Ciberseguridad básica

Sku: PC727

Horas: 60

Formato: HTML

OBJETIVOS

Adquirir los conocimientos y habilidades básicos necesarios para protegerse de las amenazas en el entorno digital, garantizando la seguridad de los equipos informáticos en términos de integridad, autenticidad y disponibilidad de la información digital.

CONTENIDOS

Introducción a la ciberseguridad.

Para comenzar.

En esta lección introductoria, descubrirás qué es la ciberseguridad y por qué es esencial hoy en día tanto para personas como para organizaciones. Conocerás sus conceptos fundamentales, los retos principales y cómo este curso te ayudará a protegerte en el mundo digital. ¡Prepárate para iniciarte en el apasionante universo de la ciberseguridad!

Introducción a la ciberseguridad.

Esta experiencia de aprendizaje combina teoría y reflexión para garantizar una comprensión sólida de los conceptos clave de seguridad informática. Los participantes serán capaces de definir y diferenciar los conceptos de integridad, autenticidad y disponibilidad en la seguridad informática, comprendiendo su importancia y aplicabilidad en entornos digitales.

Ciberseguridad en datos.

Esta experiencia de aprendizaje proporciona un enfoque integral sobre la ciberseguridad en datos, combinando teoría, juego interactivo y reflexión para garantizar una comprensión sólida del tema. Los participantes serán capaces de comprender los principios fundamentales de la ciberseguridad en datos, identificando amenazas, vulnerabilidades y

mejores prácticas para proteger la información digital.

Decálogo básico de ciberseguridad.

Esta experiencia de aprendizaje proporciona un enfoque práctico y claro para que los participantes adopten hábitos seguros en su vida digital. Los participantes serán capaces de comprender y aplicar un conjunto de diez principios fundamentales para mantener la seguridad en entornos digitales, reduciendo riesgos y fortaleciendo su protección frente a amenazas cibernéticas.

Principales riesgos y amenazas de los entornos digitales.

Esta experiencia de aprendizaje brinda un enfoque integral sobre los riesgos en entornos digitales, ayudando a los participantes a reconocer y enfrentar las amenazas cibernéticas de manera efectiva. Los participantes serán capaces de identificar y comprender los principales riesgos y amenazas en entornos digitales, así como aplicar estrategias para mitigar su impacto y fortalecer la seguridad informática.

Vulnerabilidades.

Esta experiencia de aprendizaje proporciona un enfoque claro sobre las vulnerabilidades en entornos digitales, ayudando a los participantes a identificar y comprender las principales vulnerabilidades en entornos digitales, así como aplicar estrategias para mitigarlas y fortalecer la seguridad informática.

Otros ciberataques.

Esta experiencia de aprendizaje proporciona un enfoque detallado sobre ciberataques avanzados, ayudando a los participantes a identificar y comprender diversos tipos de ciberataques más allá del phishing y malware común, analizando sus impactos y estrategias de mitigación.

Ejercicio práctico de libre expresión escrita.

En esta lección tendrás la oportunidad de poner en práctica tus conocimientos sobre ciberseguridad de manera creativa y reflexiva. A través de ejercicios de escritura, analizarás situaciones reales y compartirás tus propias ideas, opiniones y propuestas de mejora para responder a desafíos actuales relacionados con la protección digital.

Exprésate con libertad, utiliza ejemplos originales y demuestra tu capacidad para aplicar lo aprendido a distintos contextos del mundo digital. Estos ejercicios están diseñados para desarrollar tu pensamiento crítico, así como tu habilidad para comunicar conceptos clave de la ciberseguridad de forma clara y estructurada.

Role playing y estado de avance

En esta lección de repaso, tendrás la oportunidad de reforzar los conceptos principales estudiados en la unidad sobre la ciberseguridad. Primero, podrás repasar términos clave y conceptos importantes con una serie de tarjetas didácticas (flashcards). Después, pondrás en práctica tus conocimientos participando en una simulación interactiva de rol, viviendo una situación realista donde deberás aplicar lo aprendido. Aprovecha esta lección para consolidar y comprobar todo lo que has aprendido antes de pasar a la evaluación de la unidad.

Evaluación de la unidad.

