Características principales de la seguridad informática

Seguridad informática

La seguridad informática sirve para garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas y de la información contenida en ellos, así como de las redes privadas y sus recursos.

En este sentido, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.

La seguridad informática debe vigilar las siguientes propiedades:

Privacidad

La información debe ser vista y manipulada solo por quien o quienes tengan el derecho de hacerlo. Un ejemplo de ataque a la Privacidad es la Divulgación de Información Confidencial o personal.

Integridad

La información deber ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataques a la integridad es la modificación NO autorizada de los saldos en un sistema bancario, es decir, la modificación de números en un banco que provoca un caos en el ente financiero.

Disponibilidad

La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio, (Denial of Service o DoS), que es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Seguridad informática.

Dentro del concepto de seguridad de una computadora, se distinguen:

Seguridad Física

Comprende el aspecto de hardware (mouse, monitor, teclado, etc.), la manipulación del mismo, así como también del ambiente en el cual se va a instalar el equipo (en particular, la sala de servidores).

Seguridad Lógica

Comprende el aspecto de los sistemas, tanto operativos como de aplicaciones, y principalmente de la información del usuario.

Algunas de las medidas recomendadas por especialistas para evitar los ciberataques son:

- Externalizar servicios: al no tener tantos activos disminuye el riesgo de ataques.
- Contar con un buen antivirus que nos garantice protección.
- Capacitación de los usuarios: formar a los usuarios de los sistemas de seguridad informática en materia de ciberseguridad.
- Mantener actualizado el software.
- Prestar atención a las contraseñas.
- Realizar auditorías de software.
- Posibilidad de contratar un ciberseguro.

¿Cuáles son los ataques cibernéticos más recurrentes en la actualidad?

Ransomware

De acuerdo con la compañía de seguridad eset, el ransomware es el término genérico para referirse a todo tipo de software malicioso que le exige al usuario de un 'equipo secuestrado' (generalmente computadores portátiles o de escritorio) el pago de un rescate por la información almacenada en este. Seguridad informática.

Este ataque opera de la siguiente forma: el usuario verá un mensaje en la pantalla de su computador (o en varios pc de su empresa) que le avisa que todos sus archivos han sido encriptados, y que debe pagar cierta cantidad de dinero en monedas virtuales (bitcoins) antes de dos o tres días, o si no perderá sus archivos para siempre.

Lastimosamente, cuando este hecho ocurre, una gran parte de los usuarios accede a pagar la cantidad de dinero que exigen los ciberdelincuentes, la cual no suele ser una suma exacerbada; ya que los individuos que dirigen el ataque generalmente conocen cuánto dinero puede pagar la persona afectada.

Según un informe de symantec, en el mundo, el volumen de víctimas de ransomware aumentó en 266% y estados unidos es el país que más sufre ataques, debido a que el 64% de los norteamericanos pagan rescate, así las cosas, un ataque de ransomware es tan grave que puede paralizar las operaciones de una compañía, "o sacarla del negocio si al final pierde sus datos. De allí que muchas empresas paguen las extorsiones", comentábamos previamente en una nota de enter.co.

Referencia bibliográfica

Lectura 5

Características de la Seguridad Informática. (s.f.). Recuperado 27 octubre, 2018, de https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/