AGENCIA DE LA UNIÓN EUROPEA
PARA LA CIBERSEGURIDAD

Guía de ciberseguridad para pymes

12 PASOS

PARA PROTEGER SU EMPRESA

La crisis de la COVID-19 ha puesto de relieve la importancia de Internet y los ordenadores, en general, para las pymes. Para poder prosperar durante la pandemia, muchas pymes tuvieron que adoptar medidas de continuidad de la actividad, como recurrir a servicios en la nube, mejorar sus servicios a través de Internet, actualizar sus sitios web y hacer posible que el personal trabajara a distancia.

Este folleto presenta doce prácticas medidas de alta calidad para ayudar a las pymes a proteger mejor sus sistemas y sus negocios. Se trata de una publicación complementaria al informe detallado de la ENISA ***«Cybersecurity for SMES – Challenges and Recommendations»*** (Ciberseguridad para pymes: retos y recomendaciones).

1 DESARROLLAR UNA BUENA CULTURA DE LA CIBERSEGURIDAD

ATRIBUIR LA RESPONSABILIDAD DE LA GESTIÓN

Gozar de buena ciberseguridad constituye un elemento clave para lograr el éxito continuado de cualquier pyme. La responsabilidad de ejercer esta función fundamental debe atribuirse a alguien de la empresa que garantice que se destinan a la ciberseguridad los recursos adecuados: tiempo del personal, la compra de software, servicios y hardware de ciberseguridad, la formación del personal y el desarrollo de políticas eficaces.

AUMENTAR LA IMPLICACIÓN DE LOS EMPLEADOS

Aumente la participación de los empleados mediante una comunicación eficaz sobre ciberseguridad por parte de la dirección, de manera que los directivos muestren su apoyo explícito a las iniciativas de ciberseguridad, se imparta formación adecuada a los empleados y se establezcan normas específicas y claras en las políticas de ciberseguridad para los empleados.

PUBLICAR POLÍTICAS DE CIBERSEGURIDAD

Las normas contenidas en las políticas de ciberseguridad deben ser claras y específicas y explicar a los empleados cómo deben actuar cuando utilicen los servicios, los equipos y el entorno de telecomunicaciones de la empresa. Estas políticas también deben señalar las consecuencias a las que se pueden enfrentar los empleados que no cumplan dichas políticas. Estas políticas deben revisarse y actualizarse periódicamente.

REALIZAR AUDITORÍAS DE CIBERSEGURIDAD

Los profesionales con conocimientos, formación y experiencia adecuados deben llevar a cabo auditorías periódicas. Los auditores deben ser independientes, ya se trate de contratistas externo o internos de la pyme, y ajenos a las actividades informáticas cotidianas.

RECORDAR LA PROTECCIÓN DE DATOS

En virtud del Reglamento General de Protección de Datos[1] de la UE, todas las pymes que traten o almacenen datos personales de residentes en la UE/el EEE deben garantizar que se realizan los controles de seguridad adecuados para proteger dichos datos. Asimismo, se debe garantizar que los terceros que trabajan en nombre de la pyme en cuestión apliquen medidas de seguridad adecuadas.

1 Reglamento General de Protección de Datos https://ec.europa.eu/info/law/law-topic/data-protection_es

2

IMPARTIR FORMACIÓN ADECUADA

Imparta formación periódica sobre concienciación en materia de ciberseguridad para todos los empleados, a fin de garantizar que puedan reconocer y hacer frente a las distintas amenazas informáticas. Estas sesiones formativas deben adaptarse a las pymes y centrarse en situaciones de la vida real.

Imparta formación especializada sobre ciberseguridad para los responsables de la gestión de la ciberseguridad en la empresa, a fin de garantizar que poseen los conocimientos y las competencias necesarios para ejercer su trabajo.

3

GARANTIZAR UNA GESTIÓN EFICAZ DE TERCEROS

Garantice que todos los proveedores, en particular aquellos que tienen acceso a sistemas o datos sensibles, se gestionan de manera activa y que cumplen los niveles de seguridad acordados. Deben firmarse acuerdos que regulen el cumplimiento de estos requisitos de seguridad por parte de los proveedores.

4

DESARROLLAR UN PLAN DE RESPUESTA ANTE INCIDENTES

Desarrolle un plan formal de respuesta ante incidentes que incluya directrices claras, funciones y responsabilidades documentadas para garantizar que todos los incidentes de seguridad reciban una respuesta oportuna, profesional y adecuada. Para responder de forma rápida a las amenazas de seguridad, busque herramientas que permitan controlar y crear alertas cuando se detecte alguna actividad sospechosa o fallos de seguridad.

5 PROTEGER EL ACCESO A LOS SISTEMAS

Anime a todo el mundo a que utilice una frase de contraseña, una combinación de al menos tres palabras corrientes escogidas de forma aleatoria que formen una frase fácil de memorizar y segura. Si decide utilizar una contraseña corriente:

- Asegúrese de que sea larga, con caracteres en mayúscula y minúscula y, a ser posible, números y caracteres especiales
- Evite palabras obvias, como «contraseña», o secuencias de letras o números como «abc» o «123»
- No utilice información personal que se pueda encontrar en Internet

Y, tanto si utiliza contraseñas como frases de contraseña:

- No las reutilice en otros sitios
- No las comparta con compañeros
- Active la autenticación de doble factor
- Utilice un gestor de contraseñas específico

6

PROTEGER LOS DISPOSITIVOS

Dentro de un programa de ciberseguridad, mantener protegidos los dispositivos que utiliza el personal, ya sean sus ordenadores de sobremesa, portátiles, tabletas o teléfonos móviles, es un paso fundamental.

MANTENER EL SOFTWARE A PUNTO Y ACTUALIZADO

Lo ideal sería utilizar una plataforma centralizada para gestionar los parches. Es muy recomendable que las pymes:

- Actualicen de manera periódica todo su software
- Activen las actualizaciones automáticas cuando sea posible
- Sepan qué software y hardware necesitan actualizaciones manuales
- Tengan en cuenta los dispositivos móviles y de Internet de las Cosas

USAR UN ANTIVIRUS

Debe implementarse una solución de antivirus gestionada a nivel central en todos los dispositivos y mantenerla actualizada para garantizar su eficacia constante. Asimismo, no se debe instalar software pirata, ya que puede contener programas maliciosos.

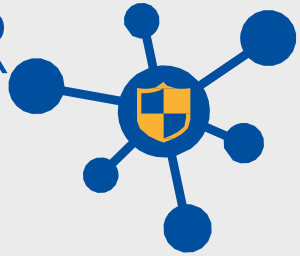
UTILIZAR HERRAMIENTAS DE PROTECCIÓN DE LA WEB Y DEL CORREO ELECTRÓNICO

Utilice soluciones para bloquear correos no deseados, correos con enlaces a sitios web maliciosos, correos con anexos maliciosos como por ejemplo virus y correos *phishing*.

CIFRAR LOS DATOS

Utilice el cifrado para proteger los datos. Las pymes deben asegurarse de que los datos almacenados en dispositivos móviles —como ordenadores portátiles, teléfonos móviles y tabletas— están cifrados. En el caso de los datos transferidos a través de redes públicas, como redes wifi de hoteles o aeropuertos, asegúrese de que estos datos estén cifrados, ya sea usando una red privada virtual (VPN) o accediendo a sitios web a través de conexiones seguras mediante un protocolo SSL/TLS. Asegúrese de que sus propios sitios web utilizan tecnología de cifrado adecuada para proteger los datos de los clientes mientras se transfiere a través de Internet.

7 PROTEGER SU RED



USAR CORTAFUEGOS

Los cortafuegos gestionan el tráfico que entra y sale de una red y constituyen una herramienta fundamental para proteger los sistemas de las pymes. Los cortafuegos deben implantarse para proteger todos los sistemas importantes; en particular, debe utilizarse un cortafuegos para proteger la red de la pyme en Internet.

REVISAR LAS SOLUCIONES DE ACCESO REMOTO

Las pymes deben revisar periódicamente todas las herramientas de acceso remoto para garantizar que están protegidas, en particular:

- Asegurarse de que todo el software de acceso remoto tiene instalados todos los parches y está actualizado
- Restringir el acceso remoto desde ubicaciones geográficas sospechosas o determinadas direcciones IP
- Limitar el acceso remoto por parte del personal solo a los sistemas y ordenadores que necesiten para su trabajo
- Implementar contraseñas seguras para el acceso remoto y, en la medida de lo posible, activar la autenticación de doble factor
- Asegurarse de que esté activado un sistema de control y alertas para avisar de posibles ataques o de actividades sospechosas extrañas

UTILIZAR UN GESTOR DE DISPOSITIVOS MÓVILES

Cuando habilitan el trabajo a distancia para su personal, muchas pymes permiten que los trabajadores utilicen sus propios ordenadores portátiles, tabletas o teléfonos móviles. Esto presenta varios problemas de seguridad en relación con los datos confidenciales de la empresa almacenados en dichos dispositivos. Una manera de gestionar este riesgo es utilizar una solución de gestión de dispositivos móviles (MDM) que permita a las pymes:

- Controlar qué dispositivos pueden acceder a sus sistemas y servicios
- Garantizar que el dispositivo cuenta con un software de antivirus actualizado
- Determinar si el dispositivo está cifrado
- Confirmar si el dispositivo cuenta con parches de software actualizados
- Hacer que el dispositivo esté protegido por una contraseña o un PIN
- Borrar a distancia cualquier dato de la pyme del dispositivo si su propietario comunica que lo ha perdido o se lo han robado, o si el propietario del dispositivo ya no trabaja para la pyme

8 MEJORAR LA SEGURIDAD FÍSICA

Deben realizarse controles físicos adecuados en los lugares donde se almacene información importante. Por ejemplo, el teléfono móvil o el ordenador portátil de la empresa no deben descuidarse en el asiento trasero del coche. Siempre que el usuario se aleje de su ordenador, debe bloquearlo o, como alternativa, activar la función de autobloqueo en los dispositivos que utilice para trabajar. Asimismo, los documentos impresos sensibles tampoco deben descuidarse y, cuando no se utilicen, deben guardarse en un lugar seguro.

9 PROTEGER LAS COPIAS DE SEGURIDAD

Para permitir la recuperación de información clave, hay que realizar un mantenimiento de las copias de seguridad, puesto que son una vía eficaz para la recuperación de desastres, como los ataques de programas *ransomware*. Deben aplicarse las siguientes normas a las copias de seguridad:

- La copia de seguridad se creará periódicamente y, a ser posible, de forma automática
- La copia de seguridad estará separada del entorno de producción de la pyme
- Las copias de seguridad estarán cifradas, sobre todo si hay que desplazarlas a otra ubicación
- Se comprobará de forma periódica la capacidad de recuperar datos a partir de la copia de seguridad Lo ideal sería realizar una prueba periódica de restauración completa de inicio a fin.

10

TRABAJAR EN LA NUBE

Además de ofrecer muchas ventajas, las soluciones en la nube presentan algunos riesgos específicos que las pymes deben tener en cuenta antes de trabajar con un proveedor de servicios en la nube. Las pymes deberían consultar la «*Cloud Security Guide for SMEs*»[2] (Guía de seguridad en la nube para pymes) publicada por la ENISA cuando decidan hacer la transición a un sistema en la nube.

A la hora de seleccionar un proveedor de servicios en la nube, la pyme debe asegurarse de que no incumple ninguna ley ni reglamento de almacenamiento de datos, sobre todo de datos personales, fuera de la UE/el EEE. Por ejemplo, el RGPD de la UE exige que los datos personales de los residentes de la UE/el EEE no se almacenen o transfieran fuera de la UE/el EEE, a menos que se den circunstancias muy específicas.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 PROTEGER SUS SITIOS WEB

Es fundamental que las pymes se aseguren de que sus sitios web estén configurados de manera segura y de que los datos personales o la información financiera, como los datos de las tarjetas de crédito, estén debidamente protegidos. Para ello, será necesario realizar pruebas de seguridad periódicas de los sitios web para identificar las posibles deficiencias de seguridad y llevar a cabo revisiones frecuentes para garantizar que el sitio está correctamente actualizado y mantenido.

12 BUSCAR Y COMPARTIR INFORMACIÓN

El intercambio de información constituye una herramienta eficaz para la lucha contra la ciberdelincuencia. El intercambio de información sobre ciberdelincuencia es fundamental para que las pymes entiendan mejor los riesgos a los que se enfrentan. Las empresas que, a través de compañeros, han conocido problemas de ciberseguridad y cómo se han superado son más propensas a tomar medidas para proteger sus sistemas que si hubiesen recibido información similar de informes del sector o encuestas sobre ciberseguridad.

AGENCIA DE LA UNIÓN EUROPEA
PARA LA CIBERSEGURIDAD

ACERCA DE LA ENISA

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada mediante el Reglamento sobre la Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del día de mañana en materia de ciberseguridad. A través del intercambio de conocimientos, el desarrollo de capacidades y la sensibilización, la Agencia coopera con las partes interesadas clave para reforzar la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para mantener la seguridad digital de la sociedad y de los ciudadanos de Europa. Para más información, consulte www.enisa.europa.eu.

ENISA
Agencia de la Unión Europea para la Ciberseguridad

Oficina de Atenas
Ethnikis Antistaseos 72 y
Agamemnonos 14,
Chalandri 15231, Attiki, Grecia

Oficina de Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Grecia

enisa.europa.eu