Lexpin

Seguridad Informática

¿Qué es?

La seguridad informática es una disciplina que busca proteger los sistemas, dispositivos y datos de los usuarios contra posibles amenazas o ataques cibernéticos. Es un aspecto crítico en cualquier aplicación web o sistema informático para garantizar la privacidad y confidencialidad de la información.

¿Qué riesgos existen?

Existen muy fácil estar vulnerable ante un ataque informático, estos ataques pueden ser por malware (que se instala en las aplicaciones que descargamos), hacking, robo de información (Robo de multimedia, robo de datos como contraseñas y usuarios), entre otros, es por ello que podemos aplicar distintos métodos para reducir el riesgo de sufrir alguno de estos ataques, sin embargo, ninguna medida asegura la protección al 100%, pues ningún sistema es totalmente seguro, solo puede ser muy robusto y complejo de burlar.

¿Cómo protegerse?

Podemos aplicar distintas medidas de seguridad informática

Mediante código podemos implementar lo siguiente:

1. **Validación de Entrada**: validar todas las entradas de datos para asegurarse de que cumplen con las reglas establecidas
2. **Encriptación**: encriptar la información sensible antes de guardarla en la base de datos.
3. **Autenticación Segura**: implementar un sistema de autenticación seguro, que incluya contraseñas seguras y autenticación de dos factores.
4. **Control de Acceso**: restringir el acceso a información sensible y sensibles para los usuarios que no tienen autorización (Manejo de roles).
5. **Verificar Software de Terceros:** Al momento de instalar algún software en tu equipo de trabajo o extensión en el entorno de desarrollo que uses asegúrate de verificar que sea de una fuente confiable.

Por otro lado, en WordPress se pueden implementar medidas de seguridad, tales como:

1. Usar una contraseña segura y cambiarla regularmente.
2. Mantener el software de WordPress y los plugins actualizados.
3. Limitar el acceso a la página administrador.
4. Usar un plugin de seguridad, como Wordfence, para proteger la página contra posibles ataques.
5. No usar plugins o temas no confiables.

Estas son solo algunas medidas que se pueden tomar para garantizar la seguridad tanto en el código como en WordPress las cuales veremos cómo aplicarlas en las clases.
Es importante recordar que la **seguridad informática** es un **proceso constante** y que requiere un enfoque recurrente para proteger los sistemas, dispositivos y datos de los usuarios.

Ha habido varios incidentes notables en los últimos años, incluidos robos de datos a gran escala y ataques a redes de alta seguridad. Estos ataques suelen ser difíciles de detectar, es muy, muy probablemente tengas algún virus que infecte tu sistema y no lo has detectado, puesto que estos han evolucionado para volverse más sigilosos y efectivos con el pasar de los años, haciendo que los sistemas de defensa deban esforzarse más para detectarlos y combatirlos.

¿Qué es y Cómo funciona un virus?

Un virus es un tipo de software malicioso que se propaga usualmente por la red de una computadora a otra, a menudo sin el conocimiento o el consentimiento del usuario, y puede causar daño o tomar el control del sistema. Los virus funcionan aprovechando las debilidades del sistema operativo o del software de una computadora.

El proceso típico de infección de un virus es:

- **Infección**: un virus se inserta en un archivo o programa en el sistema, generalmente mediante la descarga de un archivo infectado, la apertura de un archivo adjunto de correo electrónico malicioso o la descarga de software de sitios web no confiables.
- **Replicación**: En algunas ocasiones, una vez que el virus ha infectado el sistema, comienza a replicarse y propagarse a otros archivos y programas. Puede hacerlo mediante la creación de copias de sí mismo o la inserción de código malicioso en otros archivos, pero esto no siempre sucede, hay virus que no se replican y son más difíciles de detectar.
- **Activación**: en algún momento, el virus se activa y realiza su carga maliciosa. Esta carga puede ser una variedad de cosas, desde la eliminación de archivos y la corrupción del sistema, hasta la captura de información personal o el control del sistema.

Es importante tener en cuenta que los virus pueden ser diseñados de muchas maneras diferentes, y pueden tener distintas formas de infectar sistemas. Además, también hay otros tipos de software maliciosos, como los gusanos, el spyware y el ransomware, que tienen diferentes formas de propagación y carga maliciosa.

Para evitar la infección de virus, es importante mantener actualizado el sistema operativo, tener un software antivirus actualizado y evitar descargar software o archivos de sitios web no confiables o correos electrónicos no solicitados, ni mensajes sospechosos en algún servicio de mensajería como lo son Messenger, WhatsApp, Telegram, etc.., También es importante utilizar contraseñas seguras y no compartir información personal en línea.

¿Qué es y Cómo funciona un antivirus?

Un antivirus es un software diseñado para proteger un dispositivo, como una computadora o un teléfono móvil, contra software malicioso o malware. Los antivirus funcionan mediante la identificación y eliminación del malware existente en un sistema y previniendo la infección futura del sistema.

La mayoría de los antivirus utilizan una combinación de técnicas para detectar y eliminar el malware, estas pueden ser:

- **Análisis de firmas**: esta técnica implica la identificación de patrones específicos en el código del malware. Los antivirus buscan estos patrones en los archivos y procesos del sistema en busca de virus conocidos.
- **Análisis heurístico**: los antivirus utilizan el análisis heurístico para detectar y bloquear nuevos tipos de malware. Este método utiliza algoritmos para analizar el comportamiento de un archivo y determinar si se comporta de manera sospechosa o es similar al comportamiento del malware conocido.
- **Protección en tiempo real**: esta técnica monitorea continuamente el sistema para detectar cualquier actividad sospechosa, como la ejecución de un archivo infectado o la conexión a un sitio web malicioso.
- **Protección del navegador**: muchos antivirus también proporcionan una protección adicional para el navegador web, bloqueando los sitios web maliciosos y las descargas de archivos peligrosos.

Una vez que se detecta el malware, el antivirus toma medidas para eliminarlo o ponerlo en cuarentena (Moverlo a una carpeta blindada y anular su activación) para que no pueda dañar el sistema. Además, los antivirus también suelen incluir funciones de actualización automática para mantenerse al día con las últimas amenazas de malware.

Es importante tener en cuenta que **ningún antivirus es 100% efectivo**, ya que siempre hay nuevos virus y malware que pueden evitar la detección, es por eso que es importante mantener el software de protección contra virus (antivirus) actualizado.

Si quieres aprender mientras juegas como funcionan los virus y sistemas antivirus puedes probar la siguiente app, recuerda descargarla de la tienda de Google Play para Android y la App Store de Apple para IOS.

Hackers – Trickster Arts / Android - IOS