Curso de Ciberseguridad para la Educación Preuniversitaria

Elaborado por:
Direccion de Tecnologia Educativa
MINED.OC 2024

Work in progress

Descripción general

Este curso te brinda los conocimientos básicos de la ciberseguridad, incluyendo los conceptos fundamentales, las principales amenazas y ataques cibernéticos, y las mejores prácticas para proteger tus datos e información personal. Aprenderás sobre la importancia de mantener tus dispositivos y cuentas seguras, cómo identificar y prevenir ataques de phishing, y cómo navegar de manera segura por internet. Además, conocerás las herramientas y técnicas utilizadas por los profesionales de la ciberseguridad para proteger la información de individuos y organizaciones.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Introducción a la ciberseguridad

¿Qué es la Ciberseguridad?

La Ciberseguridad se refiere a la protección de los sistemas informáticos y de redes contra amenazas cibernéticas, como el acceso no autorizado, el robo de datos y el malware. En un mundo cada vez más digitalizado, la Ciberseguridad se ha vuelto fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información.

Importancia de la Ciberseguridad

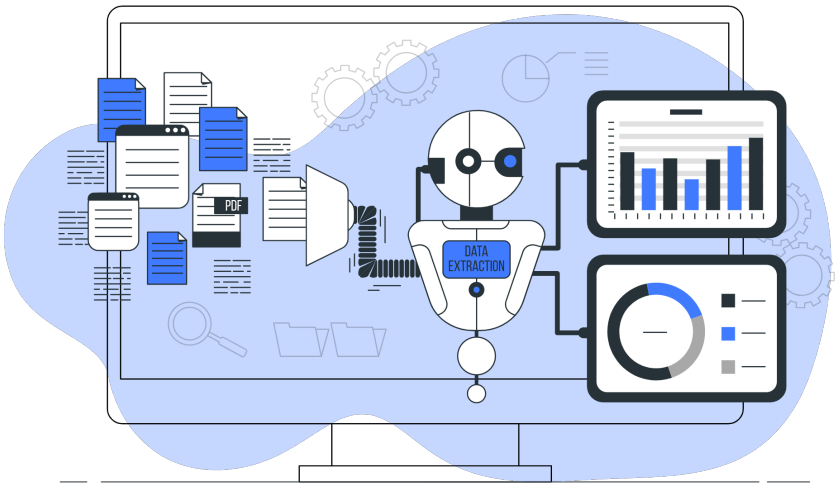
En la era digital, la información se ha convertido en uno de los activos más valiosos de una organización. La pérdida, divulgación o manipulación no autorizada de esta información puede tener consecuencias devastadoras. La Ciberseguridad desempeña un papel clave al proteger los sistemas y datos de las organizaciones, previniendo pérdidas financieras, reputacionales y legales.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Tipos de Amenazas Cibernéticas

Existen diferentes tipos de amenazas cibernéticas que pueden comprometer la seguridad de los sistemas informáticos y las redes. Algunos ejemplos comunes son:

1. **Malware:** software malicioso diseñado para dañar o acceder de manera no autorizada a los sistemas.
2. **Ataques de phishing:** intentos de engañar a los usuarios para que revelen información confidencial, como contraseñas o números de tarjeta de crédito.
3. **Ataques de fuerza bruta:** intentos de adivinar contraseñas mediante la prueba de diferentes combinaciones.
4. **Ataques de denegación de servicio (DoS):** sobrecarga intencional de un sistema o red para que no pueda responder a las solicitudes legítimas.

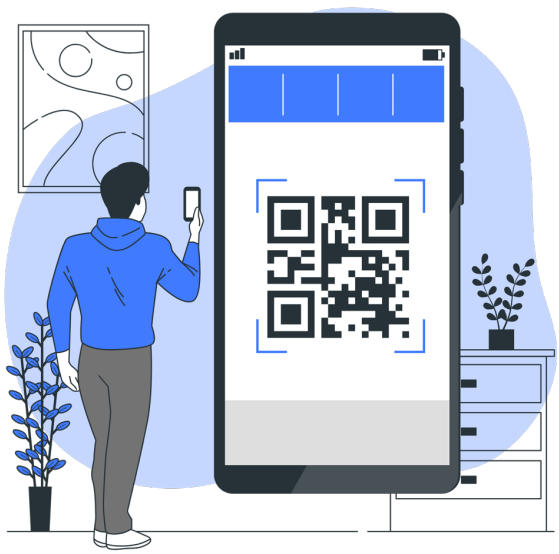


MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Principales Objetivos de la Ciberseguridad

La Ciberseguridad tiene una serie de objetivos principales que se buscan alcanzar para proteger los sistemas y datos de una organización:

1. **Confidencialidad:** asegurar que la información solo sea accesible por personas autorizadas.
2. **Integridad:** garantizar que la información no sea modificada o alterada de manera no autorizada.
3. **Disponibilidad:** asegurar que la información y los sistemas estén disponibles cuando se necesiten.
4. **Autenticidad:** verificar la identidad de los usuarios y asegurar que sean quienes dicen ser.
5. **No repudio:** garantizar que una vez que un usuario ha realizado una acción, no pueda negar haberlo hecho.

