**Ficha de Formación**

|  |  |
| --- | --- |
| **Título** | Ciberseguridad y herramientas digitales para las PYMES. Prepárate para prevenir y solventar Ciberataques. |
| **Palabras clave**  | Ciberseguridad, Seguridad, Prevención, Cibercrímenes, Ciberataques,  |
| **Proporcionado por** | ITSFA |
| **Idioma** | Español  |
| **Área** | Comunicación online y digital |  |
| Compromiso de las personas y del equipo desde casa |  |
| Conciliación de la vida laboral y familiar |  |
| Bienestar personal |  |
| ¿Como impulsar la productividad de tu equipo desde casa? |  |
| Gestión de proyectos a distancia |  |
| Gestión ágil por objetivos        |  |
| Autoeficacia inteligente |  |
| Liderazgo y motivación en la era del Smart Working |  |
| Teletrabajo: una selección de herramientas digitales para gestionar tu negocio | **X** |
| **Objetivos / metas / resultados de aprendizaje** |
| En este curso adquirirás un conocimiento básico sobre Ciberseguridad, tanto como a nivel empresarial, como a nivel de usuario/ empleado. Aprenderás las definiciones de los principales ciber riesgos que pueden poner en peligro tu seguridad y la seguridad de tu empresa. Además, aprenderás las principales herramientas para prevenir cibercrímenes con un Guía básica de ciberseguridad, que te ayudará a saber cuáles son las principales medidas a seguir para proteger tu PYME de estas amenazas, y así, poder trabajar desde casa de una manera segura. |
| **Descripción** |
| Debido a la pandemia del Covid-19, las PYMES, por sus características intrínsecas, se han convertido en el objetivo de los cibercriminales. Las nuevas formas de trabajo que ha traído la pandemia, como el teletrabajo, trabajo a distancia o en remoto, o en otras palabras, lo que es conocido como Smart working o trabajo inteligente, han propiciado que sea de vital importancia para las PYMES adquirir los conocimientos necesarios que les ayuden a sobrevivir, subiéndose al tren de la digitalización y así no quedarse atrás. Uno de estos conocimientos, es la Ciberseguridad. Con este curso, las PYME podrán obtener un conocimiento básico de ciberseguridad, y así, tener las herramientas necesarias para poder prevenir los ciber riesgos que ponen en peligro la supervivencia de sus negocios, en un mundo que se dirige sin frenos hacia la digitalización. |
| **Contenidos organizados en 3 niveles** |
|   2. Ciberseguridad y herramientas digitales para las PYME. Prepárate para prevenir y solventar Ciberataques. 2.1 Seguridad a nivel empresarial-Qué es la ciberseguridad? Debido a la digitalización, la Ciberseguridad para las PYMES es un tema crucial hoy en día. Los ciberataques se dirigen cada vez más a las pequeñas y medianas empresas que no están tan protegidas como pueden estarlo las grandes compañías. La ciberseguridad es un conjunto de prácticas para defender los sistemas y programas informáticos de los cibercrímenes. La ciberdelincuencia es toda actividad delictiva que tiene lugar en el mundo digital, en la que interviene un ordenador, un dispositivo conectado a una red o una red, y que tiene por objetivo conseguir un determinado propósito o beneficio, que puede ser de diferente índole. La ciberseguridad abarca muchas áreas: seguridad de la red, seguridad de las aplicaciones, seguridad de la información, seguridad del usuario, etc. Veamos ahora algunos conceptos a considerar desde una perspectiva empresarial, para luego finalizar el curso con la Guía básica de ciberseguridad. -Ransomware Ransomware es un tipo de software malicioso que cifra la información en diferentes dispositivos e impide a los usuarios acceder a su sistema o a sus archivos personales. Mediante este método, los ciberdelincuentes extorsionan a sus víctimas exigiendo una cantidad de dinero o pago de un rescate, a cambio de recuperar el acceso a sus datos. -MalwareMalware significa software malicioso. Siendo una de las ciber amenazas más comunes, el malware es un software que un ciberdelincuente o hacker ha creado para perturbar o dañar el ordenador de un usuario legítimo. El malware, que a menudo se propaga a través de un archivo adjunto a un correo electrónico no solicitado o de una descarga de aspecto legítimo, puede