**Ficha de formación**

|  |  |
| --- | --- |
| **Título** | Ciberseguridad en la oficina (desde casa) |
| **Palabras clave (meta tag)** | ciberseguridad, seguridad, malware, phishing, información sensible |
| **Proporcionado por** | Internet Web Solutions |
| **Idioma** | Español |
| **Área de formación** |
|  | Innovación y Servitización |
| **X** | Transformación Digital |
|  | Localización |
|  | Sostenibilidad |
| **Competencias y habilidades ESCO** |
| * Habilidades y competencias transversales
	+ Habilidades sociales y emocionales
	+ Pensamiento crítico
	+ Pensamiento analítico
	+ Resolución de problemas
	+ Autogestión
	+ Gestión de negocio
	+ Adaptabilidad
	+ Resiliencia
	+ Creatividad
	+ Networking
	+ Iniciativa
	+ Flexibilidad
	+ Sinceridad
	+ Comprensión de la complejidad
	+ Cooperación
	+ Empatía
	+ Innovación
	+ Liderazgo

 * Habilidades
	+ Habilidades tecnológicas
	+ Marketing de producto
	+ Marketing digital
	+ Habilidades digitales
	+ Comunicación
	+ Cooperación
	+ Inteligencia emocional

 * Conocimiento
	+ Gestión de negocio
	+ Aprendizaje y formación online
	+ Publicidad
	+ Computación en la nube
	+ Big data
	+ Comercio electrónico
	+ Inteligencia Artificial
	+ IoT
	+ Alfabetización digital
	+ Ciberseguridad
	+ Minado y análisis de datos
	+ Sostenibilidad
	+ Bienestar
	+ Cambio climático
	+ Gestión de redes sociales
 |
| **Adelanto** |
| “¿Sabía que el 85% de las MiPymes europeas consideran la ciberseguridad como una preocupación clave para sus negocios?” |
| **Objetivos / resultados de aprendizaje** |
| En este módulo aprenderás qué es la ciberseguridad, familiarizándote con los términos más comúnmente utilizados en este campo y conociendo cuáles son los ciberataques más habituales al trabajar desde casa y desde la oficina. De esta forma, serás capaz de prevenir los principales riesgos cibernéticos y de navegar de forma segura, no sólo al trabajar desde casa sino también al realizar gestiones cotidianas por Internet, incrementando así tus habilidades y conocimientos sobre seguridad informática. |
| **Descripción** |
| La mayoría de las MiPymes europeas consideran la ciberseguridad como una preocupación clave para sus negocios. Sin embargo, en un contexto post-pandémico, no todas las empresas han implementado nuevas medidas de seguridad para combatir los riesgos derivados del trabajo remoto debido al desconocimiento y la falta de habilidades de ciberseguridad. Este módulo permitirá al personal de las MiPymes y a los emprendedores mejorar sus competencias y conocimientos sobre ciberseguridad con el fin de incrementar sus habilidades digitales y su ciber resiliencia. |
| **Listado de beneficios para los emprendedores** |
| ✓ La implementación de estrategias de ciberseguridad en las MiPymes reducen el riesgo de pérdidas o filtraciones de información, manteniendo la integridad de los datos.✓ Al mantener la información del cliente como confidencial, la reputación y la imagen corporativa mejora de cara al público.✓ La ciberseguridad incrementa la resiliencia y la capacidad de recuperación de las empresas, con copias de seguridad que les permiten regresar a la normalidad tras un incidente inesperado.✓ Al reducir las pérdidas de información debido a los ciberataques o problemas internos, hay un incremento en la productividad.✓ La ciberseguridad es una herramienta esencial para los empleados y los emprendedores, no solo en su vida laboral sino también en su vida personal, al estar más concienciados y prevenidos frente a los riesgos cibernéticos (p.ej., en las compras online). |
| **Contenidos organizados en 3 niveles** |
| **Módulo: Ciberseguridad en la oficina (desde casa)****Unidad 1: Fundamentos de ciberseguridad****Sección 1.1: ¿Qué es la ciberseguridad?**El término “**ciberseguridad**” nació en la década de 1970 debido a la necesidad que tenían las empresas de **proteger sus sistemas informáticos** de los ataques maliciosos que pudieran comprometer su buen funcionamiento haciendo un uso indebido de la información.La ciberseguridad incluye la aplicación de herramientas, tecnologías, políticas, controles y procedimientos en la protección o la recuperación de redes, sistemas, dispositivos y aplicaciones de **ataques cibernéticos** orientados a acceder, destruir o alterar información sensible, interrumpir flujos de trabajo, o extorsionar a organizaciones o individuos a cambio de dinero.De acuerdo con un informe de 2021 elaborado por la Agencia para la Ciberseguridad de la Unión Europea (ENISA), de un total de 249 pymes europeas analizadas, el **85% considera la ciberseguridad como una preocupación clave para sus negocios**. En un contexto post-pandémico, un 45% de las Pymes implementaron nuevas tecnologías en respuesta a la pandemia, y sin embargo, el 90% no incluyeron nuevas medidas de seguridad.Del mismo informe, que aporta valiosa información sobre la ciberseguridad de las MiPymes europeas, se extraen los **principales incidentes de ciberseguridad que sufren las pymes europeas en base a su origen**, tal y como se aprecia en la gráfica.Fuente: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes> (elaboración propia)**Sección 1.2: Principales definiciones**Seguridad general:* **Copia de seguridad**: copia de los archivos y programas que se almacena en otros dispositivos u otros soportes, con el fin de recuperar la información en caso de fallo, pérdida o robo.
* **Información sensible**: información que contiene datos privados o confidenciales, como datos personales o bancarios.
* **Software**: un software es un programa informático diseñado para realizar unas tareas específicas, por ejemplo el navegador, un juego, etc. Es la contraposición del “hardware”, que son los componentes físicos del dispositivo, como la placa base o el procesador.
* **Cifrado**: es un proceso que convierte un documento o un archivo en información ilegible para las personas que no posean la clave para descifrarlo. Sirve para proteger la información de las personas que no deben acceder a ella.
* **HTTP / HTTPS**: uno de los protocolos más utilizados en la navegación por Internet. HTTPS (HyperText Transfer Protocol Secure) se trata de la versión segura, y garantiza que la información que se transmite entre nuestro dispositivo y la página web está cifrada y protegida.
* **Cortafuegos / Firewall**: al navegar por la red y acceder a una web, esta se comunica con nuestro equipo para establecer la conexión. El firewall o cortafuegos analiza este tipo de conexiones para impedir el acceso a las que puedan suponer un riesgo.

