**Clase 15**

**Seguridad informática**

**Ciberseguridad:**

La seguridad informática o ciberseguridad, es una disciplina que se encarga de proteger la integridad y la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. Se enfoca en la **protección de la infraestructura computacional** y todo lo vinculado con la misma, en especial, la información que se transmite a través de las redes de computadoras. Para minimizar todos los riesgos a la infraestructura y a la información se han creado múltiples métodos, como estándares, protocolos, reglas, herramientas y leyes informáticas.

La seguridad informática se centrará únicamente en el medio de comunicación por el cual va a viajar la información, no es lo mismo que la seguridad de la información, ya que esta última puede estar en diferentes medios y no solo en los medios informáticos.

**Tipos de amenazas informáticas:**

Cuando notamos que nuestro dispositivo tiene algún comportamiento fuera de lo normal, probablemente estemos ante ciertas amenazas tecnológicas, que, si bien están causadas por seres humanos, el atacante, utiliza un tipo de software maligno llamado **malware** para que realice todo el proceso de piratería.

**Malware *(Malicious Software)*:** es un término que se usa para describir a todos los softwares maliciosos que tienen como objetivo infiltrarse o dañar un sistema de información sin el consentimiento del usuario.

Para que este pueda cumplir con sus objetivos, debe estar oculto al usuario ya que esto le permitirá seguir actuando. Cuando el usuario nota la presencia de algún tipo de malware, hará lo necesario para tratar de eliminarlo**.**

* **Virus:** componente de software que tiene como objetivo permanecer en un sistema copiándose a si mismo en varios lugares desde el momento en que se ejecuta en el sistema. Así, cuando intentamos eliminar un archivo o programa infectado el virus sigue en memoria ya que ha infectado otras partes del sistema.  
  Su objetivo puede variar, pero en esencia será destruir o inhabilitar archivos o programas que tengamos en nuestros dispositivos además de afectar el funcionamiento del mismo.  
  La mayoría se adhieren a archivos ejecutables o también en registros maestros de arranque. Estos virus no tienen la capacidad por si mismos de infectar a otros dispositivos a menos que lo pasemos por medio de un hardware, como un usb. Por esto, son de poca infección, porque se replican a sí mismos solo dentro del mismo dispositivo.
* **Gusanos:** malware que no solo se copia a si mismo en el sistema sino que además utiliza la red para copiarse a otras máquinas a través de las vulnerabilidades de la red o agujeros de seguridad, por ello tiene una mayor capacidad de infección.  
  Su objetivo es replicarse a si mismos hasta saturar el funcionamiento del sistema
* **Troyano:** no causan daño en si mismos, es una estructura utilizada para cargar cosas ocultas, gusanos, virus, y demás malwares. Generalmente son programas sin licencia que instalamos pensando que no harán daño porque no somos conscientes de que podrían ser un troyano. Requieren de la ejecución del usuario ya que no pueden duplicarse a sí mismos.   
  Los troyanos también pueden crear ***backdoors*** que es una puerta trasera para que un dispositivo pueda ser controlado de forma remota por alguien más.  
  Puede ser usado como un servidor proxy para ocultar ataques, o para introducir span a nuestro equipo.
* **Adwares:** su objetivo es bombardear a nuestro dispositivo con publicidad. No son dañinos y suelen venir dentro de *troyanos.*

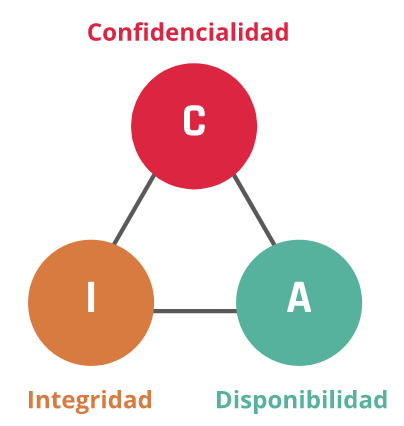
**Amenazas informáticas:** en la red nuestros equipos están constantemente expuestos a amenazas informáticas. Existen algunos malwares especialmente peligrosos con un modo más sutil de ataque para robar:

