

## GUIA PEDAGÓGICA 11

Docentes Responsables: José Antonio Caparroz, David Guerrero

Año: 3º Divisiones: 1ª, 2ª, 3ª Ciclo Básico - Nivel Secundario

Ciclo Lectivo: 2020

Turno: Mañana - Tarde

Espacio curricular: **INFORMÁTICA II**

**TEMA:** SEGURIDAD INFORMATICA

### OBJETIVOS:

- Reconocer y Poder explicar los conceptos de seguridad informática.
- Reflexionar sobre los principios de la seguridad informática y factores de riesgo.
- Distinguir las diferentes tipos de amenazas.
- Hacer uso de ejemplos para explicar los tipos de amenazas.

### CONTENIDOS CONCEPTUALES

#### Seguridad informática

La seguridad informática o seguridad de tecnologías de la información es el **área de la informática que se enfoca en la protección de la infraestructura computacional** y todo lo relacionado con esta, **y la información contenida o circulante**. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la información.

La seguridad informática o ciberseguridad se define como el **conjunto de métodos y herramientas destinados a proteger los sistemas ante cualquier amenaza**. Estos pueden ser tanto de naturaleza real como virtual, entiéndase, por ejemplo, desde un incendio en un centro de cómputos que afecte a los servidores o puestos de trabajo, hasta un ciberataque masivo por denegación de servicios (Ddos), entre un amplio y variado abanico de posibles ciberamenazas.



**“La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable”**

La definición de *seguridad de la información*, no debe ser confundida con la de «seguridad informática», ya que esta última sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática comprende al **software** (bases de datos, archivos), **hardware**, **seguridad de red** y todo lo que la organización valore como activo y signifique un riesgo si esta información confidencial llega a manos de otras personas.

Así surgen los conceptos de seguridad lógica y física.



**Seguridad lógica:** Se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como acceso ordenado y autorizado de los usuarios a la información. La "seguridad lógica" involucra todas aquellas medidas establecidas por la administración (usuarios y administradores de recursos de tecnología de información) para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información, por lo que el acceso a los archivos de datos y programas sólo se permitirá al personal autorizado.

Los principales **objetivos** que persigue la seguridad lógica son:

- **Restringir el acceso a los programas y archivos**
- **Asegurar que se estén utilizando los datos, archivos y programas correctos por medio del procedimiento correcto.**

**Seguridad física:** Consiste en la "aplicación de barreras físicas y procedimientos de control, medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

### Principios de Seguridad Informática

Para lograr sus objetivos la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

- ✚ **Confidencialidad:** Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático.
- ✚ **Integridad:** Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático
- ✚ **Disponibilidad:** Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.

### Factores de Riesgo a tener en cuenta

**Ambientales/Físicos:** Factores externos, lluvias, inundaciones, terremotos, tormentas, rayos, humedad, calor entre otros.

**Tecnológicos:** Fallas de hardware y/o software, fallas en el aire acondicionado, falla en el servicio eléctrico, ataque por virus informático, etc.

**Humanos:** Hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, y otras alteraciones.

### Gestionar la seguridad informática

Durante los últimos años hemos visto como empresas de distintos sectores fueron víctimas de ataques informáticos en diversas escalas.

Esto ha generado mayor conciencia en las organizaciones que consideran la cyber seguridad como un tema prioritario. Los directivos destacan que los ataques externos se vuelven más sofisticados y de mayor alcance, por ello deben prepararse para enfrentar esta situación.

Para prever que nuestra identidad digital no sea vulnerada o expuesta, se deben autenticar los accesos a las bases de datos y los sitios web (identificación de usuario registrado mediante contraseñas y/o sitios con firma digital).

Algunos dispositivos que se conectan a la red no cumplen con los requisitos de protección, ya que los fabricantes no elevan los controles en términos de seguridad informática, por



consiguiente los dispositivos están en riesgo que sean vulnerados (control de red pública o privada segura).

La adopción de servicios CLOUD (Nube) crece y con ello los riesgos asociados. Bajo la premisa de recursos ilimitados, los proveedores de servicios de carga de datos a la nube, le dan prioridad a la disponibilidad y dejan al usuario, la capa de diseño, acceso y control. Esto obliga a incorporar recursos para garantizar que las aplicaciones y servicios cumplan las políticas de seguridad de la empresa.

**Nota:** El concepto de nube se refiere al almacenamiento de datos fuera de nuestros dispositivos. Es decir: Si guardas una foto en la carpeta "Mis Documentos" de tu ordenador, sólo podrás acceder a ella desde ese PC. En cambio, si guardas esa misma foto en un almacenamiento en la nube como Google Drive o Dropbox, la foto se enviará a un ordenador distante y dedicado, podrás verla en tu dispositivo... aunque no esté ahí guardada.

