Ficha de formación

|  |  |  |  |
| --- | --- | --- | --- |
| Título | Fundamentos de ciberseguridad para las microempresas en ámbito rural: Como asegurar la transformación digital y empresarial en la era post-COVID | | |
| Palabras Clave | Ciberseguridad, Microempresas rurales, Transformación digital, Seguridad empresarial, Protección de datos, Seguridad de la información, Ciberamenazas, Privacidad en línea, Seguridad de la red, Ciberresiliencia, Detección de amenazas, Gestión de riesgos, ataques de phishing, Sensibilización de la seguridad, Evaluación de vulnerabilidades, Seguridad en la nube, Ciberseguridad de las pequeñas empresas, Buenas prácticas en materia de ciberseguridad | | |
| Idioma | Inglés | | |
| Objetivos y Metas | | | |
| Los objetivos y metas de esta formación son:  **Comprender los Fundamentos de Ciberseguridad**: Proporcionar una comprensión clara de los conceptos fundamentales de ciberseguridad, terminología y principios relevantes para las microempresas rurales.  **Identificar las amenazas cibernéticas**: Educar sobre las amenazas cibernéticas comunes, como el phishing, el malware, el ransomware y la ingeniería social, lo que les permite reconocer y responder de manera efectiva a posibles ataques.  **Mejorar la protección de datos**: Enseñar estrategias para salvaguardar los datos confidenciales del negocio y del cliente, haciendo hincapié en el cifrado, los controles de acceso y el almacenamiento seguro de datos.  **Transformación digital segura**: Proporcionar orientación sobre la integración de las medidas de ciberseguridad en los procesos de transformación digital de las pymes rurales para garantizar una transición segura.  **Fomentar la sensibilización sobre el riesgo**: Concienciar sobre los riesgos asociados con la ciberseguridad inadecuada y las posibles consecuencias para el negocio, incluidas las pérdidas financieras y los daños a la reputación.  **Fomentar la formación de los empleados**: Hacer hincapié en la importancia de la formación continua en ciberseguridad para todos los empleados para crear una cultura de conciencia y responsabilidad en materia de seguridad.  **Dar directrices de seguridad en el trabajo en remoto**: Proporcionar orientación sobre la protección de entornos de trabajo remotos y el uso de dispositivos personales para prevenir amenazas cibernéticas. | | | |
| Resultados de Aprendizaje | | | |
| Al final de esta formación, los usuarios podrán:   * Tener una **comprensión integral de los fundamentos de ciberseguridad** adaptados a las microempresas en ámbito rural. * **Identificar y mitigar las ciberamenazas comunes**, reduciendo el riesgo de ser víctima de ciberataques. * Tener la capacidad de **asegurar los datos de negocios y clientes**, fomentando la confianza y la reputación. * **Incorporar medidas de ciberseguridad** en su proceso de transformación digital. * **Reducir los riesgos de ciberseguridad** fomentando un enfoque proactivo de ciberseguridad. * **Establecer una cultura de conciencia de seguridad** entre los empleados para salvaguardar colectivamente los activos digitales. * **Promover la seguridad en el trabajo a distancia** para mantener la ciberseguridad mientras se trabaja en remoto. * **Aplicar estrategias de protección de datos** que incluyan encriptación, controles de acceso y almacenamiento de datos seguro para salvaguardar la información confidencial del negocio y del cliente. * **Evaluar los riesgos de ciberseguridad**, comprender las posibles consecuencias de los ciberincidentes y tomar decisiones informadas para mitigar esos riesgos. * **Evaluar las medidas y controles de seguridad existentes** dentro de la microempresa, identificando áreas de mejora. | | | |
| Contenidos | | | |
