# Qué es la seguridad informática

En primer lugar antes de entrar en materia conviene definir ciertos conceptos que nos ayudaran a comprender de mejor manera el tema que se va tratar.

En los tiempos actuales la seguridad informática ha tomado un papel privilegiado en el área informática, ya que la mayoría de la personas saben los riegos que corren al estar expuestas a la gran red de redes es decir el Internet.

En la actualidad la mayoría de organizaciones están cambiando las formas de realizar sus negocios, y esto se debe en gran medida al avance tecnológico que ha hecho posible el desarrollo de un software cada vez más complejo que facilite la interconexión entre los distintos sitios de trabajo. Pero a pesar de que esto significa una mejora, también ha hecho posible que toda la información de una determinada empresa se encuentre en la red, entonces aquí viene la gran interrogante ¿Como la empresa asegura sus sistemas, sus redes y sobretodo su información confidencial, y aún más importante como sabe la empresa que la tecnología adquirida es segura?

La información es demasiado importante para dejarla en un segundo plano y por tanto hay que protegerla, conociendo como se perpetúa un ataque desde el punto de vista de un hacker y de esta manera tomar medidas para contrarrestarlo.

**El objetivo que persigue la seguridad informática, es identificar ciertas vulnerabilidades de un sistema y establecer contramedidas que imposibiliten que distintas amenazas exploten dichas vulnerabilidades.**

Pero hay que tener en cuenta la seguridad informática es dinámica, esto quiere decir que los sistemas son actualizados constantemente por la aparición de nuevas vulnerabilidades que atentan a la seguridad de la información

Las características que la seguridad informática debe garantizar son:

* Confidencialidad: La confidencialidad es la protección de los datos transmitidos de ataques pasivos. Con respecto a la liberación del contenido del mensaje, varios niveles de protección pueden ser identificados. El servicio más amplio protege todos los datos de usuario transmitidos entre dos usuarios durante un período de tiempo. Por ejemplo, si un circuito virtual se establece entre dos sistemas, esta amplia protección impediría la liberación de los datos de usuario transmitidos por el circuito virtual. Formas más estrechas de este servicio también se pueden definir, incluida la protección de un solo mensaje o incluso campos específicos dentro de un mensaje. Estos refinamientos son menos útiles que el enfoque amplio e incluso pueden ser más complejo y costoso de implementar.
* Integridad: Al igual que con la confidencialidad, la integridad se puede aplicar a un flujo de mensajes, un mensaje solo, o campos seleccionados dentro de un mensaje. Una vez más, el enfoque más útil y directo es la protección total del flujo.

Un servicio de integridad orientado a la conexión, que se ocupa de un flujo de mensajes, asegura que los mensajes son recibidos como enviados, sin duplicación, inserción, modificación, reorganización, o las repeticiones. La destrucción de los datos también está cubierta por este servicio. Por otro lado, un servicio de integridad sin conexión, en la que se ocupa de mensajes individuales sólo sin tener en cuenta cualquier contexto más amplio, generalmente proporciona protección contra la única modificación mensaje. Kent señala que un servicio híbrido se puede ofrecer para aplicaciones que requieren algún tipo de protección contra la reproducción y reordenamiento pero que no requieren la secuenciación estricta.

Podemos hacer una distinción entre el servicio con y sin recuperación. Debido a que el servicio de integridad se refiere a ataques activos, estamos preocupados con la detección en lugar de la prevención. Si se detecta una violación de la integridad, a continuación, el servicio puede simplemente informar de esta violación, y alguna otra porción de software de la intervención humana se requiere para recuperarse de la violación. La incorporación de mecanismos de recuperación automatizados es, en general, la alternativa más atractiva.

* Disponibilidad: Una variedad de ataques puede resultar en la pérdida o reducción de la disponibilidad. Algunos de estos ataques son susceptibles a las contramedidas automatizadas, tales como la autenticación y el cifrado, mientras que otros requieren algún tipo de acción física para prevenir o recuperarse de la pérdida de la disponibilidad de los elementos de un sistema distribuido.

# Terminología Básica

## Ataque

## Vulnerabilidad

## Hacker

## Evaluacion de un objetivo

## Exploit

## Zero-Day

## Vector de ataque

## Pentesting

“Una metodología de prueba en la que los evaluadores, por lo general trabajan bajo restricciones específicas, intentando evadir o derrotar a los elementos de seguridad de un sistema de información.” [NIST 800-53].

Pero además de una metodología son necesarias ciertas técnicas que nos permitan realizar una evaluación de las debilidades de un sistema informático, siendo este sistema informático no solo los servidores o sistemas de información, sino también a las aplicaciones web, la seguridad física de una empresa y todo lo que pueda ser vulnerado.

# Pentesting

## Objetivo del Pentesting

Los intrusos siempre van a aprovechar las vulnerabilidades de un sistema para poder ingresar de forma no autorizada, pero estas vulnerabilidades a menudo no solo se deben a la falta de actualización del sistema, sino que también se debe a descuidos y malas configuraciones por parte del administrador de la red o por los usuarios de la misma.

Los objetivos que persigue el Pentesting son:

* Evaluar un sistema o proyecto
* Conocer la situación real de la organización
* Medir y obtener una calificación objetiva del nivel de seguridad
* Mejora continua de la seguridad
* Cumplir con regulaciones y auditorias

## Tipos y alcances del Pentesting

Los proyectos de un servicio de pentesting pueden clasificarse en:

* Externo: En el cual se somete a los sistemas a pruebas de seguridad informática que simulan la realización de un ataque por parte de un atacante que se encuentra fuera del red interna
* Interno: En el cual se somete a los sistemas a pruebas de seguridad informática que simulan la presencia de un atacante que se encuentra en la red interna, es decir dentro de la organización o empresa.

Las pruebas de pentesting en general se realizan sobre:

* Sistemas (\*) informáticos
* Redes y configuración de un sistema
* Aplicaciones web
* Redes wireless

Como se mencionó anteriormente existen una serie de metodologías en el Pentesting, y son las siguientes:

* Black box (caja negra)
* Gray box (caja gris)
* White box (caja blanca)