Muchos de tus archivos pasar de estar en tu ordenador a almacenarse fuera de él. Esto implica dejar de tener control sobre ellos, por lo que nunca puedes estar del todo seguro de quién accede a esta información, o si está o no protegida como debería ser.

El desafío está en poder generar un diseño seguro de arquitecturas cloud, en la gestión de vulnerabilidades, la automatización en tratamiento de incidentes de seguridad y mitigación de riesgos.

### **Tipos de amenazas:**

**Internas:** Los trabajadores pueden conocer perfectamente la red y saber cómo es el funcionamiento. Tienen ciertos niveles de acceso a la red dadas las necesidades de su trabajo.

**Externas:** Son las amenazas que se originan fuera de nuestra red como un intruso que busca la manera de acceder a nuestros sistemas, la ventaja es que en algunos casos se pueden prevenir esos ataques efectuados por Hackers o crackers, si el sistema está protegido.

- **Hacker:** Del inglés hack, hachar. Término utilizado para denominar a una persona experta en seguridad informática, con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo y para su propio bien. Este objetivo puede o no ser maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo. El término "hacker" suele tener una connotación despectiva o negativa, pues se relaciona a tareas ilegales. Es más propio llamar piratas informáticos a aquellos hackers que realizan acciones malignas con sus conocimientos.
- **Cracker:** Experto en seguridad informática que usa sus conocimientos para burlar códigos de programación. Realizar Crack, Keygen, Virus, etc. Se utiliza para referirse a las personas que *rompen* algún sistema informático. Los *crackers* pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío, aprovechaban debilidades o errores de algunos sistemas informáticos.

Las amenazas pueden ser causadas por:

**Usuarios:** En algunos casos sus acciones causan problemas de seguridad de un sistema informático. Si bien en la mayoría de los casos es porque no se les han restringido o limitado sus acciones, bloqueando el acceso a áreas que no deben acceder.

**Personas ajenas a la empresa:** Bloqueo de áreas con uso de scanner, tarjetas de acceso, etc.

**Programas maliciosos:** Programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador, abriendo una puerta



a intrusos o bien modificando los datos. Estos programas son virus informáticos, en general conocidos como malware.

**Spam o correo basura o mensaje basura:** Son los mensajes no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican al receptor. La acción de enviar dichos mensajes se denomina **spamming**. La vía, más utilizada es el correo electrónico. También se llama **correo no deseado** a los virus sueltos en la red y páginas filtradas (casino, sorteos, premios, viajes, drogas, software y pornografía), se activa mediante el ingreso a páginas de comunidades o grupos o acceder a enlaces en diversas páginas o inclusive sin antes acceder a ningún tipo de páginas de publicidad. El programa diseñado para bloquear el correo no deseado se llama **Antispam**.

**Pop-up o ventana emergente:** Es una nueva ventana, con publicidad, que aparece de repente en la pantalla de tu ordenador, cuando abres una página a través un navegador. Si no quieres ver la ventana, puedes cerrarla pinchando en la X en la esquina superior derecha.

**Anti pop-ups:** Herramienta encargada de detectar y evitar que se muestren los pop-ups mientras se navega por la web. Permiten bloquear los pop-ups, avisando al usuario cuándo y cuántas ventanas son bloqueadas.

**Spyware o programa espía:** Es un software que recopila información de un ordenador y la transmite a una entidad externa sin el conocimiento o el consentimiento del usuario.

*Spyware* viene dado de las palabras en idioma inglés *spy* que significa espía, y *ware* (deriva de programa).

El término *spyware* también se utiliza más ampliamente para referirse a procesos que realizan diferentes funciones, como recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.

Un *spyware* se auto instala en el sistema de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados. A diferencia de los virus, no se replica en otros ordenadores, por lo que funciona como un parásito.

Una infección de spyware aparte de las cuestiones de privacidad, incluyen una pérdida considerable del rendimiento del sistema y problemas de estabilidad graves (el ordenador se queda "colgado"). También causan dificultad a la hora de conectar a Internet. Algunos ejemplos de programas espía conocidos son Gator y Bonzi\_Buddy.

El programa diseñado para bloquear el spyware se llama **Antispyware**.

**Virus informático:** Es un malware (*malicious software*). También llamado **badware**, **código maligno**, **software malicioso** o **software malintencionado** que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

Habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Pueden destruir, los datos almacenados en una computadora. Los virus tienen, la función de propagarse a través de un software.

El funcionamiento de un virus informático es simple. Se ejecuta un programa que está infectado, el código del virus queda residente (alojado) en la memoria RAM de la computadora, incluso cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos



ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

Algunas de las **acciones de los virus** son:

- Unirse a un programa instalado en el computador permitiendo su propagación.
- Mostrar en la pantalla mensajes.
- Ralentizar o bloquear el computador.
- Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
- Reducir el espacio en el disco.
- Molestar al usuario cerrando ventanas, moviendo el ratón...