| Unidad 1 Fundamentos de ciberseguridad para una transformación digital fluida de las microempresas rurales   * 1. Identificación de amenazas y riesgos cibernéticos   Los fundamentos de la ciberseguridad son **esenciales para garantizar una transformación digital fluida de las pymes de ámbito rural**.  Las microempresas rurales, como cualquier otra empresa, son vulnerables a una serie de amenazas y riesgos cibernéticos. Si bien su escala podría ser menor, el impacto potencial aún puede ser significativo.  Estas son las principales amenazas y riesgos cibernéticos que las microempresas rurales deben tener en cuenta:  Ataques de phishing:   * Los atacantes envían **correos electrónicos engañosos para convencer a los empleados para que revelen información confidencial**, como credenciales de inicio de sesión o datos financieros.   Infecciones de malware:   * El software malicioso (malware) incluye virus, ransomware y spyware que pueden infiltrarse en sistemas, **robar datos o bloquear archivos para obtener un rescate**.   Ataques de ransomware:   * **Ransomware cifra archivos y exige el pago de la clave de descifrado**, lo que puede causar **pérdida de datos o interrupciones del negocio**.   Ingeniería Social:   * **Manipular a los empleados a través de tácticas psicológicas** para **divulgar información confidencial** o realizar acciones que comprometan la seguridad.   Amenazas internas:   * Los empleados que no están satisfecho con su puesto y tienen acceso a datos confidenciales pueden **comprometer intencionalmente o involuntariamente la seguridad**.   Contraseñas débiles:   * **Las contraseñas inseguras hacen que sea más fácil para los atacantes obtener acceso no autorizado** a sistemas y cuentas.   **Software sin parches**:   * **La falta de actualizaciones de software e instalación de parches puede hacer que los sistemas sean vulnerables**.   Falta de cifrado de datos:   * **Los datos no encriptados se pueden interceptar durante la transmisión**, exponiendo información sensible.   Redes Wi-Fi inseguras:   * **Las redes Wi-Fi no seguras pueden ser explotadas por los atacantes** para espiar las comunicaciones o lanzar ataques.   **Acceso no autorizado**:   * **La falta de controles de acceso** puede llevar a personas no autorizadas a acceder a información o sistemas sensibles.   Robo físico de dispositivos:   * **El robo o la pérdida de dispositivos** como portátiles o teléfonos inteligentes puede resultar en violaciones de datos si contienen información confidencial.   Riesgos de proveedores y terceros:   * **Las debilidades de ciberseguridad en proveedores externos pueden** conducir a ataques a la cadena de suministro que afectan a las microempresas.   Falta de sensibilización sobre la seguridad:   * Los empleados que no están al tanto de los riesgos de ciberseguridad pueden caer inadvertidamente en comportamientos en línea arriesgados.   Violaciones de datos:   * **La exposición de datos de clientes o negocios debido a una violación** puede conducir a consecuencias legales, financieras y de reputación.   **Vulnerabilidades en el trabajo en remoto**:   * Las **configuraciones de trabajo en remoto pueden introducir vulnerabilidades de seguridad** si no se implementan las medidas de ciberseguridad adecuadas.   Falta de copia de seguridad y recuperación de datos:   * El hecho de no realizar copias de seguridad periódicas de los datos puede dar lugar a la **pérdida de datos durante los incidentes cibernéticos**.   Incumplimiento normativo:   * El **incumplimiento de las regulaciones específicas de la industria** puede resultar en sanciones legales.   Recursos limitados para la ciberseguridad:   * Las microempresas pueden carecer de personal informático específico o presupuesto para medidas sólidas de ciberseguridad.   Vulnerabilidades de IoT:   * Los dispositivos **de Internet de las Cosas (IoT)** pueden ser comprometidos y **utilizados como puntos de entrada** para ataques.   Amenazas de las redes sociales:   * Compartir demasiada información en las plataformas de redes sociales puede **proporcionar a los atacantes información para crear ataques dirigidos**.   Para mitigar estos riesgos, las microempresas rurales deben invertir en educación en ciberseguridad, implementar medidas de seguridad sólidas, mantener los software actualizados y priorizar un enfoque proactivo de la ciberseguridad.  