Amenazas:* **Ingeniería social**: la ingeniería social no requiere de altos conocimientos informáticos, ya que consiste en la manipulación de las personas a través de técnicas psicológicas y habilidades sociales, y suele utilizarse para obtener información confidencial, como contraseñas o datos bancarios. Las técnicas de phishing se basan en la ingeniería social.
* **Phishing**: la técnica de hacerse pasar por otra persona o entidad a través de correo electrónico, que lleva al usuario a realizar alguna acción en una página fraudulenta para obtener contraseñas o descargar un archivo infectado.
* **Smishing**: SMS + phishing. De forma similar al phishing, en esta técnica se utilizan los mensajes por SMS para el mismo fin.
* **Vishing**: voice + phishing. En este caso, el atacante finge ser otra persona en una llamada de teléfono, frecuentemente haciéndose pasar por servicio técnico del dispositivo o de la compañía telefónica.
* **Ataques basados en la web**: estos complejos ataques actúan cuando utilizas Internet, haciendo uso de software malicioso para infectar los dispositivos que no cuentan con la seguridad necesaria o no están actualizados.

Tipos de malware:* **Malware**: un malware es un software malicioso que puede presentarse de distintas formas (como código ejecutable, scripts, etc.), y que puede realizar acciones como encriptar o eliminar datos confidenciales, alterar las funciones básicas del dispositivo, espiar la actividad del usuario, entre otros. El antimalware es el software cuya función es la de detectar, proteger y eliminar este tipo de software malicioso.
* **Virus informático**: este tipo de malware tiene el objetivo de alterar el funcionamiento del dispositivo, y requiere de la interacción del usuario para propagarse a otros archivos y sistemas.
* **Gusano informático**: es capaz de replicarse y moverse de un dispositivo infectado a otros a través de la red. Frecuentemente proviene de unidades USB infectadas, de archivos adjuntos en correos electrónicos, o incluso de sitios web.
* **Troyano**: este tipo de malware entra al sistema como un archivo o software inofensivo, y realiza acciones no deseadas en segundo plano, como eliminación de archivos o descarga de otros malwares.
* **Spyware**: como su nombre indica, este tipo de malware espía el dispositivo infectado, recogiendo información sobre la actividad del usuario. Suele provenir de spam o webs de descargas fraudulentas.
* **Adware**: malware que rastrea el navegador y el historial de descargas del usuario para así mostrar anuncios o banners no deseados para que el usuario haga clic. Suelen infectar los dispositivos a través de webs infectadas o webs de descargas fraudulentas.
* **Ransomware**: un peligroso tipo de malware que cifra los archivos del disco duro del dispositivo y restringe el acceso al usuario, pidiendo un rescate, por lo general en criptomonedas, a cambio de descifrar los archivos. Un caso muy conocido es el de [**WannaCry**](https://www.europol.europa.eu/wannacry-ransomware).

