



## ¿Qué es una vulnerabilidad en seguridad de la información?



Karen Quintero  
13 jun. 2022

Ahora las personas dependen más que nunca de la tecnología, tanto para el trabajo como para la vida personal, haciendo que la superficie de amenazas en los últimos años se ampliara de formas que antes no imaginábamos. Tenemos ataques cada vez más sofisticados, que van desde ransomware hasta DNS Spoofing, buscando aprovecharse de alguna vulnerabilidad en seguridad de la información.

Dicho esto, tanto consumidores como empresas en todo el mundo corren el riesgo de perder el acceso a la tecnología que utilizan e incluso de enfrentarse a pérdidas financieras que podrían ser desastrosas. Incluso, de acuerdo a datos recopilados, [los ciberdelincuentes podrían penetrar hasta en un 93% de las redes de empresas que intenten atacar.](#)

## ¿Qué es una vulnerabilidad en seguridad de la información?

Antes de entrar en la definición de vulnerabilidad en términos de ciberseguridad, vayamos por lo más simple. Una vulnerabilidad de seguridad parte de la capacidad que tienes para prevenir y resistir una vulneración a tus defensas.

Por ejemplo, una casa. En muchas ocasiones primero hay un cercado que separa la calle del patio. Así no entrará ningún intruso en propiedad privada. Sin embargo, en caso de que entrara, luego se encontraría con una puerta, alguna cámara u otro tipo de seguridad para que evitar que termine de llegar al interior del hogar. Hasta ahí todo bien. Pero, la casa tiene una ventana lateral que siempre está abierta y no cuenta con ningún tipo de protección, estamos hablando entonces de una vulnerabilidad que puede ser aprovechada por cualquier delincuente.



Lo mismo ocurre al referirnos a una vulnerabilidad en seguridad de la información. La diferencia es que aquí hablamos de debilidades en sistemas informáticos que pueden ser aprovechadas por ciberdelincuentes. Una vez que los atacantes encuentran una vulnerabilidad y la explotan, posiblemente consigan realizar un ataque con éxito.

## Diferencias entre vulnerabilidad, exploit y amenaza

Muchas veces cuando hablamos de ciberseguridad se entremezclan estos términos, por lo que no todas las personas entienden muy bien a qué hacen referencia. Primero, como veíamos previamente, una vulnerabilidad informática es una debilidad en un sistema que puede ser aprovechada por un delincuente al momento de perpetrar un ataque.

Ahora, un exploit, sería lo que conocemos como la explotación de vulnerabilidades. La explotación es el siguiente paso de un hacker después de encontrar una vulnerabilidad en el sistema de tu empresa. Básicamente, es el medio que se utiliza para aprovechar las vulnerabilidades y realizar actividades maliciosas.

Por último, una amenaza se refiere al caso hipotético en el que un atacante utiliza una vulnerabilidad para intentar penetrar al sistema. La amenaza en sí misma normalmente tendrá uno o varios exploits involucrados, ya que es una forma común en que los hackers hacen sus movimientos.

## Tipos de vulnerabilidades en ciberseguridad

Las vulnerabilidades en materia de ciberseguridad pueden dividirse en diversos tipos en función de una serie de criterios, como el lugar en el que se encuentra la vulnerabilidad, el modo en que podría utilizarse o la causa de la misma. Algunas categorías generales de estos tipos de vulnerabilidades son:

### Vulnerabilidades del sistema operativo

Se trata de las vulnerabilidades que existen dentro de un sistema operativo que los ciberdelincuentes pueden aprovechar para acceder a un dispositivo o causar daños. Por ejemplo, una cuenta de superusuario por defecto en el sistema operativo o un software de puerta trasera oculto.

### Vulnerabilidades de red

Estos son problemas que están relacionados con las debilidades del hardware o el software de una red, dejándola expuesta a una posible intrusión. Por ejemplo, un Wi-Fi inseguro o un firewall mal configurado.

## Vulnerabilidades humanas

El elemento humano es el eslabón más débil de la mayoría de arquitecturas de ciberseguridad, y los hackers lo saben. Un error humano puede exponer con mucha facilidad datos sensibles, interrumpir los sistemas o crear puntos de acceso explotables para los atacantes. Como ejemplo, tenemos el desconocimiento de qué es la ingeniería social y de cómo actuar en torno a este tipo de ataques.

## Vulnerabilidades de proceso

Algunas vulnerabilidades se generan a partir de controles en procesos específicos o por la falta de ellos. Este tipo de vulnerabilidades están muy relacionadas con las vulnerabilidades por error humano. Por ejemplo, el uso de contraseñas débiles o la ausencia de medidas de autenticación fuertes.

## Ejemplos de vulnerabilidades informáticas

Ya sabemos que una vulnerabilidad en seguridad de la información es una debilidad, una falla o un error dentro de un sistema de seguridad que tiene el potencial de ser aprovechado por un ciberdelincuente. Para que termines de hacerte una idea de qué se trata esto, aquí van algunos ejemplos:



- Autenticación comprometida: Esto ocurre cuando las credenciales de autenticación están comprometidas, implicando que las sesiones e identidades de los miembros de la organización pueden ser secuestradas por personas maliciosas.
- Malas configuraciones de seguridad: Cuando un componente del sistema de seguridad de la infraestructura TI puede ser aprovechado por los atacantes debido a un error de configuración.
- Inyección SQL: En este caso, un hacker puede insertar un código malicioso en el sitio web de una empresa con el fin acceder a datos protegidos, lo que puede conllevar a que los atacantes roben datos sensibles, falsifiquen identidades o lleven a cabo otro tipo de actividad maliciosa.

Por supuesto, en un sistema puede haber muchas más vulnerabilidades de seguridad. Lo importante es detectarlas a tiempo y tomar las medidas necesarias para corregirlas antes de que sea tarde.



## **Karen Quintero**

*Licenciada en Administración de empresas con Diplomado en Mercadotecnia por la Universidad Nacional Autónoma de México. Account Manager de iDric con experiencia en las soluciones de la marca ManageEngine y Sophos.*