1.2. Integración de las medidas de ciberseguridad en las actividades empresariales  La integración de las medidas de ciberseguridad en las actividades empresariales de las microempresas rurales (pymes) es crucial para proteger sus activos y operaciones digitales.  En este sentido, las MIPYME rurales deben realizar lo siguiente para proteger sus negocios de las ciberamenazas:  Evaluación y Gestión de Riesgos:   * Llevar a cabo una **evaluación** integral de riesgos para identificar posibles ciberamenazas y vulnerabilidades. * Desarrollar una **estrategia de gestión de riesgos** que describa cómo mitigar, transferir o gestionar riesgos.   Sensibilización y Formación en Seguridad:   * Proporcionar **formación en ciberseguridad** a todos los empleados para ayudarlos a reconocer y responder a las amenazas cibernéticas. * Fomentar una cultura de **conciencia de la seguridad** para garantizar que la seguridad sea responsabilidad de todos.   Protección de Datos y Privacidad:   * Implementar **medidas sólidas de protección de datos**, **incluyendo cifrado, controles de acceso y clasificación de datos**. * Garantizar **el cumplimiento de las regulaciones de privacidad de datos** y comunicar las políticas de uso de datos a los empleados.   Infraestructura de red segura:   * Implementar **firewalls robustos, sistemas de detección de intrusiones y sistemas de prevención de intrusiones para salvaguardar la red**.   Seguridad del punto final:   * **Instalar y actualizar regularmente software antivirus y antimalware** en todos los dispositivos. * **Aplicar políticas de contraseñas seguras e implementar la autenticación multifactor** (MFA) para acceder a los sistemas.   **Desarrollo seguro de software**:   * **Seguir las prácticas de codificación segura** para minimizar las vulnerabilidades en las aplicaciones de software. * **Actualizar y parchear regularmente el software** para abordar vulnerabilidades de seguridad conocidas.   Copia de seguridad y recuperación de datos:   * **Realizar copias de seguridad de datos y sistemas regularmente** para garantizar que los datos se puedan restaurar en caso de un incidente cibernético. * **Testear el proceso de restauración** para verificar la efectividad de las copias de seguridad.   Plan de Respuesta a Incidentes:   * Desarrollar un **plan de respuesta a incidentes bien definido** que describa los pasos a seguir en caso de un incidente de ciberseguridad. * **Designar funciones y responsabilidades** para los miembros del equipo de respuesta a incidentes.   Uso seguro de la nube:   * **Elegir proveedores de servicios en la nube** de buena reputación con fuertes medidas de seguridad. * Implementar **controles de acceso y cifrado** adecuados para los datos almacenados en la nube.   Gestión de riesgos de proveedores:   * Evaluar y gestionar los **riesgos de ciberseguridad asociados a proveedores** y socios externos. * **Incluir los requisitos de ciberseguridad en los** contratos de proveedores.   Seguridad física:   * **Asegurar el acceso físico a los locales** donde se encuentran los activos digitales. * Implementar medidas de seguridad como **controles de acceso, vigilancia y gestión de visitantes**.   Cumplimiento normativo:   * Mantenerse informados sobre **las regulaciones de ciberseguridad relevantes** y los estándares de la industria. * Garantizar el cumplimiento de la **normativa aplicable para evitar consecuencias legales y financieras**.   Monitoreo y Mejora Continua:   * **Monitorear regularmente los sistemas y redes** en busca de señales de acceso no autorizado o actividad sospechosa. * **Actualizar y mejorar continuamente las medidas de ciberseguridad** frente a nuevas amenazas.   Auditorías y evaluaciones de seguridad:   * **Llevar a cabo auditorías y evaluaciones de seguridad periódicas para identificar deficiencias** y áreas de mejora. * **Utilizar los resultados para mejorar la política de ciberseguridad** de la organización.   