Ficha de formación

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Título | Mantén tus datos seguros: Ciberseguridad para las MIPYME | | | |
| Keywords | Seguridad de datos, Ciberseguridad, Protección de datos, Seguridad de la información, Ciberamenazas, Infracciones de datos, Seguridad de la red, Gestión de riesgos, Mejores prácticas de seguridad, Concienciación cibernética | | | |
| Proporcionado por | IT Solutions for All | | | |
| Idioma | Español | | | |
| Área de formación | Fundamentos del emprendimiento digital en entornos de microempresas  Comunicación digital y branding  Finanzas digitales  Ciberseguridad | | | |
| Resultados del aprendizaje | EntreComp | | | |
| Ideas y oportunidades  Recursos  En acción  Competencias específicas abordadas:  Movilización de recursos, movilización de otros, planificación y gestión, hacer frente a la incertidumbre, ambigüedad y riesgo, aprendizaje a través de la experiencia | | | |
| DigComp | | | |
| Alfabetización en información y datos  Comunicación y colaboración  Creación de contenido digital  Seguridad  Resolución de problemas  Competencias específicas abordadas:  Proteger los dispositivos, proteger los datos personales y la privacidad, identificar las necesidades y las respuestas tecnológicas | | | |
| Nivel de competencia | | | |
| Nivel 1  Nivel 2 | Nivel 3  Nivel 4 | Nivel 5  Nivel 6 | Nivel 7  Nivel 8 |
| Fundacional | Intermedio | Avanzado | Experto |
| Descripción | En la era digital actual, los datos son un activo valioso para todas las organizaciones, incluidas las micro, pequeñas y medianas empresas (MIPYME). Sin embargo, con la creciente dependencia de la tecnología, el riesgo de amenazas cibernéticas y violaciones de datos nunca ha sido mayor.  Nuestro curso de formación, "Mantén tus datos seguros: Ciberseguridad para las MIPYME", está diseñado específicamente para empoderar a los propietarios, gerentes y empleados de las MIPYME con los conocimientos y habilidades necesarios para proteger sus valiosos datos e información confidencial. | | | |
| Objetivos de aprendizaje | * Obtener una comprensión completa de las amenazas a la ciberseguridad y las medidas necesarias para proteger a las MIPYME. * Estar equipado con los conocimientos y habilidades para establecer una infraestructura segura de TI. * Poder gestionar la seguridad de la información y responder eficazmente a incidentes de ciberseguridad. | | | |
| Índice (3 niveles: Módulo-Unidad-Sección) | Módulo: Mantén tus datos seguros: Ciberseguridad para las MIPYME  **Unidad 1**: Introducción a la ciberseguridad para las MIPYME  Sección 1.1. Comprensión de la ciberseguridad: definición e importancia de las políticas de seguridad  Sección 1.2. Amenazas comunes de ciberseguridad a las que se enfrentan las MIPYME  **Unidad 2**: Establecimiento de una infraestructura de TIC segura  Sección 2.1. Evaluación de vulnerabilidades de ciberseguridad  Sección 2.2. Uso efectivo de soluciones antivirus y antimalware  **Unidad 3**: Gestión de la seguridad de la información  Sección 3.1. Prácticas y directrices | | | |
| Contenido desarrollado | Módulo: Mantén tus datos seguros: Ciberseguridad para las MIPYME  Unidad 1: Introducción a la ciberseguridad para las MIPYME  **Sección 1.1.** Comprensión de la ciberseguridad: definición e importancia de las políticas de seguridad  Una política de seguridad para micro, pequeñas y medianas empresas (MIPYME) es un documento formal que describe el enfoque de la organización para la seguridad de la información. Establece las reglas, directrices y responsabilidades para proteger los activos, datos y sistemas de la compañía de posibles amenazas y accesos no autorizados. La política debe ser completa, clara y adaptada a las necesidades y riesgos específicos a los que se enfrentan las pymes. Comprender la ciberseguridad y la importancia de las políticas de seguridad para las microempresas y las pequeñas y medianas empresas después de la COVID es crucial por varias razones:  **Conciencia de las amenazas cibernéticas**: La comprensión de la ciberseguridad permite **a las personas ser conscientes de las diversas amenazas y riesgos cibernéticos que existen en el panorama digital.** **Les ayuda a reconocer posibles vulnerabilidades** y debilidades en sus sistemas, redes y prácticas.  **Protección de datos sensibles**: Las medidas de ciberseguridad protegen los datos sensibles y confidenciales del acceso no autorizado, el robo o el uso indebido. Esto es especialmente **vital para las MIPYMES, ya que a menudo manejan información valiosa de clientes,** datos financieros y propiedad intelectual.  **Prevención de violaciones de datos**: Las políticas de seguridad desempeñan un papel importante en la prevención de violaciones de datos y ciberataques. Describen **procedimientos y directrices para garantizar que los datos se manejen de forma segura** y que se minimicen los posibles puntos de entrada para los atacantes.  **Mantenimiento de la continuidad del negocio**: La ciberseguridad es esencial para el **buen funcionamiento de una MIPYME**. Las políticas de seguridad **ayudan a identificar posibles riesgos** que podrían interrumpir las operaciones comerciales y ayudan a desarrollar estrategias para mantener la continuidad frente a los incidentes cibernéticos.  **Cumplimiento y Requisitos Legales**: Muchas industrias tienen regulaciones y requisitos legales específicos en materia de protección de datos y ciberseguridad. **Comprender la ciberseguridad ayuda a las MIPYMES a cumplir con estas regulaciones, evitar sanciones** y mantener la confianza de los clientes y socios.  **Construyendo la confianza del cliente**: Demostrar un compromiso con la ciberseguridad y contar con políticas de seguridad sólidas **puede mejorar la confianza de los clientes en una MIPYME**. Los clientes son más propensos a hacer negocios con organizaciones que priorizan la protección de sus datos y privacidad.  **Prevención de pérdidas financieras: Los ciberataques pueden resultar en pérdidas financieras significativas para las MIPYME**. Comprender la ciberseguridad e implementar políticas de seguridad efectivas **puede ayudar a mitigar los riesgos financieros asociados con violaciones de datos y otros incidentes cibernéticos**.  **Gestión de la reputación**: Un ataque cibernético exitoso puede **dañar la reputación de una MIPYME**, lo que lleva a **una pérdida de clientes y oportunidades**. Las políticas de seguridad ayudan a prevenir incidentes y demuestran la dedicación de la organización a salvaguardar la información.  **Preparación para la crisis**: Las políticas de sensibilización y seguridad en materia de ciberseguridad ayudan a las MIPYMES a **estar preparadas para posibles crisis** que reduzcan el tiempo de recuperación.  **Formación y sensibilización de los empleados**: La comprensión de la ciberseguridad permite a las organizaciones proporcionar capacitación adecuada a sus empleados. **Educar al personal** sobre las mejores prácticas, las amenazas potenciales y las políticas de seguridad **ayuda a crear una cultura de seguridad sólida** dentro de la organización.  **Ventaja competitiva**: Enfatizar la ciberseguridad y tener políticas de seguridad efectivas puede **proporcionar a una MIPYME una ventaja competitiva**. **Los clientes y socios a menudo priorizan la seguridad** al elegir socios comerciales, haciendo de la ciberseguridad un diferenciador valioso.  En conclusión, comprender la ciberseguridad y la importancia de las políticas de seguridad es fundamental para que las MIPYME protejan sus datos, mantengan la continuidad del negocio, cumplan con las regulaciones y generen confianza con los clientes y las partes interesadas. Al abordar proactivamente las ciberamenazas, las MIPYME pueden reforzar su resiliencia y garantizar un entorno digital seguro para sus operaciones.  **Sección 1.2.** Amenazas comunes de ciberseguridad a las que se enfrentan las MIPYMES  Las micro, pequeñas y medianas empresas (MIPYME) se están convirtiendo cada vez más en objetivos para los ciberdelincuentes debido a sus valiosos datos y sus defensas de ciberseguridad potencialmente más débiles en comparación con las organizaciones más grandes. Algunas amenazas comunes de ciberseguridad a las que se enfrentan las MIPYME incluyen:  **Ataques de phishing**: El phishing es una técnica en la que los ciberdelincuentes envían correos electrónicos, mensajes o sitios web engañosos para engañar a los empleados para que divulguen información confidencial como credenciales de inicio de sesión, datos financieros o información personal.  **Ransomware**: Ransomware es un tipo de malware que cifra los datos de una organización, haciéndolos inaccesibles hasta que se paga un rescate. Las MIPYME pueden ser objeto de ataques debido a la percepción de que las medidas de seguridad son más débiles.  **Infecciones de malware**: Las MIPYME son susceptibles a varios tipos de malware, incluyendo virus, troyanos y spyware. Estos programas maliciosos pueden interrumpir las operaciones, robar datos u obtener acceso no autorizado a los sistemas.  **Amenazas internas**: Las amenazas internas implican acciones maliciosas o errores no intencionales cometidos por empleados o individuos con acceso a los sistemas, datos o redes de una organización.  **Ataques de ingeniería social**: La ingeniería social implica manipular a las personas para que revelen información confidencial, como contraseñas o credenciales de inicio de sesión. Esto podría ocurrir a través de llamadas telefónicas, interacciones en persona o redes sociales.  **Dispositivos IoT no seguros**: Muchas MIPYME utilizan dispositivos de Internet de las Cosas (IoT), como cámaras inteligentes o sensores. Si no están correctamente protegidos, estos dispositivos pueden convertirse en puntos de entrada para que los atacantes se infiltren en la red.  **Contraseñas débiles y autenticación**: Las prácticas inadecuadas de contraseñas, como usar contraseñas fácilmente adivinables o reutilizarlas en varias cuentas, pueden hacer que las MIPYME sean vulnerables a ataques de fuerza bruta o relleno de credenciales.  **Violaciones de datos**: Las MIPYMES a menudo recopilan y almacenan datos valiosos de clientes. Si no se protege adecuadamente, una violación de datos podría conducir a daños a la reputación, pérdidas financieras y consecuencias legales.  **Ataques de denegación de servicio (DoS):** Los ataques DoS (Denial of Service) abruman los sistemas o la red de una organización con una avalancha de tráfico, causando interrupciones y tiempo de inactividad.  **Falta de actualizaciones y parches de software regulares**: No aplicar actualizaciones oportunas y parches de seguridad al software y a los sistemas operativos puede dejar a las MIPYME expuestas a vulnerabilidades conocidas.  **Preocupaciones de seguridad en la nube**: Almacenar datos y aplicaciones en la nube puede ser conveniente para las MIPYMES, pero también puede introducir riesgos de seguridad si no se configuran y administran adecuadamente.  **Ataques a la cadena de suministro**: Los ciberdelincuentes pueden dirigirse a las MIPYME como un medio para obtener acceso a organizaciones más grandes mediante la explotación de vulnerabilidades en la cadena de suministro.  **Ajustes de seguridad mal configurados**: Los ajustes de seguridad configurados incorrectamente en sistemas, aplicaciones o dispositivos de red pueden crear brechas de seguridad no intencionales.  **Falta de conciencia de seguridad cibernética de los** **empleados**: La insuficiente concienciación y capacitación en ciberseguridad entre los empleados puede aumentar la probabilidad de ser víctima de diversas amenazas cibernéticas.  Para mitigar estas amenazas, las MIPYME deben invertir en medidas de ciberseguridad, como la formación periódica de los empleados, controles de acceso sólidos, métodos de autenticación sólidos, infraestructura de TIC segura, gestión de la seguridad de la información, software de seguridad actualizado y un plan de respuesta a incidentes bien definido. Las prácticas proactivas de ciberseguridad pueden reducir significativamente el riesgo de ser víctimas de ataques cibernéticos y proteger los valiosos activos y la reputación de la organización.  Unidad 2: Establecimiento de una infraestructura de TIC segura  **Sección 2.1.** Evaluación de vulnerabilidades de ciberseguridad  Evaluar las vulnerabilidades de ciberseguridad es esencial para que las MIPYME identifiquen posibles debilidades en sus sistemas, infraestructuras de TIC, redes y prácticas. Estos son los pasos que una MIPYME puede tomar para evaluar sus vulnerabilidades de ciberseguridad:  **Identificar activos y datos**: Comienza por identificar todos los activos, la infraestructura de TIC, los sistemas, dispositivos y datos que utiliza o almacena sus MIPYME. Esto incluye hardware, software, servidores, dispositivos de red, servicios en la nube e información confidencial.  **Llevar a cabo una evaluación de riesgos**: Realiza una evaluación integral de riesgos para identificar posibles amenazas, vulnerabilidades y el impacto potencial de un incidente cibernético en tu organización. Esta evaluación ayudará a priorizar los esfuerzos para abordar primero los riesgos más críticos.  **Pruebas de penetración**: Considera realizar pruebas de penetración (hacking ético) para simular ataques cibernéticos del mundo real en sus sistemas y redes. Esto ayuda a identificar posibles puntos de entrada y áreas débiles en sus defensas de seguridad.  **Revisión de la seguridad de la red**: Evalúa la seguridad de tu infraestructura de red, incluidos firewalls, routers, switches y redes inalámbricas. Asegúrate de que estos dispositivos estén configurados adecuadamente y de que los controles de acceso estén en su lugar.  **Evaluar software y aplicaciones**: Comprueba regularmente si hay actualizaciones de seguridad y parches para todo el software y las aplicaciones utilizadas en tu organización. El software obsoleto puede crear vulnerabilidades que los atacantes cibernéticos pueden explotar.  **Evaluar Endpoint Security**: Evaluar las medidas de seguridad en los dispositivos de punto final (por ejemplo, ordenadores portátiles, teléfonos inteligentes, tabletas) utilizados por los empleados. Implementa software antivirus, cifrado y aplica políticas para acceder a los datos de la empresa en dispositivos personales.  **Verifica la seguridad física**: No pases por alto la seguridad física. Evalúa los controles de acceso físico a las instalaciones de tu oficina, salas de servidores y áreas sensibles donde se almacenan datos y equipos.  **Examina la conciencia de los empleados**: Evalúa el nivel de conciencia de ciberseguridad entre tus empleados. Llevar a cabo capacitación y talleres para educarlos sobre las amenazas cibernéticas comunes y las mejores prácticas para la seguridad de los datos.  **Revisar las políticas de contraseña**: Asegúrate de que existen políticas de contraseñas seguras, que incluyen la necesidad de contraseñas complejas, cambios regulares de contraseñas y no reutilizar contraseñas en varias cuentas.  **Servicios seguros en** **la nube**: Si utilizas servicios en la nube, evalúa sus características de seguridad y asegúrate de que cumplan con los requisitos de tu organización. Implementa autenticación y cifrado multifactor para datos confidenciales almacenados en la nube.  **Analizar las políticas de seguridad**: Revisa y actualiza las políticas de seguridad regularmente. Asegúrate de que se alinean con los estándares de la industria y los requisitos de cumplimiento. Estas políticas deben cubrir áreas como la protección de datos, los controles de acceso, la respuesta a incidentes y el uso aceptable.  **Auditar a los proveedores de terceros**: Si trabajas con proveedores externos o proveedores de servicios, evalúa sus prácticas de ciberseguridad y medidas de protección de datos para asegurarte de que no introduzcan riesgos adicionales.  **Preparación para respuesta a incidentes**: Evalúa el plan de respuesta a incidentes de tu organización para asegurarte de que es integral y cubre los pasos apropiados a tomar en caso de un incidente cibernético.  **Auditorías periódicas de seguridad**: Realiza auditorías y evaluaciones periódicas de seguridad para mantener una comprensión continua de la postura de ciberseguridad de tu organización.  **Garantizar la seguridad de la red wi-fi:** Proteger las redes Wi-Fi es crucial para prevenir el acceso no autorizado y proteger los datos confidenciales.  Se puede lograr mediante:   * cambio de credenciales predeterminadas * uso de cifrado fuerte * habilitar el acceso protegido Wi-Fi 3 (WPA3) o WPA2 con AES (estándar de cifrado avanzado) para un cifrado sólido * evitar el uso de métodos de cifrado obsoletos y vulnerables como WEP (privacidad equivalente por cable) * modificación del identificador predeterminado del conjunto de servicios (SSID) a un nombre único que no revela información sobre su empresa u organización * desactivar la transmisión de SSID para hacer que tu red sea menos visible para los atacantes potenciales * configurar una red de invitados separada para visitantes o clientes que los aísle de tu red interna principal, utilizando contraseñas seguras * habilitar el filtrado de direcciones mac para permitir que solo dispositivos específicos con direcciones mac preaprobadas se conecten a tu red wi-fi * mantener actualizado el firmware * deshabilitar la administración remota en el router para evitar el acceso no autorizado desde fuera de la red * habilitar firewall y cifrado de red * deshabilitar el plug and play universal (UPNP) en tu router, ya que puede ser explotado por los atacantes para abrir puertos y exponer la red a amenazas potenciales. * seguimiento de la actividad de la red * asegurar el acceso físico * educar a los empleados.   **Sección 2.2.** Uso efectivo de soluciones antivirus y antimalware:  El uso efectivo de soluciones antivirus y antimalware es fundamental para que las micro, pequeñas y medianas empresas (MIPYME) protejan su infraestructura, sistemas, redes y datos de TIC de diversas amenazas cibernéticas.  Estas son algunas de las mejores prácticas para usar soluciones antivirus y antimalware de manera efectiva:  **Elige una solución integral**: Selecciona un software antivirus y antimalware de buena reputación y completo que ofrezca protección en tiempo real, actualizaciones regulares y análisis frecuentes para detectar y eliminar software malicioso.  **Mantén actualizado el software**: Asegúrate de que el antivirus y el software antimalware estén actualizados con las últimas definiciones de virus y actualizaciones de bases de datos. Esto es esencial para detectar y proteger contra amenazas nuevas y emergentes.  **Habilitar el escaneo en tiempo real**: Activa las funciones de escaneo en tiempo real del software antivirus para verificar automáticamente los archivos, descargas y archivos adjuntos de correo electrónico en busca de malware a medida que se accede a ellos.  **Programa los escaneos regulares**: Configura los escaneos programados para que se ejecuten en momentos convenientes en los que es menos probable que el sistema esté en uso intensivo, como fuera del horario comercial.  **Habilitar actualizaciones automáticas**: Habilitar actualizaciones automáticas tanto para el software antivirus como para el sistema operativo para garantizar una protección continua contra las últimas amenazas.  **Realiza escaneos completos del sistema**: Realiza análisis completos del sistema periódicamente para verificar a fondo todos los archivos, incluidos los que se encuentran en áreas con menos acceso.  **Cuarentena y amenazas aisladas**: Configurar el software antivirus para poner en cuarentena o aislar las amenazas detectadas, evitando que se propaguen o causen daños adicionales.  **Escanear dispositivos externos**: Escanea todos los dispositivos externos, como unidades USB o discos duros externos, antes de acceder a los archivos para evitar que se introduzca malware en la red.  **Educar a los empleados**: Educar a los empleados sobre la importancia de la protección antivirus y antimalware y capacitarlos para que sean cautelosos con los archivos adjuntos de correo electrónico, descargas y enlaces para evitar la introducción inadvertida de malware.  **Implementa Endpoint Protection**: Considera el uso de soluciones de protección de puntos finales que proporcionan una defensa multicapa contra varios tipos de amenazas, incluyendo ransomware y exploits de día cero.  **Gestión centralizada**: Si administras varios sistemas, utiliza herramientas de administración centralizadas para monitorear y controlar el software antivirus y antimalware en todos los dispositivos desde una sola interfaz.  **Mantenimiento regular del sistema:** Realiza regularmente tareas de mantenimiento del sistema, como la limpieza y desfragmentación del disco, para optimizar el rendimiento del sistema y mejorar la eficacia de los análisis antivirus.  **Monitorea y responde a las alertas**: Configura el software antivirus para enviar alertas de amenazas detectadas, y responde e investiga rápidamente cualquier alerta para tomar las medidas adecuadas.  **Evaluaciones periódicas de seguridad**: Realizar evaluaciones y auditorías periódicas de seguridad para evaluar la eficacia de las soluciones antivirus y antimalware e identificar áreas de mejora.  **Estrategias de copia de seguridad y recuperación de datos:** Implementa una estrategia regular de copia de seguridad de datos para garantizar que los archivos importantes estén seguros en caso de una infección grave de malware o un ataque de ransomware. Establece un programa de copia de seguridad rutinaria para garantizar que los datos críticos se respalden regularmente. Dependiendo del volumen de datos y la frecuencia de los cambios, las copias de seguridad diarias, semanales o mensuales pueden ser apropiadas. Además, las MIPYME pueden utilizar soluciones de copia de seguridad automatizadas para reducir el riesgo de error humano y garantizar que las copias de seguridad se realicen de manera consistente sin intervención manual. No olvides almacenar datos de copia de seguridad en múltiples ubicaciones físicas para mitigar el riesgo de pérdida de datos debido a robos, incendios u otros desastres que afecten a una sola ubicación. Considere las copias de seguridad basadas en la nube, además de las copias de seguridad en el sitio, como una solución rentable y confiable. Las copias de seguridad en la nube proporcionan fácil escalabilidad, accesibilidad y redundancia de datos.  Recuerda que la ciberseguridad es un proceso continuo. Las evaluaciones periódicas, el monitoreo continuo y las acciones rápidas para abordar las vulnerabilidades son esenciales para mantener a las MIPYME protegidas de las amenazas cibernéticas en evolución.  Unidad 3: Gestión de la seguridad de la información  **Sección 3.1.** Prácticas y directrices  La gestión de la seguridad de la información es crucial para las micro, pequeñas y medianas empresas (MIPYME) para **proteger sus datos confidenciales**, **mantener la confianza de los clientes** y **salvaguardar sus operaciones comerciales**.  Estas son algunas pautas y prácticas clave que las MIPYMES pueden seguir para administrar eficazmente la seguridad de la información:  **Evaluación de riesgos**: Llevar a cabo una evaluación de riesgos exhaustiva para identificar posibles vulnerabilidades y amenazas a la seguridad de la información. Comprender los tipos de datos que maneja la organización, los riesgos asociados con cada tipo y el impacto de una violación de seguridad.  **Políticas y procedimientos de seguridad**: Desarrollar e implementar políticas y procedimientos integrales de seguridad de la información que cubran áreas como el manejo de datos, controles de acceso, administración de contraseñas, copia de seguridad de datos y respuesta a incidentes.  **Formación de los empleados**: Capacita a todos los empleados sobre las mejores prácticas de seguridad de la información, los protocolos de protección de datos y cómo reconocer y responder a amenazas de seguridad como ataques de phishing. Educar a los empleados sobre ciberseguridad es vital para una estrategia de defensa integral. Los ataques de ingeniería social y el phishing son amenazas frecuentes dirigidas a las MIPYME, los empleados deben ser capaces de identificar y mitigar sus riesgos mediante el reconocimiento de correos electrónicos de phishing, el manejo de archivos adjuntos sospechosos y la implementación de protocolos de autenticación de correo electrónico. En este sentido, la seguridad de las contraseñas juega un papel crucial en la protección de datos confidenciales. Los empleados deben ser conscientes de las prácticas para crear contraseñas seguras, implementar la autenticación multifactor (MFA) y administrar políticas de contraseñas dentro de la organización.  **Controles de acceso**: Implementar controles de acceso para garantizar que solo el personal autorizado tenga acceso a datos sensibles. Utiliza el control de acceso basado en roles para restringir el acceso en función de las funciones y responsabilidades del trabajo.  **Manejo seguro de datos**: Establecer directrices para el manejo seguro de datos, tanto en formatos digitales como físicos. Esto incluye el almacenamiento adecuado, el cifrado y la eliminación segura de información confidencial.  **Actualizaciones y parches de software regulares**: Mantén todo el software, incluidos los sistemas operativos, las aplicaciones y las herramientas de seguridad, actualizados con los últimos parches y actualizaciones para abordar vulnerabilidades conocidas.  **Firewalls y software antivirus**: Implementa firewalls y software antivirus/antimalware de buena reputación para proteger contra amenazas externas.  **Configuración de red segura**: Configura las redes de forma segura, incluidas las redes Wi-Fi, para evitar el acceso no autorizado y la interceptación de datos.  **Copia de seguridad y recuperación de** **datos**: Realiza copias de seguridad periódicas de datos críticos y prueba el proceso de restauración de datos para garantizar la continuidad del negocio en caso de pérdida de datos o un ciberataque.  **Plan de respuesta a incidentes**: Desarrollar un plan claro de respuesta a incidentes que describa los pasos a seguir en caso de violación de seguridad o violación de datos. Asignar roles y responsabilidades al personal clave para una gestión eficaz de incidentes. Prepararse y responder eficazmente a los incidentes de ciberseguridad es esencial para minimizar los daños y mitigar los riesgos.  **Gestión de proveedores**: Si la MIPYME utiliza proveedores externos o proveedores de servicios, lleve a cabo la diligencia debida para garantizar que sus prácticas de seguridad de la información se ajusten a los estándares de tu organización.  **Supervisión y auditoría continuas**: Implementar monitoreo continuo y auditorías periódicas de seguridad para detectar y abordar posibles problemas de seguridad de forma proactiva.  **Cumplimiento de la privacidad de** **los datos**: Mantente actualizado con las leyes y regulaciones de privacidad de datos relevantes que se aplican a las operaciones de las MIPYME. Cumplir con los requisitos de protección de datos e informar a los clientes sobre las prácticas de manejo de datos.  **Sensibilización y cultura en materia de seguridad**: Fomentar una cultura de conciencia y responsabilidad en materia de seguridad entre los empleados. Fomentar la notificación de incidentes y preocupaciones en materia de seguridad.  **Revisiones de seguridad regulares**: Llevar a cabo revisiones periódicas de seguridad y evaluaciones de riesgos para identificar las amenazas emergentes y posibles áreas de mejora.  Al administrar proactivamente la seguridad de la información, las MIPYME pueden reducir el riesgo de violaciones de datos, proteger la información confidencial y generar confianza con los clientes y socios, contribuyendo en última instancia al éxito a largo plazo de la empresa. | | | |
| 5 entradas del glosario | **Internet de las cosas (IoT).** El Internet de las cosas, o IoT (Internet of Things), es un sistema de dispositivos informáticos interrelacionados, máquinas mecánicas y digitales, objetos, animales o personas que cuentan con identificadores únicos (UID) y la capacidad de transferir datos a través de una red sin requerir interacción de humano a humano o de humano a computadora.  Fuente: TechTarget <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>  **Denegación de Servicio (DoS).** Denegación de servicio (DoS) es un tipo de ciberataque diseñado para desactivar, cerrar o interrumpir una red, sitio web o servicio. Por lo general, un malware se utiliza para interrumpir o inhibir el flujo normal de datos dentro y fuera de un sistema para hacer que el objetivo sea inútil o inaccesible durante un período determinado. Un ejemplo de un ataque DoS: cuando se accede a un sitio web de forma masiva y repetida desde diferentes ubicaciones, lo que impide que los visitantes legítimos accedan al sitio web.  Fuente: Tendencia Micro <https://www.trendmicro.com/vinfo/us/security/definition/denial-of-service-dos>  **Autenticación multifactor.** La autenticación multifactor (del inglés, Multi-Factor Authentication, siglas MFA) es un método de autenticación que requiere que el usuario proporcione dos o más factores de verificación para obtener acceso a un recurso como una aplicación, una cuenta en línea o una VPN. La MFA es un componente central de una sólida política de gestión de identidad y acceso (Identity and Access Managament, o IAM). En lugar de solo pedir un nombre de usuario y contraseña, MFA requiere uno o más factores de verificación adicionales, lo que disminuye la probabilidad de un ataque cibernético exitoso.  Fuente: OneLogin <https://www.onelogin.com/learn/what-is-mfa>  **Identificador de conjunto de servicio (SSID).** (Servicio Set IDentifier) El nombre asignado a una red Wi-Fi (wireless). Todos los dispositivos de la red deben usar este nombre sensible al caso para comunicarse a través de Wi-Fi, que es una cadena de texto de hasta 32 bytes de largo. Fuera de la caja, los routers inalámbricos y los puntos de acceso tienen un SSID predeterminado, que puede ser el nombre del fabricante, como «linksys» o «netgear» o simplemente «por defecto». Algunos dispositivos usan su número de modelo como SSID. Utilizando un navegador web, el SSID (y la contraseña) se pueden cambiar manualmente en la configuración del dispositivo.  **Fuente: PCMAG** [**https://www.pcmag.com/encyclopedia/term/ssid**](https://www.pcmag.com/encyclopedia/term/ssid)  **Universal Plug and Play (UPnP).** UPnP (Universal Plug and Play) es un protocolo de red que permite a los dispositivos descubrirse entre sí y conectarse sin necesidad de configuración manual o intervención del usuario. El protocolo automatiza todos los pasos necesarios para el reconocimiento y la comunicación entre dispositivos en la misma red.  Fuente: **PhoenixNAP** <https://phoenixnap.com/blog/what-is-upnp>  **Ataques de día cero**: Un ataque o exploit de día cero es un ataque cibernético dirigido a una vulnerabilidad de software que es desconocida para el proveedor de software o para los proveedores de antivirus. El atacante detecta la vulnerabilidad del software antes que cualquier parte interesada en mitigarla, crea rápidamente un exploit y lo usa para un ataque. Es muy probable que tales ataques tengan éxito porque las defensas no están en su lugar. Esto hace que los ataques de día cero sean una grave amenaza para la seguridad.  Fuente: **Imperva** <https://www.imperva.com/learn/application-security/zero-day-exploit/>  **Ransomware**: Ransomware es un tipo de malware que impide o limita el acceso de los usuarios a su sistema, ya sea bloqueando la pantalla del sistema o bloqueando los archivos de los usuarios hasta que se paga un rescate. Las familias de ransomware más modernas, clasificadas colectivamente como cryptoransomware, cifran ciertos tipos de archivos en sistemas infectados y obligan a los usuarios a pagar el rescate a través de ciertos métodos de pago en línea para obtener una clave de descifrado.  Fuente: **Tendencia Micro** [**https://www.trendmicro.com/vinfo/us/security/definition/ransomware**](https://www.trendmicro.com/vinfo/us/security/definition/ransomware) | | | |
| 5 preguntas de autoevaluación de opción múltiple | Pregunta 1: ¿Qué es una política de seguridad?  Opción a: Es un documento informal que describe el enfoque de la organización para  seguridad de la información  Opción b: Es un documento formal que establece las reglas, directrices y responsabilidades para proteger los activos, datos y sistemas de la empresa de posibles amenazas y acceso no autorizado  Opción c: Una política para proteger solo los activos de la empresa  Opción d: Todas las opciones son correctas  Opción correcta: B  Pregunta 2. Por qué es importante entender la ciberseguridad y la seguridad  ¿políticas?  Opción a: La comprensión de la ciberseguridad permite a las personas ser conscientes de las diversas ciberamenazas y riesgos que existen en el panorama digital  Opción b: Las medidas de ciberseguridad protegen los datos sensibles y confidenciales de  acceso no autorizado, robo o mal uso  Opción c: Las políticas de seguridad desempeñan un papel importante en la prevención de violaciones de datos y ciberataques  Opción d: Las otras tres respuestas son correctas  Opción correcta: D  Pregunta 3. Indica qué respuesta es verdadera:  Opción a: Los ciberataques pueden causar pérdidas financieras insignificantes a las MIPYMES  Opción b: Un ciberataque exitoso puede dañar la reputación de una MIPYME, lo que lleva a una pérdida de clientes y oportunidades  Opción c: Educar al personal sobre las mejores prácticas, las amenazas potenciales y la seguridad las políticas ayudan a crear una cultura de seguridad sólida dentro de la organización  Opción d: Los clientes y socios a menudo no priorizan la seguridad al elegir  socios comerciales, haciendo de la seguridad cibernética un valioso diferenciador  Opción correcta: B & C  Pregunta 4. Por favor, señala las amenazas comunes a la ciberseguridad para las MIPYMES  Opción a: Tratamientos internos, infecciones y ajustes de seguridad bien configurados  Opción b: Violaciones de datos, contraseñas débiles y autenticación, infecciones de malware  Opción c: Ataques de phishing, ataques a la cadena de suministro, dispositivos IoT no seguros  Opción d: Todas las respuestas son incorrectas  Opción correcta: B & C  Pregunta 5. ¿Qué pasos puede tomar una MIPYME para evaluar las vulnerabilidades de su ciberseguridad?  Opción a: Verificar la seguridad física, examinar la conciencia de los empleados y revisar las políticas de contraseñas  Opción b: Identificar activos y datos, tealizar una evaluación de riesgos y comprobar la seguridad física  Opción c: Garantizar la seguridad de la red wi-fi, las pruebas de penetración y la evaluación de Software y aplicaciones  Opción d: Todas las respuestas son correctas  Opción correcta: D | | | |
| Bibliografía y otras referencias | Forbes Tech Council. (2023, May 25). Small But Mighty: Cybersecurity Best Practices for SMEs. Forbes. <https://www.forbes.com/sites/forbestechcouncil/2023/05/25/small-but-mighty-cybersecurity-best-practices-for-smes/?sh=44510c371a33>  Devonshire Green (n.d.). The Importance of Cybersecurity for SMEs. Devonshire Green. <https://www.devonshiregreen.uk/the-importance-of-cybersecurity-for-smes/>  European Union Agency for Cybersecurity (ENISA). (2021). Cybersecurity for SMEs: Challenges and Recommendations. ENISA. <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes/@@download/fullReport>  European Union Agency for Cybersecurity (ENISA). (2021). Cybersecurity Guide for SMEs. ENISA. <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport>  Ministry of Economy and Competitiveness (Spain). (2021). Digitalisation Plan for SMEs [PDF]. Government of Spain. <https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210902-digitalisation-smes-plan.pdf>  Yerik Afrianto Singgalen. (2021, August). Exploring MSMEs' Cybersecurity Awareness and Risk Management: Information Security Awareness. ResearchGate. <https://www.researchgate.net/publication/353622348_Exploring_MSMEs_>  Cybersecurity\_Awareness\_and\_Risk\_Management\_Information\_Security\_Awareness | | | |
| Material relacionado | DREAM\_WP3\_Cybersecurity\_ITSFA\_ES | | | |
| Vídeo (en su caso) | [enlace] | | | |