ser utilizado por los ciberdelincuentes para ganar dinero o en ciberataques por motivos políticos. Hay muchos tipos diferentes de malware, como Virus, Troyanos, Spyware, Ransomware, Adware, Botnets. -Antivirus Un antivirus es un programa que detecta malware, bloqueándolo, y eliminándolo para prevenir que se infecte el dispositivo. Existen diferentes tipos de antivirus, para elegir el más adecuado para ti o tu negocio, tienes que tener en cuenta las especificaciones el dispositivo a proteger y algunos criterios a considerar. Hay muchos antivirus disponibles, así que, a la hora de elegirlos, ten en cuenta estos criterios:• Compatibilidad con tu sistema operativo• Protección de tu dispositivo, sin ralentizar su velocidad, capacidad o rendimiento• Actualizaciones frecuentes. De lo contrario, podríamos estar expuestos a nuevas amenazas. • Versatilidad. Nuestro antivirus debe ser tan versátil como lo es el malware.• Capacidad de actuación. Además de reconocer la amenaza, debe erradicarla y limpiarla de nuestro dispositivo.-Antimalware¿Cuál es la diferencia entre antivirus y antimalware?Ambos se refieren a un software diseñado para detector, proteger y eliminar software malicioso. A pesar de lo que el nombre pueda sugerir, el software antivirus protege contra algo más que los virus; simplemente utiliza un nombre un poco anticuado para describir su función. El software antimalware también está diseñado para proteger contra los virus, solo que usa un nombre más moderno que engloba todo tipo de software malicioso, incluido los virus. Sabiendo esto, el antimalware puede prevenir la aparición de una infección viral, y eliminar los archivos infectados. Sin embargo, el antimalware no está necesariamente equipado para restaurar los archivos que un virus haya cambiado o sustituido. -Parches de seguridad. Vulnerabilidad Es una parte importante de la ciberseguridad en las empresas, ya que ayuda a evitar las brechas de vulnerabilidad en los sistemas de la empresa, mediante la actualización de todos sus equipos y dispositivos. Esto incluye las aplicaciones informáticas y los sistemas operativos, el firmware de los equipos electrónicos y el software antimalware. Los parches y las actualizaciones son creados por los propios desarrolladores del software y sirven para mejorar su rendimiento corrigiendo errores de seguridad y añadiendo nuevas funciones.- Proteger los datos de la empresa: Conceptos básicos de las copias de seguridad En pocas palabras, una copia de seguridad de datos no es más que una copia de los archivos de su ordenador o dispositivo. Y, como demuestran las numerosas amenazas descritas anteriormente, mantener una copia de seguridad de sus archivos y datos empresariales importantes es esencial por una serie de razones importantes.Cualquier copia de seguridad es mejor que ninguna, sin embargo, no todos los dispositivos y tecnologías de copia de seguridad son iguales ni ofrecen los mismos niveles de protección. Para una protección óptima, lo mejor es salvaguardar sus datos siguiendo la regla 3-2-1, que es la siguiente: • Mantén al menos tres (3) copias de sus datos (para que ningún imprevisto destruya todas las copias);• Almacena los datos en al menos dos (2) formatos diferentes (es decir, disco, pendrive, nube, por ejemplo.); • Guarda una (1) copia fuera de las instalaciones para protegerla contra incendios, inundaciones, robos y otros desastres físicos.-Protección de las redes inalámbricasEl uso de una red inalámbrica le ofrece la comodidad de poder trabajar y utilizar su ordenador prácticamente en cualquier lugar, y de conectarse a otros ordenadores de la red o acceder a Internet. Sin embargo, si su red inalámbrica no es segura, existen riesgos importantes. Por ejemplo, un ciberdelincuente podría interceptar cualquier dato que envíe o reciba, acceder a sus archivos compartidos, secuestrar su conexión a Internet y agotar su ancho de banda o límite de descarga.• Cuando compras un router Wi-Fi, tiene un nombre y una contraseña por defecto. Estos son muy fáciles de piratear, por lo que deberías cambiarlos. Además, el router tiene una contraseña de administrador que le permite cambiar y gestionar la configuración del router. Al igual que el nombre y la contraseña del router, también deberías cambiar esta contraseña.