**Unidad 2: Ciberseguridad…****Sección 2.1: …en el lugar de trabajo****La ciberseguridad es responsabilidad de todos en una empresa**, tanto del equipo de gestión como de los empleados, por lo que también debe formar parte de la cultura de trabajo de la empresa.Tanto en el trabajo en la oficina como desde casa, cumplir con una serie de **medidas básicas enmarcadas dentro de un plan de ciberseguridad** es totalmente necesario para el buen funcionamiento del negocio.A continuación se propone un **plan de ciberseguridad básico** a seguir para mantener la integridad de la información de la empresa:* **Informar sobre las políticas de ciberseguridad de la empresa.** Cada empresa tiene necesidades únicas, por lo que deberán elaborarse políticas de ciberseguridad a seguir por parte de todos los empleados y gerentes para crear una cultura de ciberseguridad.
* **Actualizar el software de los dispositivos.** Mantener todas las aplicaciones y sistemas operativos actualizados previene las vulnerabilidades.
* **Configurar un cortafuegos.** Un cortafuegos aportará protección adicional en la navegación por Internet.
* **Realizar copias de seguridad regularmente.** En caso de pérdidas de información, las copias de seguridad ayudarán a restaurar la normalidad rápidamente.
* **Asegurar las redes wifi.** Las redes wifi que se utilicen en la actividad diaria deberán estar correctamente configuradas para ser suficientemente seguras frente a terceros.
* **Instalar software antimalware.** Para protegerse de los posibles ataques.
* **Elaborar un plan de acción para los dispositivos móviles.** La ciberseguridad no es sólo para los ordenadores, sino también para dispositivos móviles como smartphones o tablets, que también deberán contar con medidas de protección.
* **Implementar procedimientos para la protección de la información.** Deberán establecerse procedimientos a seguir en caso de incidentes de ciberseguridad.
* **Utilizar contraseñas seguras.** Deberán combinar números, letras y caracteres especiales. Una forma de comprobar si las contraseñas son seguras es la web <https://password.kaspersky.com/es/>.
* **Restringir los permisos para la instalación de software.** Los empleados deberán tener un acceso limitado a la hora de instalar nuevo software, con el fin de evitar la instalación de aplicaciones fraudulentas que puedan infectar los dispositivos de la red.

**Sección 2.2: …en el trabajo remoto****En el trabajo remoto, la ciberseguridad es incluso más importante**, ya que al trabajar desde casa no existe el mismo control en cuanto a los procedimientos y políticas de ciberseguridad de la empresa, las redes son menos seguras, puede haber errores de configuración, falta de formación, entre otros.Es por ello que hay que tener en consideración nuevas medidas que puedan garantizar el cumplimiento de los siguientes **objetivos de ciberseguridad en el acceso remoto a la información**:* **Disponibilidad**. Los usuarios autorizados deben tener acceso a la información cuando sea necesario.
* **Confidencialidad**. Debe garantizarse que sólo los usuarios autorizados puedan acceder a la información.
* **Autenticidad**. Debe garantizarse que los usuarios autorizados (con acceso a la información) son quienes dicen ser.
* **Trazabilidad**. Debe ser posible rastrear el acceso indebido o no autorizado a la información.
* **Integridad**. Debe garantizarse que la información y sus métodos de tratamiento sean exactos y completos.

De forma complementaria al cumplimiento del plan de ciberseguridad ya mencionado, será muy recomendable el uso de una **VPN** (**Virtual Private Network** – Red privada virtual). Este tecnología de red permite una conexión segura entre la red local e Internet, de forma que se **garantiza la integridad y confidencialidad de la información**.Además, las **aplicaciones de acceso de escritorio remoto** permitirán a los teletrabajadores controlar de forma remota los equipos que se encuentran físicamente en la oficina, como por ejemplo la herramienta TeamViewer.Las **soluciones en la nube** y las **herramientas colaborativas** también constituyen importantes herramientas para la ciberseguridad en el trabajo remoto, permitiendo la **accesibilidad a la información de forma rápida y coordinada**.Algunos ejemplos de herramientas para el trabajo remoto son:**VPN:*** **hide.me**. Este servicio VPN permite navegar de forma privada, sin restricciones geográficas. Cuenta con más de 2000 servidores y 75 localizaciones. <https://hide.me/>
* **PrivadoVPN**. Con sede en Suiza, su versión gratuita permite proteger hasta 10 GB de datos al mes. <https://privadovpn.com/>