Formación y sensibilización de los empleados:   * **Formar regularmente a los empleados sobre las buenas prácticas de ciberseguridad**. * Llevar a cabo talleres sobre la **identificación de correos electrónicos de phishing y tácticas de ingeniería social**. * Promover una cultura de conciencia de la seguridad a través de la comunicación continua.   Políticas de contraseñas fuertes:   * **Aplicar políticas de contraseñas seguras para** todas las cuentas. * **Utilizar software de generación de contraseñas para generar y almacenar contraseñas complejas**. * Habilitar la **autenticación multifactor (MFA)** para mayor seguridad.   Actualizaciones regulares de software:   * Configurar las **actualizaciones automáticas** para sistemas operativos y software. * Aplicar **parches de seguridad** de forma proactiva para abordar vulnerabilidades conocidas.   Firewall y segmentación de red:   * **Instalar firewalls** para filtrar el tráfico de red entrante y saliente. * Segmentar la red para **restringir el acceso a sistemas sensibles**.   Protección del punto final:   * **Instalar y actualizar software antivirus y antimalware en todos los dispositivos**. * **Utilizar herramientas de detección y respuesta de endpoints (EDR)** para el monitoreo de amenazas en tiempo real.   Cifrado de datos:   * **Cifrar datos sensibles** tanto durante la transmisión como durante el almacenamiento. * Implementar el **cifrado para correos electrónicos, bases de datos y archivos**.   Seguro cibernético:   * Considerar la posibilidad de **comprar un seguro cibernético** para cubrir las pérdidas financieras derivadas de incidentes cibernéticos.   Controles de acceso de usuarios:   * **Asignar permisos basados** en el principio de privilegio mínimo. * **Revisar y revocar periódicamente los derechos de acceso innecesarios**.   Gestión de parches:   * Implementar **un proceso de administración de** parches para garantizar actualizaciones oportunas. * **Testear los parches** antes de la implementación para evitar interrupciones del sistema.   Programas de Concientización de Seguridad:   * Llevar a cabo **programas continuos de concientización de seguridad** para educar a los empleados. * **Proporcionar recursos** como carteles, boletines informativos y materiales de capacitación.   Políticas y procedimientos de ciberseguridad:   * Desarrollar y documentar políticas y procedimientos de ciberseguridad. * Comunicar claramente estas políticas a todos los empleados.   La integración de estas medidas requiere el compromiso por parte de los altos mandos, la formación continua de los empleados y un enfoque proactivo hacia la ciberseguridad. La evaluación y la adaptación periódicas son esenciales para hacer frente a las amenazas emergentes y mantener un entorno digital seguro para las pymes rurales.  Al implementar estos fundamentos de ciberseguridad, las MIPYME rurales pueden segui en su trasformación digital de forma segura, sabiendo que sus activos digitales, datos de clientes y operaciones están protegidos contra las amenazas cibernéticas.  Unidad 2 Buenas prácticas en materia de ciberseguridad para proteger los datos personales y la privacidad  2.1. Medidas de protección de datos para las pequeñas y medianas empresas rurales  La protección de datos es un concepto clave para que todas las MIPYME, sean rurales o urbanas, puedan salvaguardar la información sensible de las empresas y de los clientes.  Además de las medidas generales de ciberseguridad que hemos mencionado hasta ahora, hay una serie de medidas específicas de protección de datos que las MIPYME rurales deben implementar para la protección de datos, tales como:  Clasificación de datos:   * Clasificar los datos en función de su sensibilidad e importancia. * Aplicar medidas de seguridad adecuadas basadas en la clasificación de los datos.   Implementación de cifrado:   * Cifrar datos sensibles tanto en su almacenamiento como durante la transmisión. * Utilizar herramientas de cifrado para proteger la información del cliente y los secretos comerciales.   Controles de acceso:   * Implementar controles de acceso basados en roles (RBAC) para restringir el acceso a los datos. * Otorgar acceso solo al personal autorizado en función de sus roles de trabajo.   **Copias de seguridad de datos con regularidad**:   * Realizar copias de seguridad de datos regularmente para protegerlos. * Comprobar y testear la restauración de datos para garantizar que las copias de seguridad sean viables en caso de pérdida de datos.   Eliminación segura de datos:   * Desarrollar procedimientos para la eliminación segura de hardware y dispositivos de almacenamiento antiguos. * Utilizar herramientas de limpieza de datos que garanticen que los datos no se puedan recuperar.   Formación de Usuarios:   * Educar a los empleados sobre la importancia de la protección de datos. * Formarlos en prácticas seguras de gestión de datos, como no compartir contraseñas.   Políticas de seguridad:   * Desarrollar políticas de protección de datos y privacidad. * Comunicar claramente estas políticas a todos los empleados.   Minimización de datos:   * Recopilar y conservar solo los datos necesarios para las operaciones comerciales. * Eliminar datos obsoletos o innecesarios.   Responsabilidad de los empleados:   * Responsabilizar a los empleados para que se adhieran a las políticas de protección de datos. * Implementar sanciones por infringir las normas de protección de datos.   Seguimiento y registro:   * Implementar herramientas de monitoreo para rastrear el acceso y el uso de los datos. * Mantener registros para auditorías e investigaciones de incidentes.   Trabajo remoto seguro:   * Proporcionar pautas para proteger los datos cuando se trabaja de forma remota. * Fomentar el uso de redes privadas virtuales (VPN) para conexiones seguras.   Políticas de conservación de datos:   * Establecer políticas sobre cuánto tiempo deben conservarse los diferentes tipos de datos. * Eliminar los datos que ya no son necesarios.   Mejora continua:   * Revisar y actualizar periódicamente las medidas de protección de datos basadas en amenazas emergentes. * Mantenerse informado sobre las buenas prácticas y las nuevas tecnologías.   Al implementar estas medidas, las MIPYME rurales pueden mejorar significativamente sus procesos de gestión de protección de datos, minimizando el riesgo de violaciones de datos y garantizando la confianza de sus clientes y socios.  2.2. Directrices de ciberseguridad del trabajo a distancia  En el panorama laboral actual, donde el trabajo remoto se ha convertido en una práctica predominante, es imperativo que las micro, pequeñas y medianas empresas rurales (MSME) prioricen la ciberseguridad.  Esto es crucial no solo para mantener la integridad de sus operaciones, sino también para salvaguardar la información confidencial mientras sus empleados operan fuera del entorno de oficina convencional.  Para profundizar en las directrices esenciales de ciberseguridad del trabajo en remoto que estas empresas rurales deberían considerar adoptar, mencionamos las siguientes medidas:  1. Utilizar conexiones seguras:  En esta era de conectividad digital, **enfatizar el uso de redes privadas virtuales (VPN)** es vital. Las VPN proporcionan un canal seguro para la transmisión de datos a través de Internet, cifrando de forma eficaz la información que se intercambia. Es importante alentar a los empleados a usar VPN mientras acceden a los sistemas corporativos para **agregar una capa adicional de protección** contra posibles amenazas cibernéticas.  2. Autenticación multifactor (MFA):  Se puede establecer una capa adicional de seguridad a través de la implementación de la autenticación multifactor (MFA). Este enfoque **asegura que el acceso a cuentas corporativas sensibles requiere múltiples formas de verificación,** como una contraseña y un código único enviado al dispositivo móvil del usuario. Esta medida simple, pero eficaz reduce el riesgo de acceso no autorizado.  3. Uso seguro del dispositivo:  Suministrar a los empleados dispositivos emitidos por la empresa equipados con software de seguridad actualizado es un paso fundamental. Esto garantiza que todos los **dispositivos estén constantemente protegidos** contra las amenazas emergentes. Además, es importante desalentar **el uso de computadoras públicas o dispositivos compartidos para tareas relacionadas con el trabajo para evitar posible hurtos de datos confidenciales**.  