• Para proteger la información que envías a través de la red Wi-Fi, puedes encriptar tu red actualizando el software del router. Busca las configuraciones WPA3 o WPA2, que ofrecen el cifrado más fuerte.-Formación de los empleadosLos empleados pueden hacer que su empresa sea vulnerable a los ataques, o ayudar a prevenirlos. Numerosos estudios demuestran que gran parte de las pérdidas de datos provienen de los empleados internos que, en la mayoría de los casos por descuido o desinformación, dan a los ciberdelincuentes acceso a sus redes.Hay muchos escenarios que pueden dar lugar a ataques en los que las vías de acceso son los empleados. Por ejemplo, que un empleado pierda una tablet de trabajo, que facilite sus credenciales de acceso o que abra correos electrónicos fraudulentos, que desplieguen virus en la red.Para protegerse de las amenazas internas, es de vital importancia invertir en una formación de calidad en materia de ciberseguridad para los empleados que les proporcione las herramientas necesarias para actuar ante diversas situaciones y riesgos.-Políticas. Política de ciberseguridad. ¿Qué es una política de ciberseguridad?Para prevenir la ciberdelincuencia, es importante no sólo formar a sus empleados en materia de prevención de ciberdelitos, sino también crear una política de ciberseguridad de la empresa. Esto ayudará a definir claramente las directrices para la transferencia de datos de la empresa, el acceso a sistemas privados y el uso de dispositivos proporcionados por la empresa. Cuando prepare su política, asegúrese de que orienta a sus empleados sobre:• El tipo de información empresarial que se puede compartir y dónde• Uso apropiado de dispositivos y materiales online• Manejo y almacenamiento de material sensibleUn modelo completo de política de ciberseguridad incluirá las siguientes partes básicas: • Introducción• Objetivo• Alcance• Datos confidencialesSeguridad de los dispositivos:• Uso de la empresa• Uso personal• Seguridad del correo electrónico• Transferencia de datos• Acción disciplinaria2.2 Ciberseguridad a nivel de usuario/empleadoLa formación de los usuarios finales es importante porque aborda el factor más imprevisible de la ciberseguridad: las personas. Si no se siguen las buenas prácticas de seguridad, cualquiera puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñar a los usuarios a prestar atención a los factores de riesgo es fundamental para la seguridad de cualquier organización.-Protege los datos de tus dispositivosDatos personales y datos sensibles. ¿Son lo mismo?¿Qué son los datos personales?Los datos personales son cualquier pieza de información que alguien puede utilizar para identificar, con cierto grado de precisión, a una persona viva. Por ejemplo, la dirección de correo electrónico de un empleado de una empresa se considera un dato personal, porque indica que esa persona trabaja para la empresa. Una dirección física o un número de teléfono también son datos personales, porque esta información puede utilizarse para contactar con la persona. Cualquier cosa que pueda afirmar su presencia física en algún lugar también se considera un dato personal. Por ejemplo, las grabaciones de las cámaras de seguridad son datos personales, al igual que las huellas dactilares.Algunos ejemplos podrían ser:* Un nombre y un apellido
* La dirección de una casa
* Una dirección de correo electrónico
* Un número de documento de identidad
* Datos de localización
* Una dirección de protocolo de Internet (IP)
* El identificador publicitario de su teléfono

¿Qué son los datos personales sensibles?Los datos personales sensibles son un conjunto específico de "categorías especiales" que gozan de una mayor protección legal y deben ser tratados con una seguridad adicional, previa aprobación específica del sujeto al que se refieren esos datos. Esto incluye información relativa a:* Origen racial o étnico;
* Opiniones políticas;
* Creencias religiosas o filosóficas;
* La afiliación sindical;
* Datos genéticos; y
* Datos biométricos (cuando se traten para identificar a alguien de forma exclusiva).

