## Tipos de vulnerabilidades en ciberseguridad

**Una vulnerabilidad es una debilidad que puede poner en peligro toda una red** y por eso deben existir los expertos en ciberseguridad para aliviar las amenazas y sus correspondientes tipos de vulnerabilidades.

## Los tipos de vulnerabilidades

**Existen,principalmente, dos maneras para descubrir las vulnerabilidades existentes**:

* La primera nace a través de búsquedas por parte de ciberdelincuentes que intentan sacar el máximo beneficio hasta que la vulnerabilidad se haga pública y se desarrollen los parches pertinentes.
* La segunda forma es a través de publicaciones en grupos de hacktivistas como The Shadow Brokers.

**Cierto es que una vulnerabilidad es capaz de tirar abajo un sistema completo en cuestión de minutos**, por eso para intentar frenarla es indispensable realizar controles de intrusión para así, minimizar riesgos.

**¿Conoces las vulnerabilidades más destacadas?**

* **Errores en la gestión de recursos**: Una aplicación permite que se consuma un exceso de recursos afectando a la disponibilidad de los mismos.
* **Error de configuración**: Problemas de configuración de software o de los servicios web.
* **Factor humano**: Negligencias causadas generalmente por la falta de formación y concienciación.
* **Validación de entrada**: Fallo en la validación de datos introducidos en aplicaciones.
* **Salto de directorio**: Fallo en la depuración de un programa, en la validación de caracteres especiales.
* **Permisos, privilegios y/o control de acceso**: Fallos en la protección y gestión de permisos

***Una vulnerabilidad es una debilidad que puede poner en peligro toda una red y por eso deben existir los expertos en ciberseguridad para aliviar las amenazas***

# **Vulnerabilidades informáticas**

Escrito por [Ginzo Technologies](https://ginzo.tech/blog/author/he34532_ginzo/) en junio 24, 2021. Publicado en [Actualidad digital](https://ginzo.tech/blog/category/actualidad-de-transformacion-digital/).

¿Sabías que en al menos cada tres discursos sobre ciberseguridad hablan acerca de las vulnerabilidades? sin embargo, son pocos los momentos donde realmente sabemos realmente cuál es su definición, a pesar de que es algo de suma importancia ya que son bastante explotadas en los ataques cibernéticos mediante una variedad de métodos que incluyen inyección SQL, desbordamientos de búfer, scripting entre sitios (XSS) y kits de explotación de código abierto.

Previo al nacimiento de la computación, era muy común que las maquinarias primitivas, para procesar información, contarán con programas desarrollados y diseñados netamente por humanos, lo que hacía bastante factible que tuvieran toda clase de errores en su código.

Con el tiempo dichos errores de programación han ido disminuyendo en gran parte por los nuevos lenguajes de programación que son más flexibles y, además, por la existencia de mucha información tanto impresa como Internet acerca de cómo operarlos. No obstante, esto no implica que los errores ya no existan, pues siguen encontrándose al ejecutar un programa, y que los ingenieros luego con actualizaciones van parcheando a medida que los van descubriendo o son alertados por los usuarios.

Dichos errores dan ventanas de vulnerabilidad en los sistemas, pues es una realidad que cada día más empresas digitalizan sus procesos, alojando información en la nube. Esto las expone a riesgos y es por eso que en este artículo te hablaremos sobre la definición de vulnerabilidades informáticas, qué tipos puedes encontrar, algunos ejemplos y cómo puedes protegerte para evitarlas.

## **¿Qué son las vulnerabilidades informáticas?**

Se considera una vulnerabilidad informática a toda aquella debilidad que presente un software o hardware, que puede ser explotada por un ataque cibernético para acceder de forma no autorizada al sistema informático, permitiendo que un atacante comprometa la integridad, disponibilidad o confidencialidad del sistema o los datos que allí procesa. Todo esto porque puede acceder a la memoria de un sistema, instalar malware y robar, destruir o modificar datos confidenciales

Pueden presentarse por fallos en el diseño, errores en la configuración o por procedimientos no robustos. Las más peligrosas son aquellas que permiten que el atacante ejecute códigos dañinos en el sistema comprometido.

Sin embargo, para que un atacante pueda aprovechar dicha vulnerabilidad, debe poder conectarse al sistema informático, y a pesar de esto son una de las principales causas por las cuales una empresa puede sufrir un ataque informático contra sus sistemas.

