Platzi

Curso de Introducción a Ciberseguridad: Prevención de Ataques Informáticos

¡Felicidades!

Aprobaste el curso. Ya puedes acceder a tu **diploma digital**.

10	16 / 16
Calificación	Aciertos

1. ¿Cuáles son las buenas prácticas para crear una contraseña segura?

- [x] Usar una contraseña de al menos 12 caracteres que incluya una combinación de letras mayúsculas, minúsculas, números y caracteres especiales, y preferiblemente generada por una aplicación de gestión de contraseñas.

2. El uso de aplicaciones de gestión de contraseñas sirve para:

- [x] Almacenar de forma segura y encriptada múltiples contraseñas, facilitando el acceso a servicios en línea sin necesidad de recordarlas todas.

3. Las contraseñas siguen siendo uno de los puntos más vulnerables en la ciberseguridad personal, es por eso que:

- [x] Se espera que cada vez menos sistemas las utilicen y, en su lugar, usarán alternativas "sin contraseña" como el reconocimiento facial y el uso de la huella digital.

4. ¿Cómo funcionan las aplicaciones MFA (Múltiple Factor de Autenticación)?

- [x] Requieren al usuario que proporcione al menos dos formas diferentes de autenticación, como una contraseña y un código temporal generado por una aplicación de autenticación o enviado por mensaje de texto.

5. ¿Es una mala práctica al utilizar aplicaciones MFA (Múltiple Factor de Autenticación)?

Utilizar códigos MFA generados por SMS como única capa de protección. ✓

6. ¿Al utilizar redes públicas de internet, puedes sufrir con ataques Man-In-The-Middle. ¿En qué consiste este tipo de ataque?

Ocurre cuando un atacante intercepta y potencialmente altera la comunicación entre dos partes, sin que ninguna de ellas sea consciente de la presencia del atacante. ✓

7. ¿Cómo funcionan las VPNs y por qué son una alternativa para conexiones a redes públicas de internet?

Las VPNs (redes privadas virtuales) cifran el tráfico de datos entre el dispositivo del usuario y el servidor VPN, proporcionando un túnel seguro a través de redes públicas. Esto ayuda a proteger la privacidad y la seguridad de la información transmitida. ✓

8. ¿Antivirus es un software que puede ser instalado en qué tipo de dispositivos?

Smartphones, computadoras, tablets y servidores. ✓

9. Al descargar un archivo sospechoso, que te pide desactivar el antivirus: ¿Qué debes hacer?

No debes desactivarlo y eliminar el archivo sospechoso de inmediato. Desactivar el antivirus podría exponer el sistema a amenazas. ✓

10. ¿Cuál es el propósito principal del ransomware?

El ransomware está diseñado para secuestrar y retener información, esperando un rescate a cambio. Los atacantes no discriminan en sus objetivos, atacando tanto a organizaciones como a individuos. ✓

11. Un empleado recibe un correo electrónico aparentemente legítimo con un archivo adjunto que afirma ser una factura pendiente que requiere su atención inmediata. El mensaje insta al empleado a abrir el archivo para revisar los detalles y resolver cualquier problema de facturación. Al abrir el archivo, el sistema de la empresa se ve comprometido, resultando en la pérdida de datos cruciales. ¿Qué tipo de malware se ha introducido en el sistema a través de este escenario?

Ransomware ✓

12. Un usuario decide descargar e instalar una versión pirata de un popular software de edición de fotos desde un sitio web no oficial para evitar el costo de la licencia. Después de instalar el software, el usuario comienza a notar comportamientos extraños en su computadora. ¿Cuál de las siguientes consecuencias es más probable que experimente el usuario como resultado de la instalación del software pirata?

Pérdida de datos personales. ✓

13. Al configurar el control parental en los dispositivos de tu familia, tú, como persona administradora, podrás:

Limitar el acceso a contenido inapropiado según la edad de los usuarios y establecer restricciones de tiempo de uso. ✓

14. Un nuevo empleado en una empresa recibe accidentalmente un conjunto extenso de privilegios que le otorgan acceso a información confidencial de la compañía. Este empleado, con malas intenciones, aprovecha estos privilegios para robar información sensible sin ser detectado. ¿Cómo podría haberse evitado este ataque al seguir buenas prácticas de seguridad?

Aplicando el "Principio de Mínimo Privilegio", que le otorga la menor cantidad de permisos necesaria para realizar sus tareas. ✓

15. ¿Cómo identificar mensajes potencialmente inseguros?

Estar alerta a errores de ortografía y gramática, ya que los mensajes legítimos suelen tener una redacción cuidada. ✓

16. Un usuario comparte información personal sensible, como contraseñas y detalles financieros, con un sistema de inteligencia artificial como ChatGPT. ¿Cuál de las siguientes situaciones podría ocurrir como resultado de compartir esta información sensible?

Posible robo de identidad o fraude financiero. ✓

Ver menos

Cursos que podrían interesarte

Curso de Introducción a la Ingeniería Social: Técnicas,...

Por Dra. Aury Curbelo

Curso Gratis de Ciberseguridad: Simulador Práctico en WhatsApp

Por Juan José Torres

Curso Gra
Aprender

Por Jhon C

Ir a Inicio

Siguiente curso →