Los datos personales sensibles deben almacenarse por separado de otros datos personales, preferiblemente en un cajón o archivador cerrado con llave. Al igual que los datos personales en general, solo deben guardarse en ordenadores portátiles o dispositivos de mano si el archivo ha sido encriptado y/o seudonimizado.-Seguridad física La ciberseguridad comienza con una fuerte seguridad física. Esto incluye almacenar los documentos de forma segura, guardarlos bajo llave en una habitación o armario, limitar el acceso físico a los datos sensibles, eliminar la información correctamente y destruir los documentos de datos sensibles cuando ya no se necesiten. Permita el acceso a la información personal y financiera sólo al personal que realmente la necesite. • Recuerde a sus empleados que nunca deben dejar documentos de datos sensibles sin vigilancia en el lugar de trabajo o en lugares públicos. Los fallos en la seguridad física pueden exponer los datos sensibles de la empresa al robo de identidad, con consecuencias potencialmente graves. Todo puede ocurrir debido a fallos de seguridad física, como la pérdida de un ordenador portátil, el robo de un teléfono móvil o el extravío de un pendrive. Por ello, es menos probable que se produzca una violación de datos si la información de esos dispositivos está protegida. A continuación, algunos ejemplos útiles:* Exija contraseñas complejas: Exija contraseñas largas, complejas y únicas. Y asegúrese de que estas contraseñas se almacenan de forma segura. Considere la posibilidad de utilizar un gestor de contraseñas.
* Utilice la autenticación multifactorial: Exija una autenticación multifactorial para acceder a las áreas de su red con información sensible. Esto requiere pasos adicionales más allá del inicio de sesión con una contraseña, como un código temporal en un smartphone.
* Limite los intentos de inicio de sesión: Limite el número de intentos de inicio de sesión incorrectos permitidos para desbloquear los dispositivos. Esto le ayudará a protegerse de los intrusos.
* Cifrar: Cifre los dispositivos portátiles, incluidos los ordenadores portátiles y las memorias USB, que contengan información sensible. Cifre cualquier dato sensible que envíe fuera de la empresa, como por ejemplo a un contable o a un abogado.

-Seguridad del correo electrónicoEn el caso de que el usuario/empleado utilice dispositivos personales para acceder a los sistemas de la empresa, o para uso personal, se deben tomar ciertas medidas de seguridad en cuanto al uso del correo electrónico, ya que también puede ser una puerta de entrada para acciones delictivas. En el caso de que los empleados deban utilizar sus dispositivos personales para acceder a los sistemas de la empresa, los empleados deben informar a la dirección con el fin de realizar un registro. Para garantizar la protección de los sistemas de la empresa, todos los empleados deben:* Asegurarse de que todos los dispositivos personales utilizados para acceder a los sistemas de la empresa estén protegidos por una contraseña (de 8 caracteres como mínimo).
* Instalar un software antivirus completo.
* Actualizar periódicamente el software antivirus.
* Bloquear todos los dispositivos si se dejan desatendidos.
* Asegurarse de que todos los dispositivos estén protegidos en todo momento.
* Utilizar siempre redes seguras y privadas.

La protección de los sistemas de correo electrónico es una gran prioridad, ya que los correos electrónicos pueden dar lugar a robos de datos, estafas y ser portadores de programas maliciosos como gusanos y virus. Por ello, se aconseja a los usuarios/empleados que:* Verificar la legitimidad de cada correo electrónico, incluyendo la dirección de correo electrónico y el nombre del remitente.
* Evitar abrir correos electrónicos y archivos adjuntos sospechosos y hacer clic en los enlaces.
* Buscar errores gramaticales significativos.
* Evite títulos y enlaces que inciten a hacer clic.