* **Spywares:** o softwares espías, estos no dañan los dispositivos, pero roba toda la información del sistema. Su objetivo es permanecer oculto para robar todo tipo de datos. También puede acceder a la cámara o el micrófono del dispositivo sin que el usuario lo note. Estos suelen entrar por troyanos o también pueden ser instalados, como es el caso de ***keyloguer:*** *spyware que registra las pulsaciones del teclado para saber qué es lo que el usuario escribe.*
* **Rootkits:** son un conjunto de software, los demás malwares atacan al sistema operativo, por lo que una vez que se reinstala el sistema desaparece el malware. Pero los Rootkits, van dirigidos al firware del sistema o los programas de usuario y tienen acceso al dispositivo en modo sistema o kernel. Este acceso les permite a los Rootkits realizar modificaciones a los procesos internos del so, a los archivos del sistema como registros y a las cuentas de usuario.  
  Aparte, estos logran esconderse de los softwares antimalware o antivirus.
* **Botnets:** es una red robot que es puesto por un atacante en una red de computadoras para así controlar todas al mismo tiempo. Principalmente se usa con el fin de cometer crímenes digitales o crimeware. Suele propagarse a través de troyanos.
* **Ransomware *o software de secuestro*:** a diferencia de todos los malwares anteriores, que se caracterizan por permanecer ocultos al usuario, estos, permanecen visibles.  
  Suelen ser usados por atacantes contra empresas para secuestrar la información de sus servicios y productos y luego pedir recompensa por el rescate.  
  El ciberatacante, hace evidente el chantaje por el secuestro. Este tipo se puede encontrar en archivos adjuntos de correos electrónicos del correo no deseado, o al hacer click en ciertos vínculos.

**Protección de la información**

**Principios de la seguridad de la información**

**Información:** la información es un recurso clave para tomar decisiones, dimensionar cosas, y disminuir riesgos. La misma cuenta con tres dimensiones conocidas como: integridad, disponibilidad y confidencialidad también llamadas CIA por sus siglas en inglés. Los atacantes de un sistema van a tratar de vulnerar algunas de esas dimensiones.



* **Integridad:** consiste en que la información se encuentre completa, entera y que los datos que están dentro del sistema sean los que deberían ser. Un ejemplo de esta dimensión sería el ataque a una base de datos y la modificación de los datos que hay en la misma, con lo cual podemos seguir viendo la información, pero la misma es errónea debido a que la original fue alterada.
* **Disponibilidad:** una persona/usuario debe poder tener acceso a la información en el momento que lo necesita, es decir, en tiempo y forma. Un típico ataque a este tipo de dimensión es el ataque de denegación de servicio.
* **Confidencialidad:** refiere a que la información tiene que estar disponible únicamente para las personas que tienen acceso a esta información y bloqueada para el acceso a terceros. Por ejemplo, los datos personales e historiales médicos.

**Protección de la información:**

Se basa en garantizar el completo y total funcionamiento de las 3 dimensiones, para ello, debemos implementar medidas preventivas y reactivas.

**Medidas preventivas** refiere a todas las acciones que pueden tomarse para evitar problemas no deseados.

**Medidas reactivas** son aquellas donde ya se ocasionó un problema de seguridad y hay que solventarlo.

**Protección de la confidencialidad:** la confidencialidad puede romperse de varias maneras, tanto directas (hackeando la seguridad) como indirectas a través de errores humanos.