En esta lección pondrás a prueba tus conocimientos sobre los conceptos fundamentales de la ciberseguridad que has aprendido en esta unidad. Responde cada pregunta con atención y evalúa tu comprensión de los temas clave para afianzar tus conocimientos.

¡Buena suerte y sigue avanzando hacia una mayor seguridad digital!

Protección de sistemas, dispositivos y contenidos digitales.

Para comenzar.

En esta lección introductoria descubrirás los conceptos fundamentales de la protección de sistemas, dispositivos y contenidos digitales. Aprenderás por qué la ciberseguridad es esencial en el mundo actual, reconocerás las diferentes áreas que abarca y conocerás ejemplos cotidianos de amenazas y buenas prácticas. Al finalizar, estarás preparado para profundizar en cada tema en las próximas lecciones.

Seguridad en los sistemas operativos.

Los estudiantes conocerán la importancia de proteger los sistemas operativos que utilizan a diario, identificando los principales riesgos y aprenderán a seleccionar herramientas y mecanismos adecuados, como la autenticación multifactor, el cifrado y el control de accesos. Esta actividad les permitirá comprender los conceptos básicos y prepararse para aplicar medidas de seguridad esenciales en sus propios dispositivos.

Seguridad en las aplicaciones.

Los estudiantes explorarán cómo proteger las aplicaciones que utilizan en sus dispositivos y redes, reconociendo prácticas clave para prevenir vulnerabilidades, aplicarán protocolos de seguridad y aprenderán a configurar permisos y controles de acceso de forma segura. Esta actividad inicial les permitirá comprender la importancia de gestionar adecuadamente la seguridad en las aplicaciones que usan a diario.

Seguridad en los datos.

Los estudiantes conocerán la importancia de proteger y respaldar sus datos para garantizar la continuidad de los sistemas digitales. Detectando los riesgos asociados a la pérdida de información, aprenderán a ejecutar procedimientos de respaldo y recuperación, y explorarán el uso de software de protección como antivirus, firewalls e IDS/IPS para mitigar amenazas. Esta actividad les motivará a aplicar buenas prácticas de seguridad en la gestión de sus datos.

Seguridad de la información.

Los estudiantes abordarán la importancia de proteger la información en los sistemas digitales. Conocerán los conceptos clave de la seguridad de la información, practicarán procedimientos de respaldo y recuperación, y explorarán el uso de herramientas de protección como antivirus, firewalls e IDS/IPS para reducir riesgos. Esta actividad les ayudará a comprender la relevancia de mantener la confidencialidad, integridad y disponibilidad de la información.

Ejercicio práctico de libre expresión escrita.

En esta lección tendrás la oportunidad de reflexionar de forma original y creativa sobre los temas clave de la protección de sistemas, dispositivos y contenidos digitales. Se te propondrán actividades de escritura en las que podrás expresar tus opiniones, experiencias y posibles recomendaciones personales relacionadas con la ciberseguridad.

El objetivo es que conectes los conceptos fundamentales adquiridos en la unidad con situaciones reales, valorando la importancia de las buenas prácticas y la adaptación de las medidas de protección a distintos contextos y necesidades. Aprovecha esta oportunidad para desarrollar tu pensamiento crítico y tu capacidad de comunicar eficazmente tus ideas sobre ciberseguridad.

Role playing y estado de avance.

En esta lección de repaso podrás consolidar y poner a prueba los conocimientos clave adquiridos sobre la protección de sistemas, dispositivos y contenidos digitales. Comenzarás reforzando tus aprendizajes con tarjetas de memoria en formato flashcards, cubriendo los conceptos más esenciales del módulo. A continuación, participarás en un roleplay interactivo que simula situaciones prácticas relacionadas con la ciberseguridad, de modo que integres lo aprendido y desarrolles confianza para aplicar medidas de protección en casos reales.

Esta es una excelente oportunidad para afianzar los conceptos antes de pasar a la evaluación, identificar aspectos que requieran repaso y progresar hacia un dominio sólido de la ciberseguridad básica.

Evaluación de la unidad

Esta evaluación te permitirá comprobar los conocimientos adquiridos en la unidad sobre la protección de sistemas, dispositivos y contenidos digitales. Encontrarás preguntas sobre los conceptos clave: seguridad en sistemas operativos, aplicaciones, datos y la información en general. Lee atentamente cada pregunta y selecciona la opción que consideres correcta según lo aprendido.