* Póngase en contacto con el departamento de TI en relación con cualquier correo electrónico sospechoso

PhishingTambién conocido como fraude electrónico. Conocer un poco más sobre los fraudes más comunes y peligrosos nos ayudará a evitar caer en ellos.A través de estos métodos, 'phishing' y 'smishing', el atacante busca obtener información privada como contraseñas o tarjetas de crédito. En este ataque, se pide a la víctima datos vulnerables, como contraseñas o claves de acceso, por correo electrónico, haciéndose pasar por la web o entidad legítima, para que la víctima facilite los datos solicitados por el atacante. SmishingEsta amenaza es similar al phishing, la única diferencia es que se envía por SMS a los teléfonos. El hacker envía un mensaje a nuestros teléfonos, abrir el mensaje no es peligroso. El peligro radica en hacer clic en el enlace, es entonces cuando comienza el ataque.2. 3 Ciber riesgos más comunes a tener en cuenta. La guía básica de CiberseguridadDespués de familiarizarnos con los conceptos mencionados anteriormente, veamos los riesgos más frecuentes a los que se enfrentan las pymes, según estudios basados en la encuesta de la Agencia de Ciberseguridad de la Unión Europea (ENISA), encabezando la lista el phishing y los ataques basados en la web.1) Ataques de phishing Este tipo de ataque se ha vuelto extremadamente popular debido al trabajo a distancia. Un clic descuidado en un enlace es todo lo que necesita un ciberdelincuente para acceder a información empresarial sensible.2) Ataques basados en la webLos ciberdelincuentes utilizarán casi cualquier vulnerabilidad -dentro de un sistema operativo (OS) o de una aplicación- para llevar a cabo un ataque. Sin embargo, la mayoría de los ciberdelincuentes desarrollan amenazas web que se dirigen deliberadamente a algunos de los sistemas operativos y aplicaciones más comunes3) Ataques generales de malware Muchas PYMES subestiman la posibilidad de sufrir ciberataques debido a su tamaño. Sin embargo, esto es precisamente lo que buscan los piratas informáticos, ya que pueden beneficiarse rápidamente de una amenaza de ransomware a las PYMES menos seguras.4) Agentes internos maliciosos Este tipo de amenaza se refiere a la existencia de personas dentro de una organización (ya sean empleados internos o proveedores externos, entre otros) que, por descuido, ignorancia y/o mala fe, realizan una "acción" que afecta a la seguridad de los procesos, sistemas o instalaciones de un entorno operativo industrial o de una infraestructura crítica.5) Ataques de denegación de servicio El objetivo de estos ataques es interrumpir el sitio web de una empresa para que sea inaccesible, lo que el ciberdelincuente hace por diversos motivos. Un sitio web detenido puede provocar la pérdida de ingresos, la violación de datos, la desconfianza de los clientes y la paralización de la actividad de la empresa.La guía básica de Ciberseguridad1. Determina tus vulnerabilidadesLo primero que debes hacer es identificar tus vulnerabilidades, para saber qué datos debes proteger. Hazte preguntas como: ¿Cuáles son los datos más importantes que almacena mi empresa? ¿Dónde almacena estos datos? Una vez que tengas las respuestas, podrás empezar a evaluar los riesgos.2. Protege tus dispositivosLos dispositivos de trabajo son cruciales para el funcionamiento de tu empresa. Su conexión a Internet los hace vulnerables a los ciberataques. He aquí algunos consejos para protegerlosA. Actualiza tu softwareB. Protégete de los virusC. Configurar un Firewall D. Precauciones especiales para portátiles y otros dispositivos móviles3. Protege tus datosIndependientemente del tipo de negocio que tenga, los datos son una parte esencial del mismo. Los datos pueden dañarse de mil maneras diferentes, una de las cuales es a través de los ciberataques. Aquí tienes algunos consejos útiles sobre cómo proteger tus datos.A. Implementa un procedimiento para hacer copias de seguridad de los datos críticosB. Encripta la información confidencial de la empresa que almacenes en la nubeC. Proteger las contraseñasD. Establecer permisos E. Proteger tus redes inalámbricasF. Navegar por Internet de forma seguraG. Proteger la información confidencial creada por los trabajadores remotosH. Proteja los datos de sus clientes4. Instaura la ciberseguridad en el lugar de trabajoLas medidas de seguridad mencionadas en esta guía básica pueden ayudarle a reducir significativamente el riesgo de un ciberataque. Pero esto no servirá de nada si los empleados de tu empresa no tienen la concienciación y formación necesarias para poder contribuir a la prevención de los mismos. Incluya este tipo de formación en su empresa y no olvide crear una política de ciberseguridad de la empresa que todos los miembros del equipo puedan seguir. |