## **Los tipos más comunes de vulnerabilidades informáticas**

Existen muchos tipos de vulnerabilidades informáticas actualmente, y debes tenerlas en cuenta independientemente de la que sea, ya que cada una puede tener soluciones distintas, y se pueden producir en todas las etapas de desarrollo, implementación y mantenimiento de un software o sistema de información. Por ello te las listamos a continuación:

1. Vulnerabilidades ya conocidas en recursos instalados (sistemas o aplicaciones): son el tipo más común, son reconocibles porque las empresas que desarrollaron la aplicación o el sistema conocen perfectamente los puntos débiles y, por tanto, ya han creado soluciones inmediatas para solventar. Para dar respuesta a estas vulnerabilidades se usan parches y actualizaciones para mejorar esos errores que pueda presentar el sistema instalado.
2. Vulnerabilidades ya conocidas en recursos no instalados: en este caso también se conocen las vulnerabilidades, pero no te afectarán porque se relacionan con aplicaciones que no están instaladas. Por tanto, aunque los desarrolladores de las aplicaciones instaladas conozcan la debilidad en cuestión, tu no deberás actuar en consecuencia porque realmente no afecta tu sistema, puesto que no se usa dicha aplicación por el momento.

No obstante, siempre es bueno que tengas conocimiento de dichas vulnerabilidades en caso de que a futuro tengas que usar estas aplicaciones en tu entorno informático.

* Vulnerabilidades no conocidas: también llamadas vulnerabilidad de día cero, en este caso nadie, ni siquiera la empresa desarrolladora sabe frente a qué tipos de debilidades se está enfrentando, puesto que no han sido detectadas. Así que estas resultan ser las más peligrosas, ya que los ciberdelincuentes las aprovechan para hacer ataques a distintos sistemas informáticos. Permite que se genere un mercado ilegal de compra-venta de vulnerabilidades.

Además de las vulnerabilidades ya presentadas, existen otras como:

* Vulnerabilidades de diseño: se deben a fallos en el diseño de protocolos de redes o deficiencias políticas de seguridad.
* Vulnerabilidades de implementación: se dan por errores de programación o descuidos de los fabricantes, también por presencia de “puertas traseras” en los sistemas informáticos.
* Vulnerabilidades por falta de mantenimiento: cuando los softwares ya no reciben actualizaciones por el fabricante.
* Vulnerabilidades por uso o causadas por factor humano: son las menos consideradas, pero en algunos casos pueden tener mayor impacto que todas las anteriores. Se asocian con falta de formación o conciencia en los usuarios o empleados de una empresa sobre prácticas de seguridad. Por configuración inadecuada de los sistemas informáticos, existencia de herramientas que facilitan los ataques y por limitaciones gubernamentales de tecnología de seguridad.

Por su parte, se pueden clasificar globalmente de la siguiente forma:

* Vulnerabilidades de desbordamiento de buffer: es cuando se da la situación donde un programa no controla la cantidad de datos que se copian en buffer. Esto significa que si dicha cantidad es mayor a la capacidad del buffer entonces los bytes sobrantes se van a almacenar en zonas de la memoria adyacentes, de manera que se sobreescriba contenido original. Esta vulnerabilidad es aprovechable para ejecutar códigos que nos de privilegios de administrador.
* Vulnerabilidades de condición de carrera (race condition): se da cuando varios procesos acceden al mismo tiempo en un recurso compartido.
* Vulnerabilidades de error de formato de cadena (format string bugs): ocurren por aceptar sin validación la entrada de datos proporcionada por el usuario. Corresponde a un error de programación y el lenguaje más afectado es C/C++. Este ataque puede conducir inmediatamente a ejecutar código arbitrario y a revelar información.
* Vulnerabilidades de Cross Site Scripting (XSS): lo conforman todos los ataques que permitan ejecutar scripts como VBScript o JavaScript, en el contexto de otro sitio web. Pueden encontrarse en cualquier aplicación que tenga por objetivo final la presentación de información en un navegador web. Se usa para la realización de phishing, donde la víctima al ingresar a un sitio web, en la barra de dirección ve una URL pero realmente está en otra, entonces la víctima introduce su contraseña y realmente se la está enviando al atacante.
* Vulnerabilidades de Inyección SQL: se da cuando se inserta o inyecta un código SQL invasor dentro del código SQL programado, con la finalidad de alterar el funcionamiento normal de dicho programa, todo esto para lograr que sea ejecutada la porción de código «invasor» incrustado, dentro de la base de datos.
* Vulnerabilidades de denegación del servicio: esto causa que el recurso sea inaccesible para usuarios legítimos: causa la pérdida de conectividad de red debido al consumo de ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.
* Vulnerabilidades de ventanas engañosas (Window Spoofing): son aquellas donde le dicen al usuario que es ganador de un determinado premio, siendo eso mentira, pues lo único que desean es que el usuario de su información confidencial. Por su parte, hay otro tipo de ventanas donde si haces clic van a obtener datos del ordenador para posteriormente realizar el ataque.

