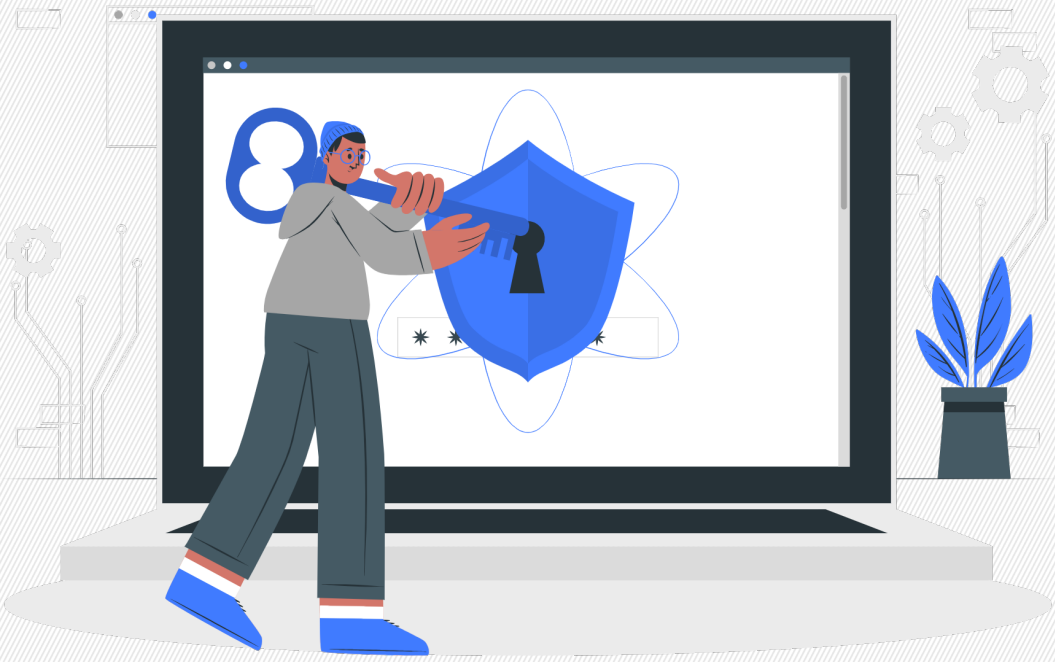


Curso de Ciberseguridad para la Educación Secundaria

Elaborado por:
Direccion de Tecnologia Educativa
MINED.OC 2024

Work in progress

Descripción general

Este curso está diseñado para estudiantes de secundaria que deseen aprender cómo protegerse en línea y mantener su información personal segura. A lo largo del curso, exploraremos los conceptos básicos de la ciberseguridad y aprenderemos sobre las distintas amenazas y riesgos en línea. También descubrirás cómo proteger tus datos y tu privacidad en redes sociales y otras plataformas en línea. ¡Únete a este curso y conviértete en un experto en ciberseguridad!

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Introducción a la ciberseguridad

La ciberseguridad es un campo crucial en el mundo tecnológico actual, y se ha convertido en una preocupación cada vez mayor para individuos y organizaciones de todo tipo. En esta sección del curso "Curso de Ciberseguridad para estudiantes de secundaria", se explorarán los conceptos básicos de la ciberseguridad y su importancia en nuestra vida diaria.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

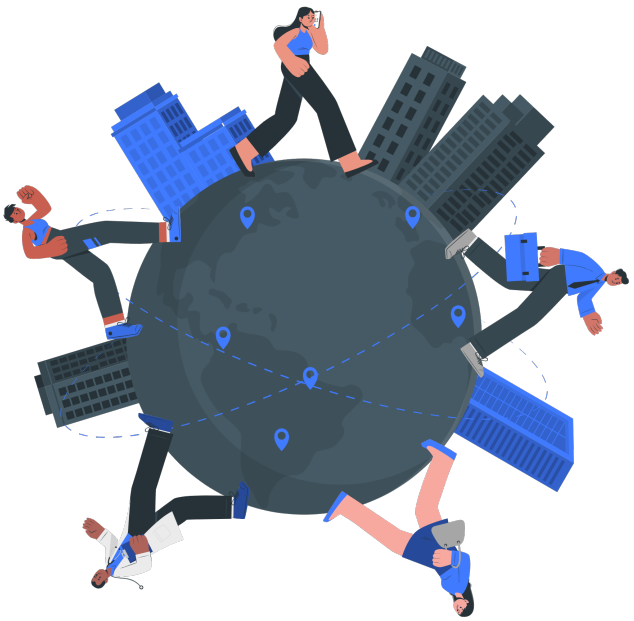
¿Qué es la ciberseguridad?

La ciberseguridad se refiere a la protección de los sistemas informáticos y de internet contra amenazas que puedan comprometer la seguridad, la privacidad y el uso adecuado de la información. Estas amenazas pueden incluir ataques cibernéticos, hacking, robo de datos, malware y muchas otras formas de actividad malintencionada en línea.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Importancia de la ciberseguridad

En la actualidad, nuestra sociedad está cada vez más conectada a través de internet. Utilizamos la tecnología para comunicarnos, estudiar, trabajar y realizar transacciones comerciales. Sin embargo, estas actividades en línea también nos exponen a riesgos y vulnerabilidades. La ciberseguridad es esencial para garantizar que nuestras actividades en línea sean seguras y protegidas.



MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Principios fundamentales de la ciberseguridad

Para comprender cómo se protegen los sistemas informáticos, es importante conocer los principios fundamentales de la ciberseguridad. Estos principios nos ayudan a establecer una base sólida para la protección de nuestros datos y sistemas:

1- **Confidencialidad:** garantizar que la información solo sea accesible a personas autorizadas.

2- **Integridad:** asegurar que la información se mantenga completa y sin alteraciones no autorizadas.

3- **Disponibilidad:** garantizar que la información y los sistemas estén disponibles cuando sean necesarios.

4- **Autenticidad:** verificar la identidad de los usuarios y asegurar la veracidad de la información.

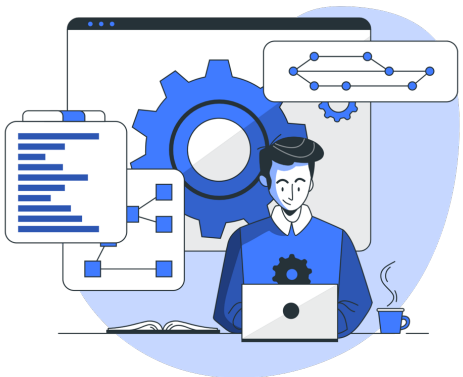
5- **No repudio:** asegurar que ninguna de las partes involucradas en una actividad en línea pueda negar su participación.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Amenazas comunes en línea

Existen varias amenazas comunes en línea que pueden comprometer nuestra seguridad y privacidad. Algunas de las amenazas más conocidas incluyen:

- **Malware:** software malicioso diseñado para dañar, bloquear o acceder ilegalmente a un sistema informático.
- **Ataques de phishing:** suplantación de identidad para engañar a las personas y obtener información confidencial, como contraseñas o datos financieros.
- **Ataques de fuerza bruta:** intentos de adivinar contraseñas o claves mediante la prueba de diferentes combinaciones hasta encontrar la correcta.
- **Ataques de denegación de servicio:** sobrecargar un sistema o red con tráfico para hacer que sea inaccesible para los usuarios legítimos.

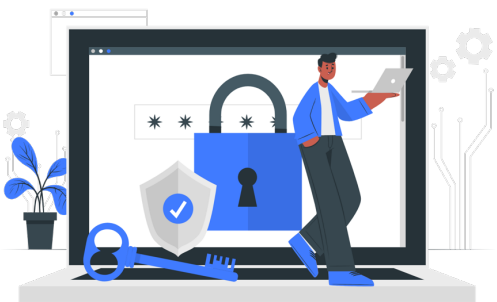


MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Medidas de seguridad en línea

Para protegernos de las amenazas en línea, es importante tomar medidas de seguridad adecuadas. Algunas de las medidas de seguridad recomendadas incluyen:

1. **Mantener el software actualizado:** instalar las últimas actualizaciones de software y parches de seguridad para mantener los sistemas protegidos contra vulnerabilidades conocidas.
2. **Utilizar contraseñas seguras:** elegir contraseñas fuertes y únicas para cada cuenta en línea y evitar compartir contraseñas con otros.
3. **Ser cauteloso con los enlaces y archivos adjuntos:** no hacer clic en enlaces desconocidos o descargar archivos adjuntos de fuentes no confiables.
4. **Utilizar un software antivirus:** instalar y mantener actualizado un buen software antivirus en todos los dispositivos.
5. **Habilitar la autenticación en dos pasos:** utilizar la autenticación en dos pasos siempre que sea posible para agregar una capa adicional de seguridad a las cuentas en línea.

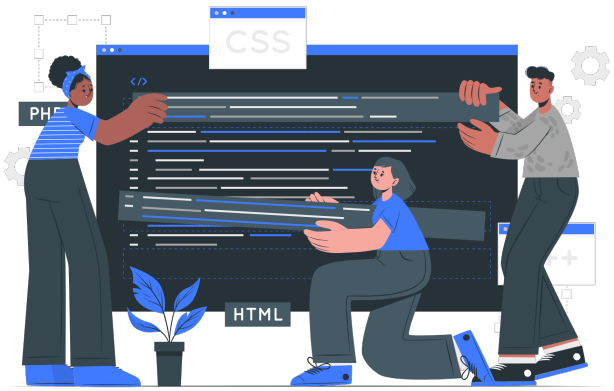


MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Conclusiones

En esta sección, hemos explorado los conceptos básicos de la ciberseguridad y su importancia en nuestra vida diaria. Hemos aprendido sobre los principios fundamentales de la ciberseguridad, las amenazas comunes en línea y las medidas de seguridad recomendadas. A medida que avancemos en este curso, profundizaremos en estos temas y exploraremos estrategias avanzadas para proteger nuestros sistemas y datos. Recuerda siempre estar consciente de la ciberseguridad y tomar las precauciones necesarias para mantenernos seguros en línea.

La ciberseguridad es un tema crucial en la sociedad actual. A través del curso de Ciberseguridad para estudiantes de secundaria, hemos aprendido los conceptos fundamentales de este campo y cómo aplicarlos en nuestra vida diaria. Ahora estamos preparados para enfrentar los desafíos de la era digital con conciencia y responsabilidad.



MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Ciberbullying y cómo prevenirlo

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Definición de ciberbullying

El ciberbullying es un tipo de acoso que involucra el uso de medios digitales, como teléfonos móviles, redes sociales, correos electrónicos y aplicaciones de mensajería instantánea, para intimidar, molestar o amenazar a una persona. A diferencia del acoso tradicional, el ciberbullying ocurre en línea y puede tener un alcance mucho mayor.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Tipos de ciberbullying

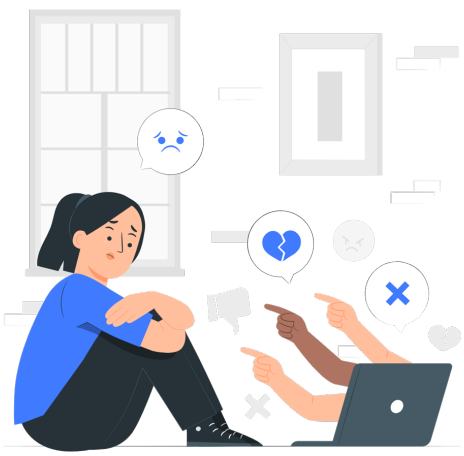
1. **Acoso verbal:** se refiere a insultos, comentarios ofensivos o difamatorios realizados a través de mensajes de texto, comentarios en redes sociales o chats en línea.
2. **Acoso social:** implica excluir a una persona de un grupo o difundir rumores falsos y vergonzosos sobre ella.
3. **Acoso sexual:** consiste en enviar imágenes o mensajes con contenido sexual no deseado, o realizar chantajes de naturaleza sexual.
4. **Suplantación de identidad:** se refiere a la creación de perfiles falsos para difamar, humillar o acosar a una persona.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Consecuencias del ciberbullying

El ciberbullying puede tener un impacto significativo en la salud emocional y psicológica de las personas afectadas. Algunas de las consecuencias más comunes son:

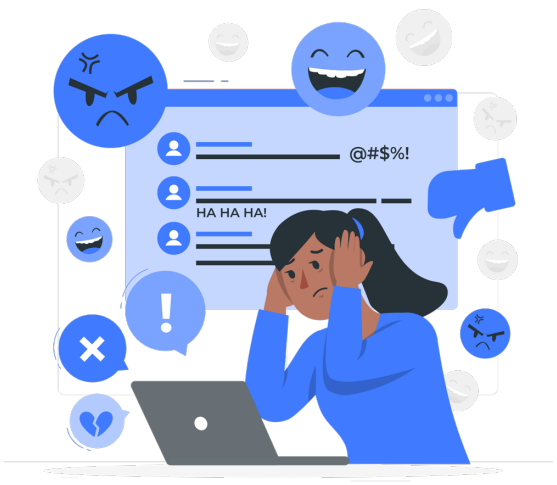
1. **Ansiedad y depresión:** las víctimas de ciberbullying pueden experimentar altos niveles de ansiedad, depresión e incluso pensamientos suicidas.
2. **Baja autoestima:** el acoso constante puede socavar la confianza y la autoestima de la persona afectada.
3. **Aislamiento social:** las víctimas pueden retirarse de las interacciones sociales y sentirse excluidas por temor a sufrir más acoso.
4. **Rendimiento académico disminuido:** el ciberbullying puede afectar negativamente el desempeño escolar de las víctimas, dificultando su concentración y motivación.



MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

¿Cómo prevenir el ciberbullying?

1. **Educación y concienciación:** es fundamental educar a los estudiantes sobre el impacto del ciberbullying y promover la empatía y el respeto por los demás.
2. **Uso responsable de la tecnología:** enseñar a los estudiantes sobre el uso responsable de la tecnología, incluyendo la importancia de proteger la privacidad y no compartir información personal en línea.
3. **Mantenerse informado:** los padres y educadores deben estar al tanto de las tendencias en línea y supervisar las actividades de los estudiantes en Internet para detectar posibles signos de ciberbullying.
4. **Crear un entorno seguro:** fomentar la creación de un entorno escolar seguro donde los estudiantes se sientan cómodos buscando ayuda si son víctimas de ciberbullying.
5. **Promover el reporte y la denuncia:** alentar a los estudiantes a reportar cualquier incidente de ciberbullying a los adultos responsables y a denunciarlo a las plataformas en línea correspondientes.

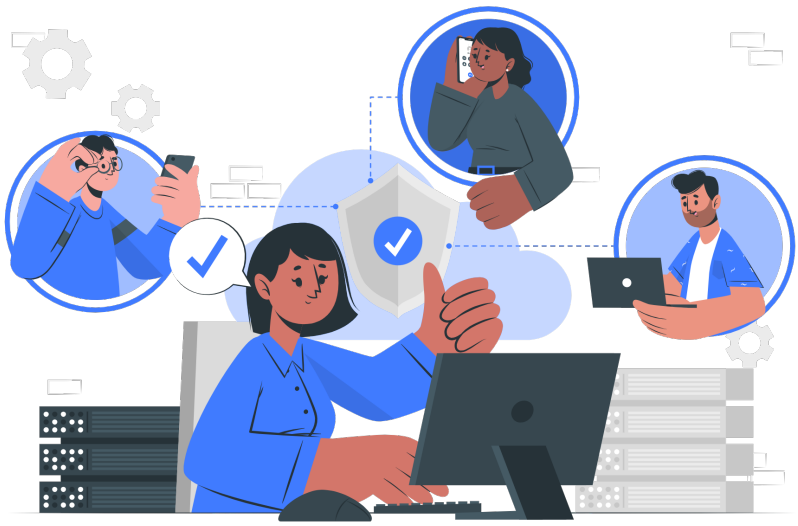


MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

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

El ciberbullying es un problema que afecta a muchos estudiantes. A lo largo del curso, hemos comprendido la importancia de prevenir y combatir esta forma de acoso. Con las herramientas y estrategias aprendidas, podemos protegernos y ayudar a nuestros compañeros a enfrentar esta situación de manera segura y eficaz.

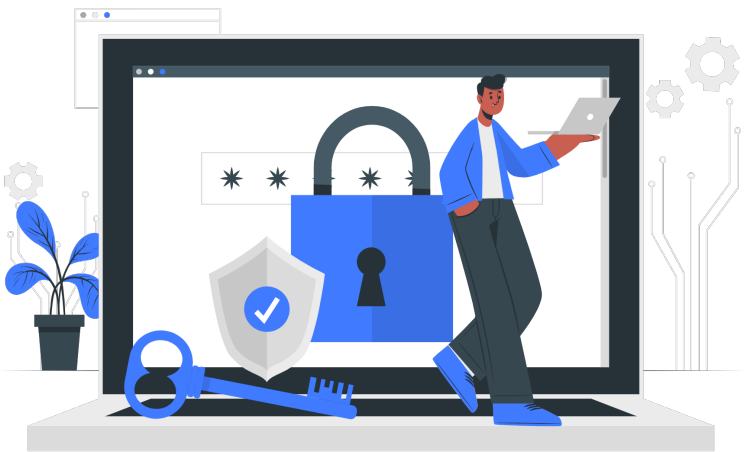
MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Prevención de ciberataques y malware

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Introducción

En la actualidad, la seguridad cibernética se ha convertido en una preocupación importante debido a la creciente amenaza de ciberataques y malware. Estos ataques pueden tener consecuencias devastadoras, como la pérdida de información, el robo de identidad y daños a la reputación. Por lo tanto, es fundamental que los estudiantes de secundaria adquieran conocimientos y habilidades en prevención de ciberataques y malware para protegerse a sí mismos y a sus dispositivos.

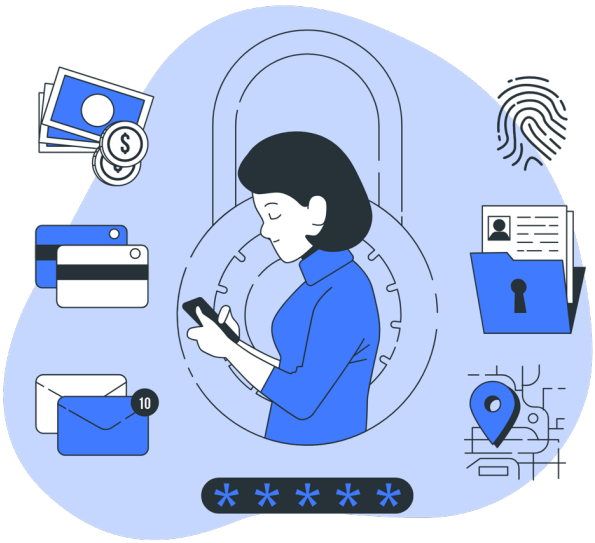


MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Seguridad en contraseñas

Una de las formas más comunes en las que se producen ciberataques es a través del robo de contraseñas. Por lo tanto, es crucial que los estudiantes aprendan a crear contraseñas seguras y a protegerlas adecuadamente. Algunas prácticas recomendadas incluyen: de ciberataques

- Utilizar contraseñas largas y complejas, que incluyan letras mayúsculas y minúsculas, números y caracteres especiales.
- Evitar el uso de contraseñas obvias, como fechas de cumpleaños o nombres de mascotas.
- No utilizar la misma contraseña para diferentes cuentas.
- Cambiar regularmente las contraseñas.



MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Actualizaciones de software y parches

Los desarrolladores de software están constantemente actualizando sus productos para corregir vulnerabilidades y mejorar la seguridad. Sin embargo, muchos usuarios no instalan estas actualizaciones debido a la falta de conocimiento o la pereza. Es esencial que los alumnos entiendan la importancia de mantener sus dispositivos y aplicaciones actualizados. Esto se puede lograr a través de las siguientes recomendaciones:

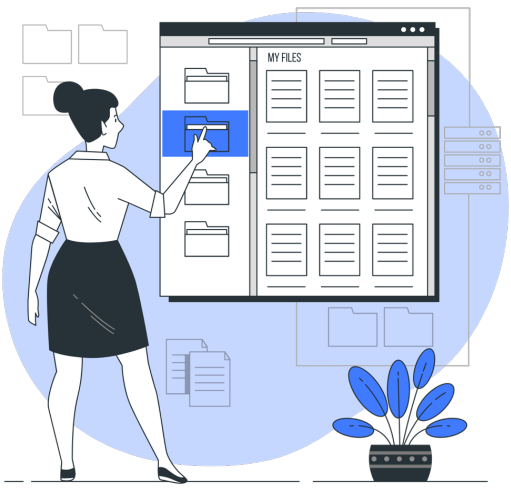
- Configurar actualizaciones automáticas en los dispositivos.
- Comprobar regularmente las actualizaciones disponibles para las aplicaciones utilizadas.
- Instalar parches de seguridad tan pronto como estén disponibles.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Phishing y correos electrónicos sospechosos

El phishing es una técnica utilizada por los ciberdelincuentes para obtener información personal sensible, como contraseñas o números de tarjetas de crédito. La identificación de correos electrónicos sospechosos y la práctica de medidas de seguridad al interactuar con ellos son esenciales para prevenir este tipo de ciberataques. Algunas recomendaciones importantes son:

- No hacer clic en enlaces ni descargar archivos adjuntos de correos electrónicos no solicitados o sospechosos.
- Verificar cuidadosamente la dirección de correo electrónico del remitente antes de proporcionar cualquier información personal.
- No proporcionar información confidencial, como contraseñas o números de tarjetas de crédito, a través de correos electrónicos o enlaces sospechosos.



MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Uso seguro de redes. Wi-Fi públicas

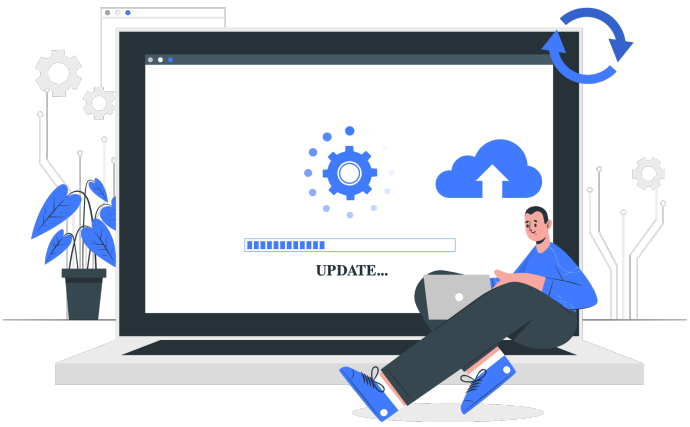
Las redes Wi-Fi públicas son convenientes pero también pueden ser inseguras. Los ciberdelincuentes pueden interceptar la información transmitida a través de estas redes y robar datos sensibles. Para evitar esto, los estudiantes deben seguir estas pautas al utilizar redes Wi-Fi públicas:

- Evitar realizar transacciones financieras o acceder a cuentas sensibles mientras se está conectado a una red Wi-Fi pública.
- Utilizar una conexión VPN (Red Privada Virtual) para cifrar la comunicación y proteger los datos transmitidos.
- Configurar ajustes de seguridad adecuados en los dispositivos, como desactivar la conexión automática a redes Wi-Fi desconocidas.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Conclusiones

La prevención de ciberataques y malware es fundamental para garantizar la seguridad en línea. Los estudiantes de secundaria deben adquirir conocimientos y habilidades en seguridad cibernética para protegerse a sí mismos y a sus dispositivos de las amenazas en línea. A través de la implementación de prácticas adecuadas, como crear contraseñas seguras, mantener el software actualizado y tener precaución al interactuar con correos electrónicos y redes Wi-Fi públicas, los estudiantes pueden reducir significativamente el riesgo de sufrir un ciberataque o una infección de malware.



MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

La prevención de ciberataques y malware es esencial para salvaguardar nuestra información personal y seguridad en línea. En este curso, hemos adquirido conocimientos sobre los diferentes tipos de ciberataques y cómo prevenirlos. Ahora tenemos las habilidades necesarias para proteger nuestros dispositivos y datos frente a posibles amenazas.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

Ejercicios Prácticos

Pongamos en práctica tus conocimientos

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

En esta lección, pondremos la teoría en práctica a través de actividades prácticas. Haga clic en los elementos a continuación para verificar cada ejercicio y desarrollar habilidades prácticas que lo ayudarán a tener éxito en el tema.

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

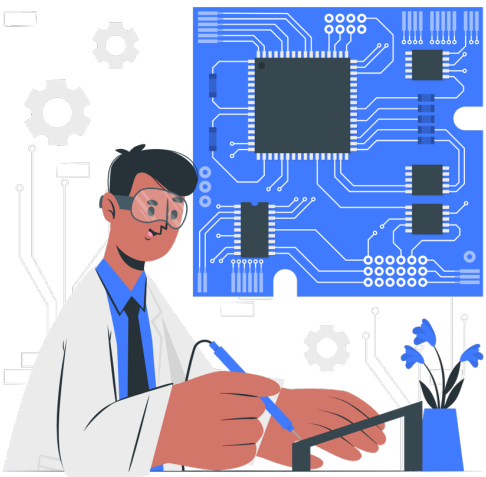
Protege tus contraseñas

En este ejercicio, aprenderás la importancia de tener contraseñas seguras y cómo protegerlas adecuadamente. Sigue los siguientes pasos: 1. Elije una contraseña segura utilizando una combinación de letras mayúsculas, minúsculas, números y símbolos. 2. Utiliza diferentes contraseñas para cada cuenta o servicio. 3. No compartas tus contraseñas con nadie. 4. Utiliza un gestor de contraseñas para almacenar de forma segura todas tus contraseñas. 5. Actualiza tus contraseñas periódicamente.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Identifica el ciberbullying

En este ejercicio, aprenderás a identificar el ciberbullying y cómo prevenirlo. Sigue los siguientes pasos: 1. Familiarízate con las diferentes formas de ciberbullying, como acosar, difamar, insultar o amenazar a alguien en línea. 2. Aprende a reconocer los signos de ciberbullying, como cambios repentinos de comportamiento, aislamiento social o negatividad extrema. 3. Crea conciencia sobre el impacto del ciberbullying y promueve una cultura de respeto y empatía en línea. 4. Aprende a tomar medidas para prevenir el ciberbullying, como bloquear y denunciar a los acosadores, y hablar con un adulto de confianza si eres víctima de ciberbullying.



MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Protege tu dispositivo

En este ejercicio, aprenderás cómo proteger tu dispositivo contra ciberataques y malware. Sigue los siguientes pasos: 1. Mantén tu dispositivo actualizado instalando las últimas actualizaciones de seguridad. 2. Utiliza un programa antivirus confiable y mantenlo actualizado. 3. Evita hacer clic en enlaces o descargar archivos adjuntos sospechosos de fuentes desconocidas. 4. Utiliza contraseñas seguras para desbloquear tu dispositivo. 5. Evita conectarte a redes Wi-Fi públicas no seguras. 6. Realiza copias de seguridad periódicas de tus datos importantes. 7. Aprende a reconocer los signos de un posible ciberataque, como un rendimiento lento del dispositivo o la aparición de ventanas emergentes no deseadas. 8. Si sospechas que tu dispositivo ha sido comprometido, desconéctalo de Internet y busca ayuda de un profesional de ciberseguridad.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