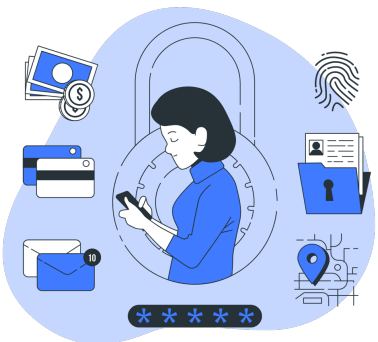


MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Medidas de Protección en Ciberseguridad

Existen una serie de medidas de protección que se pueden implementar para garantizar la seguridad de los sistemas y datos:

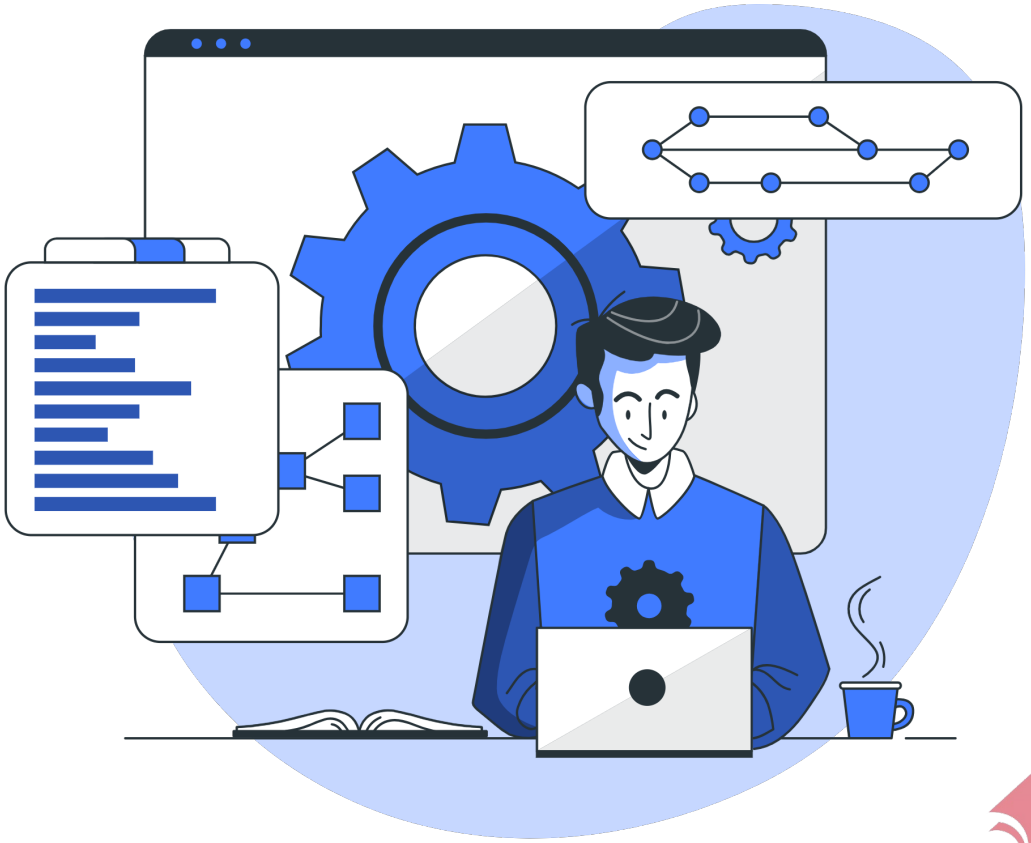
1. **Uso de contraseñas seguras:** utilizar contraseñas complejas y únicas para cada cuenta.
2. **Actualización de software:** mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
3. **Cortafuegos y antivirus:** utilizar software de protección para detectar y bloquear amenazas cibernéticas.
4. **Copias de seguridad:** realizar copias de seguridad regularmente para protegerse contra la pérdida de datos.
5. **Educación y Concientización:** capacitar a los usuarios sobre las mejores prácticas de seguridad y cómo identificar amenazas cibernéticas.



MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Conclusiones

La Ciberseguridad es esencial en la actualidad para proteger los sistemas informáticos y las redes de las organizaciones de las amenazas cibernéticas. Con el aumento de la digitalización y la dependencia de la información, es fundamental implementar medidas de protección adecuadas y fomentar una cultura de seguridad. La comprensión de las amenazas cibernéticas más comunes y los objetivos de la Ciberseguridad ayudarán a garantizar la protección de los sistemas y datos en un mundo cada vez más conectado.



MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Fundamentos de la seguridad informática

La seguridad informática es un área crucial en el mundo actual, donde la tecnología juega un papel fundamental en todas las esferas de nuestra sociedad. Con el incremento de amenazas cibernéticas, es esencial comprender los fundamentos de la seguridad informática para proteger de manera efectiva nuestros sistemas y datos.

En este módulo, exploraremos los principales conceptos y fundamentos en seguridad informática que todo profesional debe conocer. No solo nos enfocaremos en los aspectos técnicos, sino también en los aspectos legales y éticos asociados a la seguridad informática.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Temas clave a cubrir:

1. Amenazas cibernéticas

- Tipos de amenazas cibernéticas: Malware, hacking, ingeniería social, robo de identidad, entre otros.
- Impacto económico y social de las amenazas cibernéticas.
- Ejemplos de ataques cibernéticos famosos.

2. Principios de seguridad informática

- Confidencialidad, integridad y disponibilidad de la información.
- Autenticación y autorización de usuarios.
- No repudio y privacidad de la información.
- Principio de mínimos privilegios.

3. Criptografía

- Conceptos básicos de criptografía: cifrado simétrico y asimétrico.
- Algoritmos criptográficos comunes: AES, RSA, ECC.
- Uso de certificados y firmas digitales.
- Protección de la información en tránsito y en reposo.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

4. Seguridad en redes

- Firewalls y sistemas de detección de intrusiones (IDS).
- Arquitecturas seguras: DMZ, VPN.
- Protocolos seguros: SSL/TLS, SSH.
- Protección contra ataques de denegación de servicio (DDoS).

5. Gestión de riesgos

- Evaluación de riesgos y análisis de vulnerabilidades.
- Planificación y implementación de medidas de seguridad.
- Roles y responsabilidades en la gestión de la seguridad informática.

6. Legislación y ética en seguridad informática

- Normativas y leyes que regulan la seguridad informática a nivel internacional y nacional.
- Responsabilidades legales y éticas de los profesionales de la seguridad informática.
- Protección de la privacidad y datos personales.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Conclusiones

En conclusión, comprender los fundamentos de la seguridad informática es fundamental para garantizar la protección de nuestros sistemas y datos en un mundo cada vez más dependiente de la tecnología. Este módulo nos proporcionará las bases necesarias para entender y gestionar los riesgos cibernéticos, así como para fomentar una cultura de seguridad en las organizaciones y en nuestra sociedad en general.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Protección contra amenazas cibernéticas

Introducción

En el mundo actual, las amenazas cibernéticas son una preocupación constante para individuos y organizaciones. Los delincuentes informáticos están constantemente desarrollando nuevas formas de atacar sistemas, robar datos sensibles y comprometer la seguridad en línea. Por lo tanto, es esencial adoptar medidas de protección adecuadas para salvaguardar nuestra información y mantenernos a salvo en el entorno digital. En este tema, exploraremos las principales amenazas cibernéticas y las estrategias de protección que podemos implementar.

Amenazas Cibernéticas Comunes

1. Malware

El malware, abreviatura de software malicioso, es una de las amenazas cibernéticas más frecuentes y peligrosas. Se trata de programas diseñados para dañar, infiltrarse o controlar un sistema informático sin el conocimiento o consentimiento del usuario. Los tipos comunes de malware incluyen virus, ransomware, gusanos y troyanos. Estos pueden ser distribuidos a través de enlaces o archivos adjuntos maliciosos, y una vez instalados en nuestro dispositivo, pueden causar daños significativos, como el robo de datos, el bloqueo del sistema o el espionaje.