## **Ejemplos de vulnerabilidad y amenazas informáticas**

Antes de entrar en este punto, debes saber que amenazas y vulnerabilidades no son lo mismo. La primera corresponde a todas aquellas acciones que aprovechan una vulnerabilidad para así atacar o invadir un sistema informático, en su mayoría son ataques externos, pero también existen las amenazas internas.

Por su parte, como ya lo hemos mencionado, las vulnerabilidades corresponden a los fallos o debilidades que presenta un sistema de información, y que a su vez lo pone en riesgo en cuanto a su seguridad. Puede ser producida por un error de configuración o fallos del sistema. Este es el paso 1 para proceder con una amenaza. En función de esto, te presentamos algunos ejemplos de vulnerabilidades informáticas más comunes:

1. Contraseñas débiles.
2. Software que ya está infectado con virus.
3. Bugs.
4. Falta de cifrado de datos.
5. Falta de autorización.
6. Redireccionamiento de URL a sitios no confiables.
7. Falta de autenticación para una función crítica.
8. Carga sin restricciones de tipos de archivos peligrosos y descarga de códigos sin controles de integridad.
9. Dependencia de entradas no confiables en una decisión de seguridad.
10. Cross-site scripting y falsificación.
11. Errores de configuración.
12. Errores en la gestión de recursos.
13. Errores en los sistemas de validación.
14. Errores que permiten el acceso a directorios.
15. Errores en la gestión y asignación de permisos.

Asimismo, algunos ejemplos de amenazas informáticas son:

1. Ataques por denegación de servicio distribuido (DDoS).
2. Amenazas de malware, entre los que se encuentran los virus, gusanos, troyanos, ransomware y las keyloggers.
3. Ataques de inyección SQL.
4. Ingeniería social.
5. APT o amenazas persistentes avanzadas.
6. Botnets.
7. Redes sociales.
8. Servicios en la nube.

## **¿Cómo protegerse y evitar las vulnerabilidades informáticas?**

Para protegerte y evitar tener vulnerabilidades informáticas, lo primero que debes hacer es realizar un inventario de tus activos TI: servidores, infraestructura de redes, aplicaciones y periféricos (impresoras, etc.). Luego tendrás que proceder a hacer un análisis de posibles amenazas que pudiera sufrir el sistema informático mediante pruebas de penetración y además estimar las pérdidas que podrían causar dichas amenazas y estudiar cuáles son las probabilidades de que ocurran.

Hecho lo antes mencionado, entonces deberás aplicar las medidas correctivas necesarias, para reparar vulnerabilidades o reducir las amenazas. Posteriormente debes diseñar la política de seguridad que vas a implementar, estableciendo las responsabilidades y reglas que se deberán seguir para así evitar las vulnerabilidades o minimizar los efectos en caso de que se llegue a producir una amenaza.

* Política de seguridad: se refiere a un documento para definir las directrices organizativas en cuanto a seguridad, se implementa a través de mecanismos de seguridad basados en herramientas destinadas a proteger el sistema, apoyándose en normas que abarcan áreas más específicas. Entre los que se encuentran los mecanismos de prevención, de detección y de recuperación. A su vez, cuentan con un subgrupo de mecanismos, denominado de análisis forense, destinado a regresar el sistema a su estado normal y a averiguar cuál fue el alcance del ataque, lo que hizo el intruso en el sistema y qué puerta usó para ingresar al sistema, para entonces prevenir posteriores ataques.
* Establece mecanismos de prevención, constituidos por el de identificación y autentificación, de control de acceso, de separación y de seguridad en las comunicaciones.
* Concientiza a todo el personal de la empresa para evitar vulnerabilidades informáticas de factor humano.
* Realiza copias de seguridad periódicamente y mantén una gestión adecuada para las contraseñas.
* Mantente actualizado en cuanto a las últimas vulnerabilidades conocidas, puedes apoyarte en el repositorio de vulnerabilidades del CERTSI.
* Asegúrate de cumplir con normas, como la ISO 27001.

Con estos consejos de seguridad cerramos este artículo, no sin antes recordar que desde el momento de la creación de una empresa ya se expone a vulnerabilidades y amenazas, de allí que sea imprescindible la realización de un análisis de riesgos adecuado y llevar una correcta gestión de vulnerabilidades que logre **prevenir** y **proteger** a la empresa de ataques.

Otra fuente: [Top 10 vulnerabilidades web de 2021 | INCIBE](https://www.incibe.es/protege-tu-empresa/blog/top-10-vulnerabilidades-web-2021)

[Vulnerabilidad informática: ¿cómo protegerse? (mdcloud.es)](https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/)