**Escritorio remoto:*** **AnyDesk**. Se trata de un software de escritorio remoto que también está disponible gratuitamente para uso personal. Este tipo de herramienta permite acceder a la información desde cualquier lugar, lo que mejora la comunicación interna. <https://anydesk.com/>
* **TeamViewer**. Esta herramienta se centra más en el acceso remoto a la información, ya que permite acceder a cualquier dispositivo desde cualquier lugar. Permite compartir archivos de forma segura y acceder a otros dispositivos, y es gratuita para uso personal. <https://www.teamviewer.com/>

**Soluciones en la nube:*** **Dropbox**. El plan gratuito ofrece 2 GB de almacenamiento, y los planes de pago llegan hasta los 3 TB de almacenamiento. <https://www.dropbox.com/>
* **MEGA**. Esta plataforma incluye 20 GB gratuitos, y cuenta con planes de pago para particulares de hasta 16 TB, y para empresas de hasta 10 PB, lo que la convierte en una de las soluciones con mayor capacidad. <https://mega.io/>

**Herramientas colaborativas:*** **Slack**. Esta plataforma de mensajería instantánea permite la integración con otras herramientas y simplifica la comunicación en equipo. La versión gratuita permite acceder al historial de los últimos 10.000 mensajes de equipo, realizar videollamadas con compañeros e integrarse con 10 aplicaciones. <https://slack.com/>
* **Trello**. Esta herramienta funciona con el sistema de tarjetas Kanban, y permite incluir notas, archivos, plazos y otros elementos. Es fácil de gestionar arrastrando las tarjetas, y está disponible en varios idiomas. Esta herramienta es gratuita hasta 10 tarjetas por equipo. <https://trello.com/>

**Unidad 3: Recomendaciones para emprendedores y personal****Sección 3.1: Recomendaciones para emprendedores*** Asegúrate de que tu empresa cuente con un **plan de ciberseguridad** adecuado a las necesidades y a las posibles vulnerabilidades de tu negocio.
* Establece **normativas y procedimientos para una gestión segura de la información**; p. ej., que no se utilicen dispositivos personales, destruir los documentos de forma segura.
* **Forma a tus trabajadores** en materia de ciberseguridad para que puedan cumplir con las políticas y procedimientos.
* **Mejora tus habilidades digitales y de ciberseguridad**; recuerda que manejas información muy sensible.
* ¡Cumple también con las **recomendaciones para el personal**! ☺

