguridad y la elaboración de un Plan de Ciberseguridad específico para la misma con un diseño personalizado de acciones de mejora de ciberseguridad

04 INFORMACIÓN Y RECURSOS ÚTILES SOBRE CIBERSEGURIDAD PARA PYMES.

ENISA (Agencia de Ciberseguridad de la Unión Europea)

- Ciberseguridad para las pymes (2021).
  https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes
- SME Cloud Security Tool (2021).
  https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security/security-for-smes/sme-guide-tool
- Mes Europeo de la Ciberseguridad.
  https://cybersecuritymonth.eu/
- Estar alerta, estar preparado - Consejos de ciberseguridad para pymes.
  https://www.youtube.com/watch?v=epJTYOdW3sU&t=24s&ab_channel=ENISAvideos
- Directrices sobre cultura de ciberseguridad. Aspectos conductuales de la ciberseguridad (2021).
  https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/at_download/fullReport
- Marco Europeo de Competencias en Ciberseguridad[7] 2022.
  https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

INCIBE

- Políticas de seguridad para la pyme
  https://www.incibe.es/empresas/herramientas/politicas
- Guías de ciberseguridad para empresas
  https://www.incibe.es/empresas/guias
- Kit de concienciación para empleados
  https://www.incibe.es/empresas/formacion/kit-concienciacion
- Herramientas
  https://www.incibe.es/empresas/herramientas
- Línea de ayuda
  https://www.incibe.es/linea-de-ayuda-en-ciberseguridad

ACTIVA Ciberseguridad (Industria 4.0)

- https://www.industriaconectada40.gob.es/programas-apoyo/Paginas/ACTIVA-Ciberseguridad.aspx

Kit Digital

- https://espanadigital.gob.es/lineas-de-actuacion/programa-kit-digital

Europol

- En caso de ataque de ransomware, las pymes pueden encontrar apoyo para planes de reacción y claves de descifrado, como aconseja Europol.
- https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides
- https://www.nomoreransom.org/es/index.html

ETSI

- Ciberseguridad para pymes. Primera parte: Aspectos esenciales de la normalización de la ciberseguridad.
  https://www.etsi.org/deliver/etsi_tr/103700_103799/10378701/01.01.01_60/tr_10378701v010101p.pdf

OCDE

- Seguridad digital en las pymes 2021.
  https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en#-chapter-d1e7025

Foro Económico Mundial

- ¿Qué deben hacer las pymes para un futuro de ciberseguridad en 2021?
  https://www.weforum.org/agenda/2021/06/cybersecurity-for-smes-europe/

CyberWatching.eu

- Guías para pymes:
  https://cyberwatching.eu/smes-guides

CSIRT (Equipos de Respuesta a Incidentes de Seguridad Informática)

- https://csirtsnetwork.eu/
- https://www.csirt.es/

TALENTO. Universidad de León

- Máster Universitario en Investigación en Ciberseguridad (presencial y a distancia)
- Máster Universitario en Derecho de la Ciberseguridad y Entorno Digital (presencial y a distancia)
- Máster Universitario en Inteligencia de Negocio y Big Data en Entornos Seguros (Interuniversitario y a distancia)
- Máster Universitario Europeo en Derecho, Datos e Inteligencia Artificial (título conjunto internacional)
- Título propio: Certificado de Formación Permanente en Ciberseguridad
- Título propio: Certificado de Formación Permanente en Internet de las Cosas (IoT), Ciberseguridad y Aplicaciones
  https://www.unileon.es/estudiantes/oferta-academica
  https://www.unileon.es/universidad/catedras-extraordinarias-e-institucionales/catedra-ciberseguridad

La información contenida en este documento puede contener declaraciones predictivas incluyendo, sin limitación, declaraciones relativas a los futuros resultados financieros y operativos, futura cartera de productos, nuevas tecnologías, etc.
Existen diversos factores que podrían hacer que los resultados y desarrollos reales difieran materialmente de los expresados o implícitos en las declaraciones predictivas.
Por lo tanto, dicha información se proporciona solo con fines de referencia y no constituye ni una oferta ni una aceptación. Huawei puede cambiar la información en cualquier momento sin previo aviso.