| **Índice de contenidos** |
| 2. Ciberseguridad y herramientas digitales para las PYMES. Prepárate para prevenir y solventar Ciberataques.2.1 Seguridad a nivel empresarial2.2 Ciberseguridad a nivel de usuario/empleado2.3 Ciber riesgos más comunes a tener en cuenta. La guía básica de Ciberseguridad |
| **Glosario** |
| **Ciberseguridad:** Es un conjunto de prácticas para defender los sistemas informáticos y el software de la ciberdelincuencia. La ciberseguridad abarca muchos ámbitos: seguridad de la red, seguridad de las aplicaciones, seguridad de la información, seguridad de los usuarios, etc.**Ciberdelincuencia:** Es toda actividad delictiva que se desarrolla en el mundo digital, en la que interviene un ordenador, un dispositivo conectado a la red o una red, y que tiene por objeto conseguir un determinado propósito o beneficio, que puede ser de distinta índole. **5** **Ransomware:** Es un tipo de software malicioso que encripta la información en diferentes dispositivos. Mediante este método, los ciberdelincuentes extorsionan a sus víctimas exigiendo un rescate a cambio de recuperar el acceso a sus datos. **Malware:** significa software malicioso. El malware, una de las ciber amenazas más comunes, es un software que un ciberdelincuente o un hacker ha creado para perturbar o dañar el ordenador de un usuario legítimo. Hay muchos tipos diferentes de malware, como: Virus, Troyanos, Spyware, Ransomware, Adware, Botnets. **Backup:** Copia de seguridad. Sencillamente, una copia de seguridad de datos no es más que una copia de los archivos de su ordenador o dispositivo. Y, como demuestran las numerosas amenazas descritas anteriormente, mantener una copia de seguridad de los archivos y datos importantes de su empresa es esencial por una serie de razones importantes.**5**  |
| **Bibliografía y otras referencias** |
| <https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-europes-smes><https://www.kaspersky.com/resource-center/preemptive-safety/protecting-wireless-networks><https://www.pandasecurity.com/es/mediacenter/seguridad/parches-brechas-datos/><https://searchsecurity.techtarget.com/definition/cybercrime><https://es.malwarebytes.com/antivirus/><https://ciberseguridad.com/normativa/espana/medidas/actualizaciones/><https://www.betterteam.com/cyber-security-policy><https://business.gov.au/online/cyber-security/create-a-cyber-security-policy><https://www.daemon4.com/empresa/noticias/las-principales-amenazas-de-ciberseguridad-para-pymes/><https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data><https://www.bbva.com/es/phishing-y-smishing-que-son-y-como-evitarlos/><https://www.acronis.com/en-us/articles/data-backup-for-business/> <https://www.ciberseguridadlogitek.com/la-amenaza-del-malicious-insider-en-los-entornos-de-operacion-industrial-y-de-infraestructuras-criticas/><https://usa.kaspersky.com/resource-center/threats/web><https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/><https://es.vpnmentor.com/blog/la-guia-completa-de-ciberseguridad-para-pequenas-y-medianas-empresas/><https://www.ncsc.gov.uk/collection/small-business-guide><https://insights.ascentor.co.uk/blog/2019/11/12-practical-cyber-security-tips-for-smes> <https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf><https://www.