4. Actualizaciones regulares de software:  Es muy importante **actualizar regularmente los sistemas operativos, las aplicaciones y el software de seguridad**. Estas actualizaciones suelen incluir parches que cubren vulnerabilidades conocidas. Mantener el software actualizado protege contra posibles exploits por parte de los ciberdelincuentes.  5. Conexiones Wi-Fi seguras:  Guiar a los empleados a conectarse a **redes Wi-Fi seguras y protegidas con contraseña es vital**. Esta práctica impide el acceso no autorizado a los datos mientras se trabaja de forma remota. Al mismo tiempo, evitar las redes Wi-Fi públicas abiertas para tareas de trabajo minimiza la exposición a posibles ataques.  6. Contraseñas fuertes:  El uso de **contraseñas sólidas y únicas para cuentas relacionadas con el trabajo** es una práctica fundamental. Esto evita ataques e intentos de acceso no autorizados. Es importante desalentar el uso compartido y la reutilización de contraseñas en varias cuentas para mejorar aún más la seguridad.  7. Cifrado de datos:  Otra práctica útil es **cifrar datos sensibles tanto durante la transmisión como durante el almacenamiento.** El cifrado transforma los datos en código ilegible, imposibilitando su interceptación. Fomentar el uso de herramientas de comunicación cifradas para conversaciones confidenciales fortalece la seguridad.  8. Conciencia de phishing:  Educar a los empleados sobre **el reconocimiento de correos electrónicos de phishing y otros ataques de ingeniería social es una medida proactiva**. En este sentido es vital resaltar los riesgos asociados con hacer clic en enlaces sospechosos o descargar archivos adjuntos de fuentes desconocidas puede evitar posibles infracciones.  **9. Compartir archivos seguros**:  Además de lo anterior, es muy útil el **uso de herramientas de intercambio de archivos** aprobadas por la empresa que tengan con controles de cifrado y acceso para garantizar que los archivos sensibles se intercambien de forma segura. Por el contrario, es fundamental **desalentar el intercambio de archivos confidenciales a través de correo electrónico personal o servicios en la nube** para **evitar fugas de datos**.  10. Seguridad física:  Es prioritario enfatizar la **necesidad de proteger los dispositivos de trabajo** cuando no están en uso y mantener los materiales relacionados con el trabajo fuera de la vista de personas no autorizadas para mitigar los riesgos de seguridad física. Esto es especialmente relevante para los trabajadores que trabajan desde accesos remotos y que operan en entornos diversos.  11. Copia de seguridad de datos:  Educar a los empleados sobre la importancia de **hacer una copia de seguridad regularmente de los datos de trabajo** en una ubicación segura. Esto prepara a las empresas para recuperar los datos rápidamente en caso de pérdidas de datos debido a incidentes cibernéticos u otros eventos imprevistos.  12. Videoconferencia segura:  Elegir plataformas de videoconferencia que emplean cifrado de extremo a extremo garantiza que los intercambios permanezcan confidenciales. La implementación de características de seguridad **como contraseñas de reuniones y salas de espera agrega una capa adicional de control** sobre quién puede acceder a estas reuniones virtuales.  13. Uso los canales de comunicación oficiales:  Promover el uso de **herramientas de comunicación aprobadas por la empresa** para las discusiones relacionadas con el trabajo contribuye a crear un entorno controlado para compartir información. Es importante evitar hablar de asuntos sensibles en plataformas de mensajería personal para minimizar el riesgo de exposición de datos.  14. Seguridad del protocolo de escritorio remoto (RDP):  Si se emplea el Protocolo de Escritorio Remoto (RDP), es esencial protegerlo **con contraseñas seguras y controles de acceso**. El uso de una VPN junto con RDP añade una capa adicional de protección contra el acceso no autorizado.  