Algunas técnicas para asegurar la confiabilidad pueden ser:

* **Encriptación:** significa cambiar el formato de los datos con la razón de que si estos son interceptados solo las personas autorizadas sepan cómo leerlos (medida preventiva).
* **Controles de acceso:** asegurar que solo las personas autorizadas puedan acceder a la información (medida preventiva).
* **Borrado remoto:** refiere al esfuerzo de mantener los datos siempre privados, en el caso de que se perdiera el acceso, la capacidad de bloquear el dispositivo o borrar la información (medida reactiva).
* **Capacitación al personal:** existe un concepto llamado ***ingeniería social***, que es la denominación que se le da a cómo los usuarios son engañados para otorgar sus accesos, la capacitación en estos problemas es una acción preventiva para evitarlos.

**Protección de la integridad:** la integridad puede romperse de varias maneras similares a la de la confiabilidad, por lo cual, varias de sus acciones de seguridad son reutilizadas.

Algunas técnicas para asegurar la integridad pueden ser:

* **Auditorias:** se utilizan para comprobar que la información coincide con lo que debería ser correcto (medida reactiva)
* **El control de versiones:** si ha ocurrido un inconveniente con la información, diversas herramientas de control de versiones ayudan a “volver a un estado anterior” (medida reactiva)
* **Firmas digitales:** esta medida permite asegurar la autenticidad del documento (medida preventiva)
* **Detección de intrusos:** diseñados para detectar problemas cuando un acceso no autorizado se ha cometido (medida reactiva)

**Protección de la disponibilidad:** la disponibilidad debe tenerse en cuenta para cuando ocurra un problema de seguridad como de forma preventiva al mismo.

Algunas técnicas para asegurar la disponibilidad pueden ser:

* **Tolerancia a fallos:** la capacidad de los sistemas o servidores a que, si algún tipo de fallo sucede, la información pueda ser utilizada (preventiva o reactiva dependiendo la situación)
* **Redundancia:** de esta forma la información y las validaciones de acceso se repitan tanto que la información está segura de no perderse en su totalidad (preventiva)
* **Parches de seguridad:** cuando se detecta una falla, debe solucionarse el problema para que no vuelva a ocurrir, igualmente si la falla fue por un software, actualizarlo con la vulnerabilidad resuelta

**Fallas y vulnerabilidades**

**Fallas:** una falla, también conocida como bug, es un error en un programa o sistema operativo que desencadena un resultado indeseado.

El termino bug viene desde 1947 cuando Grace Hopper, mientras estaba programando el Mark II, descubrió que un insecto había provocado un error en uno de sus relés electromagnéticos.

En el desarrollo del software existen muchos tipos de fallas, pero en general se pudieron establecer unos tipos generales de bugs según su comportamiento.

**Tipos de fallas:**

* **Heisenbug:** basados en el principio de incertidumbre de Heisenberg se denominan a aquellos bugs que alteran o desaparecen su comportamiento al tratar de depurarlos
* **Bohrbug:** nombrados así por el modelo atómico de Bohr, es una clasificación de un error de software inusual que siempre produce una falla al reiniciar la operación que causó la falla.
* **Mandelbug:** llamado así por el matemático Benoit Mandelbrot, un mandelbug es un fallo con causas tan complejas que su comportamiento es totalmente caótico.
* **Schroedinbugs:** son errores que no aparecen hasta que alguien lee el código y descubre que, en determinadas circunstancias, el programa podría fallar. A partir de ese momento, el Schroedinbug comienza a aparecer una y otra vez.

**Vulnerabilidades:** una vulnerabilidad es una debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información.

La evaluación o detección de vulnerabilidades permite reconocer, clasificar y caracterizar los agujeros de seguridad.

**Pasos para detectar una vulnerabilidad:**

Si bien no existe un método único para detectar vulnerabilidades, es posible armar una serie de ítems a tener en cuenta para considerar nuestra información segura.

* Evaluar cómo está constituida la red e infraestructura de la empresa.
* Delimitar quién puede y debe acceder a la información confidencial.
* Probar que las copias de seguridad realizadas funcionen.
* Identificar las partes más sensibles y esenciales del sistema.
* Realizar auditorias del estado de la seguridad informática.