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security><https://ciberseguridadbidaidea.com/ciberseguridad/6-principales-amenazas-de-una-empresa-en-ciberseguridad/><https://www.widefense.com/recursos/ciberseguridad/pequenas-empresas/><https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security><https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices><https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware><https://internetpasoapaso.com/antimalware/><https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited><https://me-en.kaspersky.com/blog/how-to-set-up-wifi-router/4390/><https://blog.walkme.com/5-employee-training-fails/><https://almamate.in/importance-of-selecting-the-best-salesforce-institute-in-noida/><https://cmitsolutions.com/blog/6-ways-protect-data-devices-digital-identity/><http://www.rbntechnologies.com/products.html><https://memoori.com/physicalsecurity-2016-rounded_v1/><https://www.djcs.com.ve/djcsnews/1901-automationedge-password-reset><https://www.datacenterknowledge.com/security/managing-encryption-data-centers-hard-and-it-will-get-harder><https://nakedsecurity.sophos.com/es/2016/08/09/email-how-secure-is-yours-survey/><https://www.valoradata.com/blog/que-es-el-phishing/><https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/><https://www.keepnetlabs.com/7-ways-to-prevent-phishing-attacks-in-2021/><https://www.teceze.com/what-is-vmdr-vulnerability-management><https://cypheradda.blogspot.com/2019/05/5-cybersecurity-tips-for-workplace.html><https://molinaoposiciones.com/2021/03/22/por-fin-fecha-definitiva-de-auxilio/><https://unaaldia.hispasec.com/2021/04/malware-en-plantillas-empresariales-de-descarga-gratuita.html> |
| **Preguntas de autoevaluación de opción múltiple** |
| 1. ¿Qué son los datos personales?**a) Los datos personales son cualquier pieza de información que alguien puede utilizar para identificar, con cierto grado de precisión, a una persona viva. Por ejemplo, la dirección de correo electrónico de un empleado de una empresa se considera un dato personal, porque indica que esa persona trabaja para la empresa.**b) Los datos personales son un conjunto específico de "categorías especiales" que gozan de una mayor protección legal, y deben ser tratados con una seguridad adicional, previa aprobación específica del sujeto al que se refieren esos datos. 2. Seleccione la respuesta correcta relacionada con el concepto de Parches de Seguridad.**a) Es una parte importante de la ciberseguridad en las empresas, ya que ayuda a evitar brechas de vulnerabilidad en los sistemas de la empresa, mediante la actualización de todos sus equipos y dispositivos. Esto incluye las aplicaciones informáticas y los sistemas operativos, el firmware de los equipos electrónicos y el software antimalware.** b) Es una parte importante de la ciberseguridad que incluye el almacenamiento de documentos de forma segura, guardándolos bajo llave en una habitación o armario, limitando el acceso físico a los datos sensibles, eliminando la información correctamente y destruyendo los documentos de datos sensibles cuando ya no son necesarios. 3. En cuanto a la ciberseguridad a nivel de usuario/empleado, ¿por qué es importante una formación para el usuario final? a) No es tan importante, ya que el usuario final es el único afectado por la ciberdelincuencia y no tiene más remedio que instalar un buen antivirus. b) **La formación del usuario final es importante porque aborda el factor de ciberseguridad más imprevisible: las personas.** 4. ¿Cuál es la diferencia entre antivirus y antimalware?a) **Ambos se refieren a un software diseñado para detectar, proteger y eliminar el software malicioso.** b) Sólo un antimalware puede detectar software malicioso, un antivirus está diseñado específicamente para eliminar la amenaza del ordenador. 5. Seleccione la opción correcta sobre la protección de las redes inalámbricas.**a) Si su red inalámbrica no es segura, existen riesgos importantes. Por ejemplo, un ciberdelincuente podría interceptar cualquier dato que envíe o reciba, acceder a sus archivos compartidos, secuestrar su conexión a Internet y agotar su ancho de banda o límite de descarga.****b) Cuando compras un router Wi-Fi, tiene un nombre y una contraseña por defecto. Estos son muy fáciles de piratear, por lo que deberías cambiarlos. Además, el router tiene una contraseña de administrador que le permite cambiar y gestionar la configuración del router, también debería cambiar esta contraseña.** |
| **Material relacionado** |  |
| **PPT relacionado** | SWIFTSME\_Curso 2\_ Ciberseguridad y herramientas digitales para las PYMES\_ES |
| **Link de referencia** |  |
| **Vídeo en formato YouTube (si lo hay)** |  |