No olvides que puedes regresar a las preguntas anteriores si es necesario. Intenta responder todas antes de finalizar la prueba. ¡Mucho éxito!

Protección de datos personales y su privacidad

Para comenzar.

En esta lección introductoria descubrirás los conceptos clave sobre la protección de datos personales y la privacidad en el entorno digital. Aprenderás por qué es fundamental proteger tu información, cuáles son los principales riesgos, y qué aprenderás a lo largo del módulo. Además, podrás ponerte a prueba con unas preguntas sencillas para asegurarte de que comprendes los conceptos básicos antes de continuar.

Fundamentos de la privacidad y la protección de datos personales.

Los estudiantes explorarán los conceptos fundamentales de la privacidad y la protección de datos personales, analizando cómo diferentes estrategias de seguridad impactan en la protección de la información tanto en entornos digitales como físicos. Reflexionarán sobre la importancia de mantener la confidencialidad, integridad y disponibilidad de los datos, y se prepararán para identificar riesgos y aplicar medidas efectivas para resguardar su privacidad.

Identificación de riesgos para la privacidad en el entorno digital.

Los estudiantes analizarán los principales riesgos que amenazan la privacidad en el entorno digital, como el robo de datos y la suplantación de identidad. Reflexionarán sobre cómo distintas herramientas y protocolos de seguridad ayudan a prevenir estos riesgos y compararán su efectividad, preparándose para tomar decisiones informadas en la protección de sus datos personales.

Medidas de protección de datos personales.

Los estudiantes analizarán diversas medidas de protección de datos personales, evaluando su efectividad en diferentes contextos. Desarrollarán recomendaciones fundamentadas para mejorar las estrategias de seguridad en la gestión de la información personal, promoviendo prácticas responsables y seguras en entornos digitales.

Herramientas y tecnologías claves para proteger la privacidad.

Los estudiantes explorarán diversas herramientas y tecnologías clave para proteger la privacidad en entornos digitales. Analizarán su funcionamiento y efectividad, con el objetivo de proponer recomendaciones basadas en evidencia que mejoren las estrategias de seguridad en la gestión de datos personales.

Desarrollo de habilidades para la toma de decisiones informadas sobre privacidad.

Los estudiantes desarrollarán habilidades para tomar decisiones informadas sobre la protección de su privacidad en entornos digitales. Analizarán escenarios prácticos, identificarán riesgos y evaluarán diferentes opciones para gestionar su información personal de manera segura. Al finalizar, propondrán recomendaciones fundamentadas que mejoren sus estrategias de privacidad y seguridad en el uso de plataformas y servicios digitales.

Ejercicio práctico de libre expresión escrita.

En esta lección tendrás la oportunidad de reflexionar y expresarte libremente sobre los conceptos esenciales relacionados con la protección de datos personales y la privacidad en el entorno digital. Pondrás en práctica tus conocimientos, analizando situaciones reales y proponiendo soluciones utilizando tu creatividad, espíritu crítico y experiencia personal.

Los ejercicios permitirán que desarrolles habilidades para identificar riesgos, evaluar medidas de protección y comunicar buenas prácticas, reforzando así lo aprendido durante la

unidad.

Role playing y estado de avance.

En esta lección de repaso, tendrás la oportunidad de revisar los conceptos clave sobre la protección de datos personales y la privacidad en el entorno digital, utilizando tarjetas de aprendizaje (flashcards) para consolidar tu memoria. Después, pondrás en práctica tus conocimientos en un ejercicio de roleplay interactivo donde asumirás un rol dentro de una situación práctica de privacidad y protección de datos. Prepara tus conocimientos para avanzar hacia la evaluación de la unidad consolidando lo aprendido en actividades participativas e interactivas.

Evaluación de la unidad.

En esta evaluación comprobarás tu comprensión sobre los conceptos principales de la protección de datos personales y la privacidad en el entorno digital. Responde a las preguntas seleccionando la opción correcta según los conocimientos adquiridos en la unidad.

Este test te ayudará a repasar y consolidar los puntos clave relacionados con riesgos, herramientas, normativas y buenas prácticas de privacidad digital.

Protección de la salud, el bienestar y el entorno.

Para comenzar.