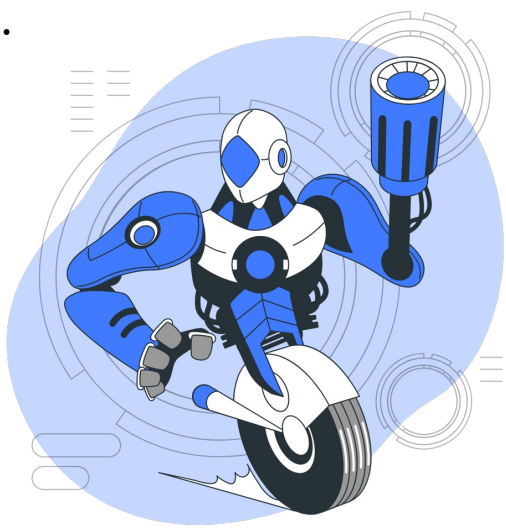
MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

2. Phishing

El phishing es una técnica utilizada por los ciberdelincuentes para engañar a los usuarios y obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales. Por lo general, se realiza a través de correos electrónicos fraudulentos o sitios web falsos que imitan a organizaciones legítimas. Estos mensajes o páginas web intentan convencernos de que brindemos información confidencial, como iniciar sesión en una cuenta o realizar un pago. Es fundamental ser cauteloso y verificar cuidadosamente la autenticidad de los mensajes y los sitios web antes de proporcionar cualquier dato personal.

3. Ataques de Denegación de Servicio (DDoS)

Los ataques de denegación de servicio (DDoS) tienen como objetivo inundar un sistema, red o sitio web con un gran volumen de tráfico, lo que provoca una saturación y la imposibilidad de atender a las solicitudes legítimas de los usuarios. Los atacantes suelen utilizar una botnet, una red de dispositivos comprometidos, para enviar esta gran cantidad de tráfico hacia el objetivo seleccionado. Estos ataques pueden causar interrupciones en los servicios en línea y afectar la disponibilidad o rendimiento de sitios web y sistemas.



MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Estrategias de Protección Cibernética

1. Utilizar Software de Seguridad

Es fundamental contar con un software de seguridad actualizado en nuestros dispositivos, como antivirus y cortafuegos. Estas herramientas ayudan a detectar y prevenir la instalación de malware, así como a bloquear actividades sospechosas y mantener la integridad de nuestro sistema. Es importante mantener estos programas actualizados y realizar escaneos periódicos para garantizar una protección continua.

2. Fortalecer Contraseñas

El uso de contraseñas seguras y únicas para nuestras cuentas en línea es esencial para proteger nuestros datos. Se deben utilizar combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales, evitando palabras o secuencias predecibles. Además, se recomienda utilizar distintas contraseñas para cada cuenta y cambiarlas regularmente.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

3. Actualizar el Software de forma Regular

Es crucial mantener actualizado el software de nuestros dispositivos, incluyendo los sistemas operativos y las aplicaciones. Las actualizaciones suelen incluir correcciones de seguridad que solucionan vulnerabilidades conocidas. Ignorar las actualizaciones puede dejar nuestros dispositivos expuestos a posibles ataques. Configurar las actualizaciones automáticas es una opción recomendada para garantizar una protección constante.

4. Capacitación y Concientización

La educación y la capacitación son componentes clave de la protección cibernética. Debemos aprender a identificar las señales de alerta de amenazas cibernéticas, como correos electrónicos sospechosos o sitios web no seguros. Al estar informados sobre las últimas técnicas utilizadas por los delincuentes y comprender las mejores prácticas de seguridad en línea, podemos evitar caer en trampas y proteger nuestra información.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

5. Copias de Seguridad Regulares

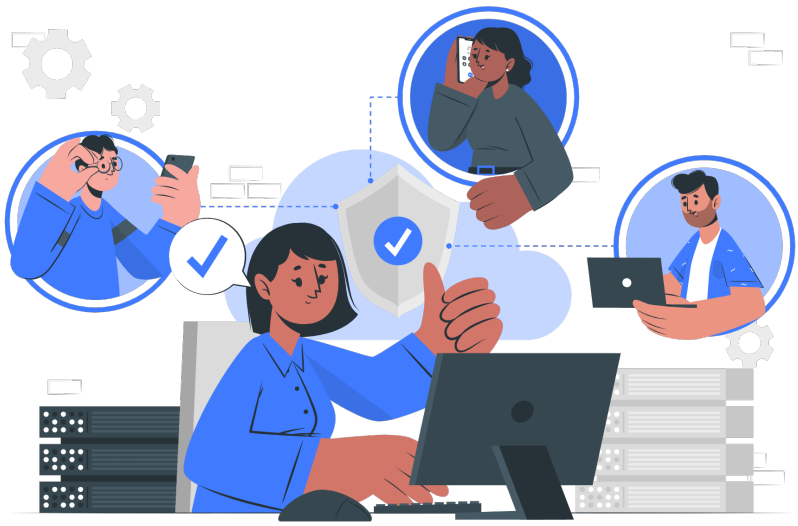
Realizar copias de seguridad periódicas de nuestros datos importantes es una estrategia fundamental para protegernos contra la pérdida o destrucción de información debido a un ataque cibernético. Al mantener copias actualizadas de nuestros archivos en un dispositivo externo o en la nube, podemos recuperar los datos en caso de que sean afectados por un malware o un ataque.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Recursos de apoyo

- Sitio Web: www.osri.gob.cu/incident-reports/report-form
- Correo electrónico: reportes@osri.gob.cu
- Número único de atención a la población: 18810

Recordar que la prevención y la acción contundente contra el ciberbullying son fundamentales para garantizar un entorno en línea seguro y saludable para todos.



MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Ejercicios Prácticos

Pongamos en práctica tus conocimientos

En esta lección, pondremos la teoría en práctica a través de actividades prácticas.

Identificación de amenazas

Descripción:

Realiza una investigación en línea para identificar las principales amenazas cibernéticas a las que se enfrentan las organizaciones en la actualidad. Proporciona ejemplos específicos y describe las consecuencias que pueden tener estas amenazas.

Análisis de vulnerabilidades

Descripción:

Analiza una aplicación o sistema informático y identifica posibles vulnerabilidades de seguridad. Explica cómo podrían ser explotadas por atacantes y sugiere medidas para mitigar estos riesgos.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Diseño de política de seguridad

Descripción:

Diseña una política de seguridad cibernética para una organización. Incluye medidas de protección física y lógica, políticas y procedimientos de seguridad, y educación y concientización de los empleados. Explica cómo esta política ayudaría a proteger la organización de amenazas cibernéticas.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Prueba

Comprueba tus conocimientos respondiendo las siguientes preguntas. Marque la respuesta correcta

¿Qué es la ciberseguridad?

- La protección de sistemas informáticos contra amenazas cibernéticas
- El estudio de las redes sociales
- La prevención de enfermedades en la computadora

¿Cuáles son los principales objetivos de la seguridad informática?

- Proteger los datos de los usuarios
- Incrementar la velocidad de Internet
- Mejorar la estética de las páginas web

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

¿Qué es un ataque de phishing?

- Un ataque que impide el acceso a la red
- Un ataque en el que se engaña a las personas para obtener información confidencial
- Un ataque que apaga los dispositivos electrónicos

¿Cuál es una buena práctica para protegerse contra las amenazas cibernéticas?

- Usar contraseñas simples
- Actualizar regularmente el software
- Compartir información sensible en redes sociales

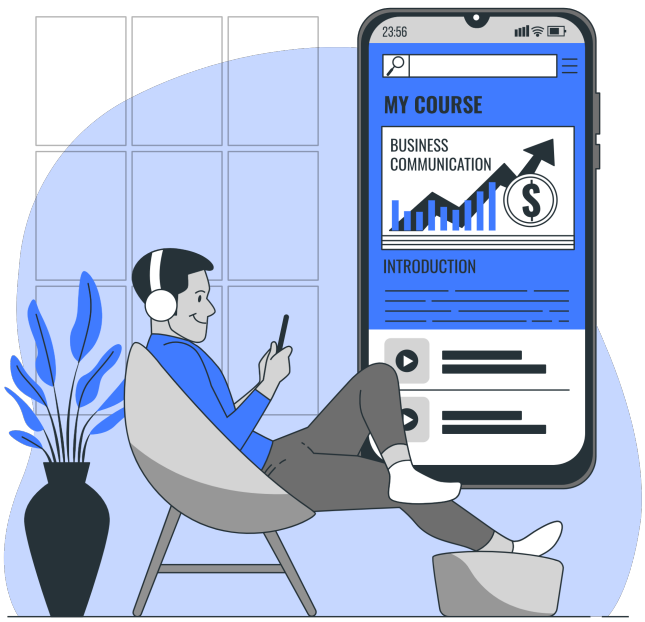
MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

¿Qué es un firewall?

- Un programa para escanear virus en el ordenador
- Un dispositivo que controla el tráfico de red y protege contra amenazas
- Una contraseña para acceder a la red

¿Qué es el ransomware?

- Un programa que permite controlar de forma remota una computadora
- Un tipo de malware que cifra los archivos y exige un rescate para desbloquearlos
- Una técnica para aumentar la velocidad de Internet



MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Felicidades!

¡Felicitaciones por completar este curso! Has dado un paso importante para desbloquear todo tu potencial. Completar este curso no se trata solo de adquirir conocimientos; se trata de poner ese conocimiento en práctica y tener un impacto positivo en el mundo que te rodea.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA