




## Cuestionario

### Pregunta 1

La ciberseguridad es el esfuerzo continuo para proteger a las personas, las organizaciones y los gobiernos de los ataques digitales mediante la protección de los sistemas y datos en red contra el uso o daño no autorizados.

¿Qué nivel de ciberprotección requiere cada uno de los siguientes factores?

Su identidad en línea	
Telepresencia	
Base de datos de clientes	
Organizacional	
Estabilidad económica	
Gobierno	

## Pregunta 2

Un perfil de usuario individual en un sitio de red social es un ejemplo de una  identidad.

## Pregunta 3

Su vecino le dice que no tiene una identidad en línea. No tienen cuentas de redes sociales y solo usan Internet para navegar. ¿Su vecino tiene razón?

☐ Sí



☒ No

## Pregunta 4

¿Cuál de los siguientes datos se clasificaría como datos personales?

**Selecciona tres respuestas correctas**



☒ Número de seguridad social



☒ Número de licencia de conducir

☐ Fecha y lugar de nacimiento

☐ Cargo



☐ dirección IP

## Pregunta 5

¿Cuáles son los principios fundamentales para proteger los sistemas de información tal como se describe en el McCumber Cube?

Elige tres respuestas correctas

Acceso



Integridad

Escalabilidad



Disponibilidad



Confidencialidad

Call Barge (Interrupción de llamadas)

## Pregunta 6

¿Cuál de los siguientes métodos se puede utilizar para garantizar la confidencialidad de la información?

Elige tres respuestas correctas

Respaldo.

Control de versiones



Cifrado de datos



Configuración de permisos de archivo



Autenticación de dos factores

ID de usuario y contraseña

## Pregunta 7

¿Por qué las amenazas de seguridad internas pueden causar un daño mayor a una organización que las amenazas de seguridad externas?

Los usuarios internos tienen mejores habilidades de hacking.



Los usuarios internos tienen acceso directo a los dispositivos de la infraestructura.

Los usuarios internos pueden acceder a los datos de la organización sin autenticación

Los usuarios internos pueden acceder a los dispositivos de la infraestructura a través de Internet

## Pregunta 8

¿Cuál de las siguientes es una motivación clave de un atacante de sombrero blanco?

Aprovecharse de cualquier vulnerabilidad para beneficio personal ilegal

Ajuste fino de los dispositivos de red para mejorar su rendimiento y eficiencia.

Estudiar sistemas operativos de varias plataformas para desarrollar un nuevo sistema.



Descubrir las debilidades de las redes y los sistemas para mejorar el nivel de seguridad de estos sistemas.

## Pregunta 9

¿Puedes identificar el tipo de atacante cibernético a partir de las siguientes descripciones?

Hacen declaraciones políticas para concientizar sobre problemas que les resultan importantes.

Hactivistas



Recopilan inteligencia o cometen ataques a objetivos específicos en nombre de su gobierno.

Atacantes patrocinados por el estado



Utilizan herramientas ya existentes en Internet para iniciar ataques.

Script kiddies



## Pregunta 10

¿Cuál de las siguientes afirmaciones describe "ciberseguridad"?

La ciberseguridad es el esfuerzo continuo para proteger a las personas, las organizaciones y los gobiernos de los ataques digitales

La ciberseguridad es el esfuerzo continuo para proteger a las personas, las organizaciones y los gobiernos de los delitos que ocurren solo en el ciberespacio

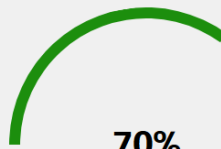


La ciberseguridad es el esfuerzo continuo para proteger las computadoras, las redes y los datos de los ataques maliciosos

1.6. Cuestionario



ES



Has obtenido un 70%.

Felicitaciones, ha pasado la prueba.

**Desplace hacia abajo para ver qué pasa después.**

## **Introducción**

En la era digital, la ciberseguridad ha emergido como una disciplina importante para proteger la información y los sistemas informáticos frente a una amplia gama de amenazas. El Módulo 1 del curso de ciberseguridad de Cisco ofrece una introducción fundamental a este campo, explorando los conceptos clave y la importancia de proteger tanto a individuos como a organizaciones. Este ensayo abordará los aspectos más destacados del módulo, incluyendo la definición de ciberseguridad, las amenazas comunes, y la importancia de la ciberhigiene, subrayando la necesidad urgente de conciencia y educación en este ámbito.

## **Desarrollo**

El Módulo 1 comienza definiendo la ciberseguridad como el conjunto de prácticas y tecnologías diseñadas para proteger redes, dispositivos, programas y datos de ataques, daños o acceso no autorizado. En un mundo donde la información digital se ha convertido en un activo esencial, la ciberseguridad es crucial para garantizar la confidencialidad, integridad y disponibilidad de los datos. Este módulo hace hincapié en la creciente importancia de la ciberseguridad en todos los sectores, desde las grandes corporaciones hasta los usuarios individuales.

Un aspecto clave del módulo es la descripción de las principales amenazas cibernéticas. Entre estas amenazas se incluyen el malware, que abarca virus, troyanos y ransomware; el phishing, que utiliza engaños para obtener información confidencial; y los ataques DDoS, que buscan saturar un sistema para hacerlo inaccesible. Cada una de estas amenazas puede tener consecuencias devastadoras, tanto a nivel financiero como reputacional, lo que subraya la importancia de estar preparado y bien informado.

El módulo también introduce el concepto de actores de amenaza, que son individuos o grupos responsables de llevar a cabo ataques cibernéticos. Estos actores pueden ser hackers con motivaciones económicas, terroristas cibernéticos con fines destructivos, o incluso empleados internos que, por descontento o negligencia, ponen en riesgo la seguridad de la organización. La diversidad y sofisticación de estos actores refuerzan la necesidad de un enfoque integral en la ciberseguridad.

Además, se discute la ciberhigiene como una práctica clave para la protección personal y organizacional. La ciberhigiene implica mantener prácticas seguras en el uso de la tecnología, como la creación de contraseñas robustas, la realización de copias de seguridad regulares y la actualización constante de software para cerrar posibles vulnerabilidades. Estas prácticas son esenciales no solo para los profesionales de TI, sino para cualquier persona que utilice dispositivos conectados a internet.

Otra área de enfoque es la educación y concienciación en ciberseguridad. El módulo subraya que la seguridad en el ciberespacio no es solo responsabilidad de los especialistas, sino de todos los usuarios de la tecnología. La capacitación continua y la sensibilización sobre los riesgos cibernéticos son fundamentales para construir una cultura de seguridad sólida. Esto incluye no solo conocer las amenazas, sino también entender las medidas de mitigación que se pueden implementar a nivel personal y corporativo.

## **Conclusión**

El Módulo 1 de la Introducción a la Ciberseguridad de Cisco proporciona una comprensión básica pero crucial de la importancia de proteger la información en el entorno digital actual. A medida que el mundo se vuelve cada vez más interconectado, la ciberseguridad se convierte en una habilidad indispensable que todos, desde usuarios individuales hasta grandes corporaciones, deben adoptar. Este módulo no solo resalta las amenazas cibernéticas más comunes, sino que también enfatiza la necesidad de una educación continua y una ciberhigiene robusta para mitigar riesgos y proteger activos digitales. En definitiva, la ciberseguridad es un pilar esencial en la era digital, y su conocimiento es clave para salvaguardar nuestro futuro tecnológico.

## **Bibliografía**

- Cisco Networking Academy. (2024). **Introducción a la Ciberseguridad**. Curso en línea. Cisco Systems, Inc.