**Sección 3.2: Recomendaciones para el personal*** La ciberseguridad comienza por la **seguridad física de la información**: mantén el escritorio libre de información confidencial, post-its con contraseñas, emails, etc.
* No conectes **dispositivos USB** que provengan de personas que no son de confianza, ya que podrían infectar tu equipo.
* **Cifra la información confidencial antes de enviarla**, por ejemplo a través de un archivo compromido con contraseña.
* Recuerda **vaciar la papelera** de tu ordenador con regularidad.
* Realiza **copias de seguridad** con regularidad.
* Fuera de la empresa, **vigila bien tus dispositivos móviles**.
* En la medida de lo posible, **evita conectarte a redes wifi abiertas** con dispositivos de trabajo. Si necesitas hacerlo, utiliza una VPN por seguridad.
* **Bloquea tu ordenador** cuando te ausentes de tu puesto de trabajo.
* Utiliza **contraseñas que sean seguras**. Puedes comprobar la seguridad de tus contraseñas en webs dedicadas a ello, como <https://password.kaspersky.com/es/>.
* **No utilices siempre las mismas contraseñas**, puesto que serás más vulnerable en caso de que se filtren.
* No descargues archivos adjuntos de **remitentes desconocidos**, desconfía de **mensajes sospechosos** e **informa** a tus superiores de cualquier incidente.
 |
| **Contenido por puntos** |
| * La ciberseguridad surgió por la necesidad de las empresas de proteger sus sistemas informáticos de ataques maliciosos.
* Los incidentes de ciberseguridad que más sufren las MiPymes europeas se relacionan con el phishing.
* La ciberseguridad es responsabilidad de todos en una empresa, y es necesario contar con un plan de ciberseguridad que se cumpla debidamente por parte de gerentes, directivos y empleados.
* En el trabajo remoto, la ciberseguridad se complementa con el uso de herramientas TIC que permiten el cumplimiento de los cinco objetivos de la ciberseguridad en el acceso a la información.
* El empresario debe asegurarse de que exista un plan de ciberseguridad, y de que los empleados cuenten con las habilidades necesarias para cumplirlo.
* Los trabajadores deberán estar comprometidos en la gestión segura de la información durante su trabajo.
 |
| **5 entradas de glosario** |
| **Ciberseguridad.** La aplicación de herramientas, tecnologías, políticas, controles y procedimientos en la protección o la recuperación de redes, sistemas, dispositivos y aplicaciones de ataques cibernéticos orientados a acceder, destruir o alterar información sensible, interrumpir flujos de trabajo, o extorsionar a organizaciones o individuos a cambio de dinero.**Phishing.** La técnica de hacerse pasar por otra persona o entidad a través de correo electrónico, que lleva al usuario a realizar alguna acción en una página fraudulenta para obtener contraseñas o descargar un archivo infectado. Similares son el vishing (voz + phishing) o el smishing (SMS + phishing).**Malware.** Software malicioso que puede presentarse de distintas formas (como código ejecutable, scripts, etc.), y que puede realizar acciones como encriptar o eliminar datos confidenciales, alterar las funciones básicas del dispositivo, espiar la actividad del usuario, entre otros. Los virus, gusanos, adwares, troyanos, spyware y ransomware también son malwares.**Copia de seguridad.** También conocida como “backup”, es una copia de los archivos y programas que se almacena en otros dispositivos u otros soportes, con el fin de recuperar la información en caso de fallo, pérdida o robo.**Información sensible.** Información que contiene datos privados o confidenciales, como datos personales o bancarios. |
| **Bibliografía y referencias** |
| <https://www.redseguridad.com/especialidades-tic/como-definir-la-ciberseguridad-en-un-entorno-laboral-hibrido_20210928.html> <https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-web-based-attacks-ebook-en-es.pdf> <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes> <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes> <https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf> <https://www.microfocus.com/en-us/what-is/cyber-security> <https://www.osi.es/es/actualidad/blog/2021/06/28/conceptos-basicos-de-ciberseguridad-que-debes-conocer> <https://es.linkedin.com/pulse/recomendaciones-de-ciberseguridad-en-el-puesto-trabajo-pizarro> <https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html> <https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/> <https://uniserveit.com/blog/10-step-cybersecurity-plan-for-your-small-business> <https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-europes-smes> <https://www.europol.europa.eu/wannacry-ransomware>  |
| **Cinco preguntas de elección múltiple para autoevaluación**Una vez completado el mecanismo de validación, los usuarios podrán generar certificados de asistencia y de finalización personalizados. | **Pregunta 1. ¿Qué se entiende por “ciberseguridad"?**Opción a: Las herramientas destinadas a proteger los dispositivos de ataques de malwares.Opción b: Los procedimientos destinados a proteger la información sensible de los ataques maliciosos.Opción c: La protección de los sistemas informáticos de la empresa.Opción d: Todas las respuestas son correctas.**Opción correcta: d****Pregunta 2. ¿Qué deberías hacer para prevenir el phishing?**Opción a: Desconfiar de emails no solicitados para cambiar una contraseña.Opción b: Hacer clic en los enlaces de los emails..Opción c: Descargar archivos adjuntos de emails de spam.Opción d: Coger llamadas de teléfono de números desconocidos.**Opción correcta: a****Pregunta 3. ¿Cuál es el ataque más común a las MiPymes europeas?**Opción a: Denegación de servicio.Opción b: Ransomware.Opción c: Phishing.Opción d: Ninguna es correcta.**Opción correcta: c****Pregunta 4. ¿Cuáles de los siguientes son objetivos de ciberseguridad en el acceso remoto a la información?**Opción a: Disponibilidad, confidencialidad.Opción b: Trazabilidad, públicidad.Opción c: Confidencialidad, corrupción.Opción d: Integridad, medible.**Opción correcta: a****Pregunta 5. ¿Qué harías con un USB que encuentras en una mesa de la oficina?**Opción a: Conectarlo a mi ordenador para ver qué contiene y poder devolverlo a su dueño.Opción b: Trataría de buscar su dueño sin conectarlo a ningún equipo.Opción c: Denunciarlo a la policía.Opción d: Tirarlo a la basura.**Opción correcta: b** |
| **Material relacionado** | RESTART\_PR3\_COU\_03\_IWS\_Cybersecurity\_ES.pptx |
| **Enlace de referencia** | - |
| **Vídeo en formato YouTube (si lo hay)** | <https://www.youtube.com/watch?v=PSrnvEEDpuY>  |