En esta lección introductoria conocerás por qué la protección de la salud, el bienestar y el entorno es fundamental en el ámbito de la ciberseguridad. Descubrirás de forma sencilla los principales riesgos y aprenderás cómo la tecnología puede influir en tu vida diaria, tanto de manera positiva como negativa. ¡Prepárate para adquirir los conocimientos iniciales que te ayudarán a avanzar en este módulo!

Comprensión de los riesgos para la salud.

Los estudiantes identificarán los principales riesgos que el uso de la tecnología puede generar en la salud, como el ciberacoso, la adicción a las redes sociales y el síndrome de la vista cansada. Reflexionarán sobre cómo estos riesgos afectan distintos entornos y analizarán estrategias para equilibrar los beneficios y los posibles impactos negativos en la adopción tecnológica.

Comprensión de los riesgos para el bienestar.

Los estudiantes analizarán los riesgos que el uso inadecuado de la tecnología puede generar en el bienestar, como la fatiga digital, la pérdida de privacidad y la discriminación en entornos digitales. Reflexionarán sobre estas problemáticas y se prepararán para proponer soluciones innovadoras que promuevan un uso responsable y equilibrado de la tecnología, cuidando el bienestar de los usuarios.

Comprensión de los riesgos para el entorno.

Los estudiantes explorarán los riesgos que el uso de la tecnología puede generar en el entorno, como el consumo excesivo de energía, la contaminación digital y el impacto social. Reflexionarán sobre estas problemáticas y se prepararán para elaborar guías o protocolos que fomenten un uso seguro, responsable y sostenible de las tecnologías emergentes.

Adopción de medidas de protección para la salud, el bienestar y el entorno

Los estudiantes reflexionarán sobre los riesgos que el uso de la tecnología puede generar en su salud, bienestar y entorno. A partir de un diagnóstico de su entorno inmediato, identificarán problemas como el uso excesivo de pantallas o el consumo ineficiente de energía, y propondrán acciones concretas para mitigarlos. Esta actividad los preparará para diseñar estrategias de implementación tecnológica que integren criterios de ciberseguridad, privacidad y sostenibilidad.

Ejercicio práctico de libre expresión escrita

En esta lección, tendrás la oportunidad de reflexionar y expresar tus ideas sobre temas clave relacionados con la protección de la salud, el bienestar y el entorno digital. A través de ejercicios de escritura creativa y crítica, podrás aplicar los conocimientos adquiridos en la unidad y proponer soluciones o compartir experiencias propias.

Estos ejercicios están diseñados para fomentar la reflexión personal, la creatividad y el desarrollo de una conciencia digital responsable y sostenible. ¡Deja volar tu imaginación y comparte tus ideas originales!

Role playing y estado de avance.

En esta lección de repaso, consolidarás los conocimientos adquiridos sobre la protección de la salud, el bienestar y el entorno en el uso de la tecnología. Comenzarás con una actividad de tarjetas para reforzar conceptos clave y posteriormente pondrás en práctica lo aprendido a través de un roleplay interactivo en un contexto realista de seguridad digital.

Esta lección está diseñada para ayudarte a identificar áreas de mejora y reforzar la aplicación práctica de estrategias de ciberseguridad orientadas al cuidado personal, el bienestar digital y la sostenibilidad en el entorno tecnológico.

Evaluación de la unidad.

En esta evaluación comprobarás tus conocimientos sobre los riesgos asociados al uso de la tecnología en la salud, el bienestar y el entorno, así como las mejores prácticas para protegerte y actuar de manera responsable, ética y sostenible. Las preguntas abarcan conceptos clave y estrategias prácticas vistas en esta unidad.

Lee atentamente cada pregunta y selecciona la opción más adecuada según lo aprendido. ¡Éxito!

Evaluación final.

Evaluación final.

En esta evaluación final podrás comprobar tus conocimientos sobre los conceptos, riesgos, buenas prácticas y herramientas clave de la ciberseguridad vistos en todo el curso. Encontrarás preguntas cerradas, así como ejercicios donde tendrás la oportunidad de reflexionar y aplicar lo aprendido en casos y situaciones prácticas. Lee bien cada pregunta antes de responder y confirma tus respuestas antes de avanzar. ¡Éxito en tu evaluación final!