15. Formación en seguridad:  La realización de **sesiones de formación en ciberseguridad con regularidad** mantiene a los empleados bien informados sobre la evolución de las amenazas y las mejores prácticas. Esto les permite tomar decisiones informadas y mejora la postura general de seguridad de la organización.  16. Notificación de incidentes:  El establecimiento de **procedimientos claros para denunciar incidentes de ciberseguridad** o actividades sospechosas garantiza que las posibles infracciones se aborden con prontitud. Los empleados deben ser conscientes de a quién contactar en caso de una violación de seguridad.  17. Política de trabajo en remoto:  Desarrollar y comunicar una **política integral de trabajo remoto que describa las expectativas y directrices de seguridad** proporciona a los empleados una comprensión clara de sus responsabilidades. Esto fomenta un entorno de trabajo remoto seguro.  18. Monitoreo continuo:  Implementar **herramientas de monitoreo que puedan detectar y responder a incidentes de seguridad en tiempo real** es crucial. La revisión periódica de los registros de acceso remoto para actividades no autorizadas permite la detección y mitigación proactiva de amenazas.  19. Chequeos regulares:  Mantener **una comunicación continuada con los empleados que trabajan en remoto** sirve para múltiples propósitos. No solo permite abordar las preocupaciones de seguridad, sino que también proporciona soporte continuo, reforzando una sensación de conexión incluso en entornos de trabajo remotos.  20. Cumplimiento de los reglamentos:  Garantizar que las **prácticas de trabajo a distancia se ajusten a las normas pertinentes de protección de datos y privacidad no es negociable**. El cumplimiento de estas regulaciones protege tanto la información confidencial del negocio como de sus clientes.  Si se respetan estas pautas de ciberseguridad del trabajo en remoto, las MIPYME rurales pueden permitir a sus empleados trabajar de forma remota sin comprometer la seguridad de los datos. Estas medidas contribuyen a minimizar el riesgo de ciberamenazas y a mantener un sólido nivel de seguridad, incluso en el contexto de un entorno de trabajo en remoto. | | | |
| Autoevaluación (5 consultas y respuestas de opción múltiple) | | | |
| Unidad 1: Identificación de amenazas y riesgos cibernéticos  ¿Qué tipo de ataque cibernético implica que los atacantes envíen correos electrónicos engañosos para engañar a los empleados para que revelen información confidencial?  a) Infecciones de malware  B) Ataques de ransomware  C) Amenazas internas  D) Ataques de phishing  ¿Qué tipo de ataque cibernético implica encriptar archivos y exigir el pago de la clave de descifrado?  a) Ataques de Phishing  B) Ingeniería Social  C) Ataques de ransomware  D) Infecciones de malware  Unidad 1.2: Integración de las medidas de ciberseguridad en las actividades empresariales  ¿Cuál es el objetivo principal de llevar a cabo una evaluación de riesgos en ciberseguridad?  a) Aumentar las ciberamenazas  B) Identificar posibles ciberamenazas y vulnerabilidades  C) Eliminar todos los riesgos cibernéticos  D) Crear nuevas vulnerabilidades de seguridad  Unidad 2.1: Medidas de protección de datos para las pequeñas y medianas empresas rurales  ¿Cuál es el propósito de clasificar los datos en función de su sensibilidad e importancia?  a) Hacer más fácil el acceso a los datos  B) Aplicar medidas de seguridad adecuadas basadas en la clasificación de los datos  C) Aumentar las políticas de retención de datos  D) Eliminar las necesidades de cifrado de datos  ¿Cuál es el propósito de respaldar regularmente datos críticos?  a) Eliminar la necesidad de encriptación de datos  B) Para evitar actualizaciones de software  C) Asegurar que los datos puedan ser restaurados en caso de pérdida de datos  D) Para acelerar el rendimiento de la red  Unidad 2.2: Directrices de ciberseguridad del trabajo remoto  ¿Cómo mejora una red privada virtual (VPN) la seguridad del trabajo en remoto?  a) Aumenta el intercambio de datos  B) Elimina la necesidad de autenticación multifactor  C) Proporciona un canal seguro para la transmisión de datos  D) Fomenta el uso de la red Wi-Fi pública abierta | | | |
