
BIENVENIDOS AL CURSO



INSTRUCTORA ING. NUBIA LÓPEZ

SEGURIDAD INFORMÁTICA



OBJETIVOS DEL CURSO

- Este curso tiene como objetivo principal conocer los diversos conceptos de la seguridad informática, principalmente basado para las personas que requieren conocer acerca de este importante curso, está dirigido a estudiantes de informática, profesionales de la seguridad y docentes que incursionan en el mundo de la seguridad informática.



INTRODUCCIÓN



- En este pequeño curso les estaremos impartiendo los principales conocimientos básicos relacionados a la seguridad informática, que les permitirá adquirir una visión general y amplia de la seguridad informática, este curso constara de 11 videos, es totalmente gratis para todo aquel que quiera reforzar sus conocimientos en cuanto a seguridad.

¿QUÉ ES LA SEGURIDAD INFORMÁTICA



- **La seguridad informática** —también llamada ciberseguridad— se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros.
- Es por esto que esta disciplina del área de la informática encargada de la protección de la privacidad de datos dentro de los sistemas informáticos se ha convertido en una **parte indispensable para los negocios y la operación de las empresas.**

¿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 puede ser mal utilizados por intrusiones no autorizadas.

PRINCIPALES TIPOS DE SEGURIDAD INFORMÁTICA

- Seguridad de hardware
- Seguridad de *software*
- Seguridad de red



TIPOS DE SEGURIDAD INFORMÁTICA

Seguridad de *hardware*

- Este tipo de seguridad se relaciona con la protección de **dispositivos** que se usan para proteger sistemas y redes —apps y programas de amenazas exteriores—, frente a diversos riesgos. El método más usado es el manejo de sistemas de alimentación ininterrumpida (SAI), servidores proxy, *firewall*, módulos de seguridad de *hardware* (HSM) y los data lost prevention (DLP). Esta seguridad también se refiere a la protección de equipos físicos frente a cualquier daño físico.

TIPOS DE SEGURIDAD INFORMÁTICA

Seguridad de *software*

- Usado para salvaguardar los **sistemas** frente ataques malintencionados de *hackers* y otros riesgos relacionados con las vulnerabilidades que pueden presentar los *softwares*. A través de estos “defectos” los intrusos pueden entrar en los sistemas, por lo que se requiere de soluciones que aporten, entre otros, modelos de autenticación.



Seguridad de red

- Principalmente relacionada con el diseño de actividades para proteger los datos que sean accesibles por medio de la red y que existe la posibilidad de que sean modificados, robados o mal usados. Las principales amenazas en esta área son: virus, troyanos, phishing, programas espía, robo de datos y suplantación de identidad.

Los tipos de seguridad informática siempre se mantendrán en desarrollo. Pues la innovación en tecnología de los equipos y su conexión a Internet son constantes, y las amenazas para los mismos proliferan día a día.



TIPOS DE AMENAZAS DENTRO DE LA SEGURIDAD DE RED

Existen multitud de tipos de amenazas para las redes, y la mayoría de ellas se propagan desde Internet. Entre las más comunes se encuentran:

- Los virus, programas gusano y de tipo caballo de Troya.
- Ataques por parte de delincuentes informáticos o hackers.
- Software espía y de propaganda invasiva.
- Ataques de día cero, o de hora cero.
- Robo de datos o interceptación de los mismos en comunicaciones.
- Ataques de denegación del servicio.
- Robo de datos personales e identidad.



LA SEGURIDAD INFORMÁTICA SE CARACTERIZA AQUÍ COMO LA PROTECCIÓN DE:

- La confidencialidad: asegurar que la información es accesible solo para aquellos autorizados a tener acceso;
- b) La integridad: salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento;
- c) La disponibilidad: asegurar que los usuarios autorizados tengan acceso a la información y activos asociados cuando se requiera.

La seguridad informática se logra mediante la implementación de un apropiado sistema de controles, que pudieran ser políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software. Estos controles necesitan ser establecidos para asegurar que los objetivos específicos de seguridad se cumplan.

COMPONENTES DE SEGURIDAD INFORMÁTICA

Corresponden a los siguientes tipos:

1. Programas **antivirus y antispyware**.
2. **Cortafuegos o firewalls**, que bloquean accesos sin autorización a una red.
3. **Modelos de prevención de intrusiones o IPS**, que identifican amenazas de propagación rápida, como pueden ser los ataques de día cero o de hora cero.
4. **Diseño de redes privadas virtuales o VPN**, que proveen de un sistema de acceso remoto y seguro para los sistemas locales.



MECANISMOS DETECTIVOS EN SEGURIDAD INFORMÁTICA

- Los mecanismos de detección son los más complejos y son en los que se necesita tener alto grado de conocimientos técnicos dependiendo de la materia que se aborde, por ejemplo, seguridad de plataformas en línea, en específico de un tipo de bases de datos o tecnología como Wordpress, esto depende del sistema, aplicación o el ecosistema que tenga funcionando.



Estos mecanismos de detección tienen dos objetivos:

- Poder detectar el punto exacto del ataque para poder llegar a una solución y recuperarse del mismo, pero no siempre es posible esto, depende de los problemas que se afrontan.
- Detectar la actividad que se considera sospechosa y conocer lo sucedido, ya que si no se encuentra donde fue el ataque, lo mínimo que se necesita es saber qué fue lo que sucedió y partir de esa parte.

IMPORTANCIA DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

- La seguridad informática se ha convertido con el paso de los años en una de las principales preocupaciones de las empresas, ya que es un factor clave para su competitividad. La era digital exige que las organizaciones tengan una gestión ágil y efectiva y un alto nivel de disponibilidad de los recursos y plataformas TIC así como que conozcan cuáles son las normas de seguridad informática.
- Las políticas de seguridad informática ayudan a que todo el personal de la compañía acceda a los recursos tecnológicos y de la información proporcionados por la organización a través de unas pautas de actuación y protocolos con los que velar por la protección de los datos e informaciones sensibles para la empresa.

LA SEGURIDAD INFORMÁTICA VELA POR LOS SIGUIENTES TRES TIPOS DE CARACTERÍSTICAS DE LA INFORMACIÓN:

- **Disponibilidad.** La información debe ser accesible cuando sea necesaria su consulta. Es decir, debe estar disponible en el lugar, momento y forma solicitado por el personal autorizado.
- **Integridad.** Es la condición de seguridad que asegura que la información conserve el contenido original. Es decir, garantiza que la información sólo será modificada, creada y/o borrada por aquellas personas que estén autorizadas para ello. La firma digital es uno de los recursos empleados para velar por la integridad de la información.
- **Confidencialidad.** Es la característica que permite la legibilidad de la información únicamente para las personas autorizadas, es decir, restringe y garantiza la seguridad de la revelación de información a individuos, entidades o procesos no autorizados.

¿CÓMO FUNCIONA LA SEGURIDAD INFORMÁTICA EN REDES SOCIALES?

- Las redes sociales son parte de tu vida digital y muchas veces un referente de contenidos, noticias o trabajo. Las tienes instaladas en tus dispositivos y casi siempre abiertas en el navegador. Pero, si eres un fan de la seguridad, te habrás preguntado cuáles son esos protocolos informáticos que garantizan que tus datos y archivos personales estén protegidos

GRACIAS POR LLEGAR HASTA EL FINAL DEL CURSO

HASTA LA PRÓXIMA

