¿Qué es la seguridad informática y cómo puede ayudarme?

Podemos definir qué es la seguridad informática como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos. La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.

Las cuatro áreas principales que cubre la seguridad informática

1. **Confidencialidad**: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
2. **Integridad**: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
3. **Disponibilidad**: Los datos deben estar disponibles para los usuarios cuando sea necesario.
4. **Autenticación**: Estás realmente comunicándote con los que piensas que te estás comunicando.

¿Por qué es tan importante la seguridad informática?

Prevenir el robo de datos tales como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos relacionados con el trabajo, hojas de cálculo, etc. es algo esencial durante las comunicaciones de hoy en día. Muchas de las acciones de nuestro día a día dependen de **la seguridad informática** a lo largo de toda la ruta que siguen nuestros datos. Y como uno de los puntos iniciales de esa ruta, los datos presentes en un ordenador también pueden ser mal utilizados por intrusiones no autorizadas. Un intruso puede modificar y cambiar los códigos fuente de los programas y también puede utilizar tus imágenes o cuentas de correo electrónico para crear contenido perjudicial, como imágenes pornográficas o cuentas sociales falsas. Hay

también ciberdelincuentes que intentarán acceder a los ordenadores con intenciones maliciosas como pueden ser atacar a otros equipos o sitios web o redes simplemente para crear el caos. Los hackers pueden bloquear un sistema informático para propiciar la pérdida de datos. También son capaces de lanzar ataques DDoS para conseguir que no se pueda acceder a sitios web mediante consiguiendo que el servidor falle. Todos los factores anteriores vuelven a hacer hincapié en la necesidad de que nuestros datos deben permanecer seguros y protegidos confidencialmente. Por lo tanto, es necesario proteger tu equipo y eso hace que sea necesario y muy importante todo lo **que es la seguridad informática**.

Medidas para el mantenimiento de la seguridad informática y la prevención de intrusiones

Los ataques más utilizados en contra de un sistema informático son los troyanos, los gusanos y la suplantación y espionaje a través de redes sociales. También son populares los ataques DoS/DDoS, que pueden ser usados para interrumpir los servicios. A menudo algunos usuarios autorizados pueden también estar directamente involucrados en el robo de datos o en su mal uso. Pero si se toman las medidas adecuadas, la gran mayoría de este tipo de ataques pueden prevenirse, por ejemplo a través de la creación de diferentes niveles de acceso, o incluso limitando el acceso físico. Las medidas de **seguridad informática** que puedes tomar incluyen:

- **Asegurar la instalación de software legalmente adquirido**: por lo general el software legal está libre de troyanos o virus.
- **Suites antivirus**: con las reglas de configuración y de los sistemas adecuadamente definidos.
- **Hardware y software cortafuegos**: los firewalls ayudan con el bloqueo de usuarios no autorizados que intentan acceder a tu computadora o tu red.
- **Uso de contraseñas complejas y grandes**: las contraseñas deben constar de varios caracteres especiales, números y letras. Esto ayuda en gran medida a que un hacker pueda romperla fácilmente.
- **Cuidado con la ingeniería social**: a través de las redes sociales los ciberdelincuentes pueden intentar obtener datos e información que pueden utilizar para realizar ataques.
- **Criptografía, especialmente la encriptación**: juega un papel importante en mantener nuestra información sensible, segura y secreta.