### **Tipos de virus:**

Existen muchos tipos de virus solo mencionaremos:

**Bomba de tiempo:** Son programados para que se activen en determinados momentos, definido por su creador. Una vez infectado un determinado sistema, el virus solamente se activará y causará algún tipo de daño el día o el instante previamente definido.

**Lombrices, worm o gusanos:** Tiene la propiedad de duplicarse a sí mismo, **sólo se repliquen, sin el objetivo de causar graves daños al sistema**. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

**Troyanos o caballos de Troya:** Programa que trae en su interior un código, que permite acceder a la computadora infectarla, recolectar datos y enviarlos por Internet a un pirata informático, sin que el usuario se dé cuenta de esto.

**Ransomware:** Un malware que secuestra los datos de tu ordenador bloqueándolos o todo el equipo, y pidiéndote un rescate económico a cambio de recuperarlos. Es importante nunca pagar el rescate para no fomentar su uso y no hay garantías de liberar los datos de tu ordenador.

**Antivirus:** Es un programa creado para prevenir o evitar la activación de los virus, así como su propagación y contagio. Cuenta con rutinas de detención, eliminación y reconstrucción de los archivos y las áreas infectadas del sistema.

El antivirus es un programa que ayuda a proteger la computadora contra los virus, que puedan infectarla.

Un antivirus tiene tres **principales funciones**:

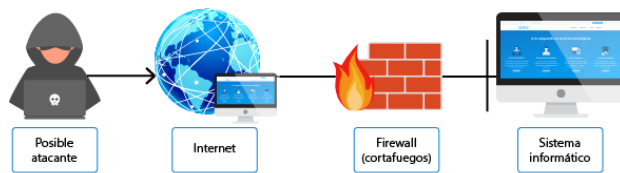
**VACUNA** Una vez instalado reside en la memoria, actuando como "filtro" de los programas que son ejecutados, en tiempo real.

**DETECTA** Examina todos los archivos existentes en el disco o a los que se les indique en una determinada dirección. Tiene instrucciones de control y reconocimiento exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y desarma su estructura.

**ELIMINA** Una vez desactivada la estructura del virus procede a eliminarlo o reparar o reconstruir los archivos y áreas afectadas.

Los **antivirus desarrollados y más conocidos** son: Avast, Panda Security, Norton, McAfee, AVG, BitDefender, F-Prot, F-Secure, Kaspersky, NOD32, PC-cillin, y Avira.

**Firewall o cortafuego:** Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo solo comunicaciones autorizadas.



Se trata de **un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, y descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y criterios.**

Los cortafuegos pueden ser **implementados en hardware o software, o una combinación de ambos.** Se utilizan para

evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas. Todos los mensajes que entren o salgan de internet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Un firewall puede ayudar a impedir que piratas informáticos o software malintencionado (como troyanos) obtengan acceso al equipo a través de una red o Internet.

Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos.

## CONTENIDOS PROCEDIMENTALES

- Leer, analizar e interpretar los conceptos y ejemplos de seguridad informática.

## METODOLOGÍA:

- Leer los conceptos y ejemplos sobre seguridad informática.
- Responder:
  - 1- De los conceptos de seguridad informática.
  - 2- ¿En qué consiste la seguridad lógica y seguridad física?
  - 3- Tipos de amenazas. Explique.
  - 4- ¿Qué es hacker y cracker?
  - 5- ¿Qué es un Spam y cómo evitarlos?
  - 6- ¿Qué es pop up y anti pop up?
  - 7- ¿Qué es Spyware y cómo evitarlos?
  - 8- Explique Virus. Menciones los tipos de virus.
  - 9- ¿Qué es un antivirus? Mencione los más conocidos por Ud.
  - 10- ¿Qué es firewalls?
- Transcribir a un documento de Word las preguntas y respuestas del cuestionario. El documento debe respetar las pautas enunciadas en la guía 8 y guardar como **Curso\_división\_Apellido\_Nombre\_Seg2.docx**.
- Investigar las páginas sugeridas en la bibliografía para ampliar y visualizar los contenidos de este documento.

## BIBLIOGRAFÍA:

<https://www.viewnext.com/tipos-de-seguridad-informatica/>  
<https://www.netec.com/que-es-seguridad-informatica>  
<https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos>  
<https://es.ccm.net/faq/2809-diferentes-tipos-de-programas-maliciosos>  
<https://www.tecnologia-informatica.com/que-es-firewall-como-functiona-tipos-firewall/>

**Director: Jorge Grosso**