Resumen

Repasemos lo que acabamos de ver hasta ahora

La ciberseguridad es un tema crucial en la sociedad actual. A través del curso de Ciberseguridad para estudiantes de secundaria, hemos aprendido los conceptos fundamentales de este campo y cómo aplicarlos en nuestra vida diaria. Ahora estamos preparados para enfrentar los desafíos de la era digital con conciencia y responsabilidad.
El ciberbullying es un problema que afecta a muchos estudiantes. A lo largo del curso, hemos comprendido la importancia de prevenir y combatir esta forma de acoso. Con las herramientas y estrategias aprendidas, podemos protegernos y ayudar a nuestros compañeros a enfrentar esta situación de manera segura y eficaz.
La prevención de ciberataques y malware es esencial para salvaguardar nuestra información personal y seguridad en línea. En este curso, hemos adquirido conocimientos sobre los diferentes tipos de ciberataques y cómo prevenirlos. Ahora tenemos las habilidades necesarias para proteger nuestros dispositivos y datos frente a posibles amenazas.

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

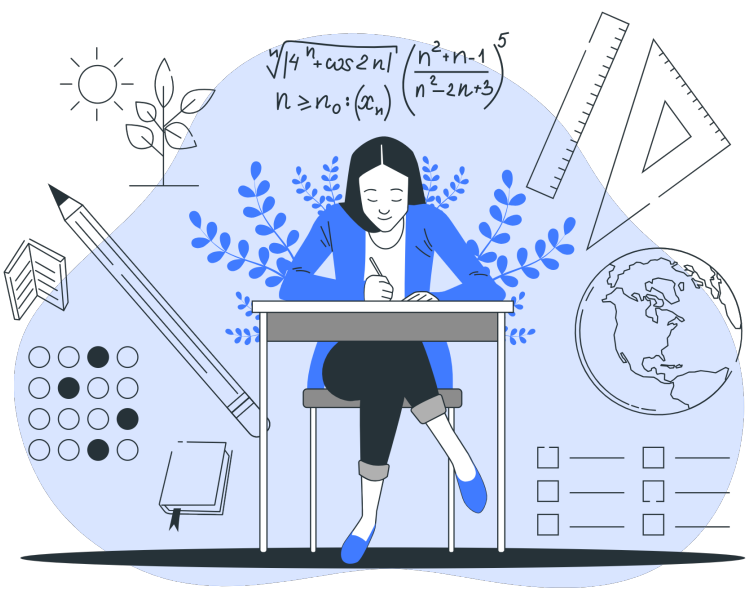
Prueba

Comprueba tus conocimientos respondiendo unas preguntas

MINISTERIO
de EDUCACIÓN
REPÚBLICA DE CUBA

¿Qué es la ciberseguridad?

- Es el conjunto de medidas para proteger la información y los sistemas informáticos
- Es el conjunto de normas para regular el uso de internet
- Es el conjunto de métodos para hackear sistemas informáticos



MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

¿Qué es el ciberbullying?

- Es el robo de contraseñas de usuarios
- Es el acoso o intimidación a través de medios electrónicos
- Es el envío de correos electrónicos no deseados

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

¿Qué es un ciberataque?

- Es la implementación de medidas de seguridad en los sistemas informáticos
- Es la propagación de virus y malware
- Es la protección de la privacidad en internet

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

¿Qué es el malware?

- Es el software que permite el acceso no autorizado a un sistema informativo
- Es el proceso de eliminación de virus de un dispositivo
- Es el conjunto de reglas de seguridad en internet

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

¿Qué es un ataque de phishing?

- Es el envío de correos electrónicos no deseados
- Es el robo de información personal a través de engaños
- Es la implementación de medidas de seguridad en los sistemas informáticos

MINISTERIO de EDUCACIÓN
REPÚBLICA DE CUBA

¿Cuál es una medida efectiva para prevenir el ciberbullying?

- No compartir información personal en línea
- Responder a los mensajes de odio
- Participar en discusiones en línea sin límites

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