| Definir el nivel del MEC (Marco de Cualificación de la UE) de nuestra formación (3-5) | | | | |
| Nivel 3  **X** Nivel 4  Nivel 5 | | | | |
| Referencias cruzadas: DigComp 2.2 + EntreComp | | | | |
| **alfabetización en información y datos**  **comunicación y colaboración**  **creación de contenido digital**  **seguridad**  **resolución de problemas**  Competence(s):   * Dispositivos de protección * Protección de los datos personales y de la privacidad | | | **ideas y oportunidades**  **recursos**  **en acción**  Competencia(es):   * Autoconciencia y autoeficacia | |
| Glosario (máximo 5 términos) | | **Detección y respuesta de endpoints (EDR)**: La detección y respuesta de endpoints (EDR), también conocida como detección y respuesta de amenazas de endpoints (ETDR), es una solución integrada de seguridad de endpoint que combina el monitoreo continuo en tiempo real y la recopilación de datos de endpoint con capacidades de respuesta y análisis automatizadas basadas en reglas.  Fuente: Trellix <https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html>  **Controles de acceso basados en roles (RBAC):** El control de acceso basado en roles (RBAC) se refiere a la idea de asignar permisos a los usuarios en función de su rol dentro de una organización. Ofrece un enfoque simple y manejable para la administración de acceso que es menos propenso a errores que asignar permisos a los usuarios individualmente.  Al utilizar RBAC para la gestión de roles, se analizan las necesidades de los usuarios y los agrupa en roles basados en responsabilidades comunes. A continuación, se asigna uno o más roles a cada usuario y uno o más permisos a cada rol. Las relaciones usuario-rol y permisos-rol facilitan la realización de asignaciones de usuarios, ya que los usuarios ya no necesitan ser administrados individualmente, sino que tienen privilegios que se ajustan a los permisos asignados a sus roles.  Fuente: Auth0 <https://auth0.com/docs/manage-users/access-control/rbac>  **Red privada virtual (VPN)**: Una red privada virtual, o VPN, es una conexión encriptada a través de Internet desde un dispositivo a una red. La conexión cifrada ayuda a garantizar que los datos sensibles se transmitan de forma segura. Evita que personas no autorizadas escuchen el tráfico y permite al usuario realizar el trabajo de forma remota. La tecnología VPN es ampliamente utilizada en entornos corporativos.  Fuente: Cisco <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>  **Protocolo de escritorio remoto (RDP):** Remote Desktop Protocol (RDP), es un protocolo de comunicación de red seguro ofrecido por Microsoft, que permite a los usuarios ejecutar operaciones remotas en otros equipos. Facilita el intercambio seguro de información entre máquinas conectadas remotamente a través de un canal de comunicación encriptado.  Fuente: SolarWinds <https://www.solarwinds.com/resources/it-glossary/remote-desktop-protocol>  Autenticación **multifactor (MFA): La autenticación** multifactor (MFA) es un método de autenticación que requiere que el usuario proporcione dos o más factores de verificación para obtener acceso a un recurso, por ejemplo 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 (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> | |
| Recursos (vídeos, enlace de referencia) | |  | |
| Proporcionado por | | IWS | |
| Bibliografía | | 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>  OECD (2021), The Digital Transformation of SMEs, OECD Studies on SMEs and Entrepreneurship, OECD Publishing, Paris, <https://doi.org/10.1787/bdb9256a-en>.  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/>  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 | |
| PPT relacionado | | MICRO2\_ Training course\_PPT\_WP3\_Cybersecurity\_ES.pptx | |
| Materiales relacionados | |  | |