# ¿Cómo definir las amenazas de seguridad en tus activos informáticos?

Son diversas las **amenazas que pueden afectar a los activos de información** de una organización, pero pocas son las personas que saben **cómo detectarlas y priorizarlas correctamente**, ya que no tienen mucha idea de cómo deben [enfocar la ciberseguridad en el negocio.](https://blog.easysec.com.mx/2022/06/como-enfocar-la-ciberseguridad-al-negocio.html)

Primero, me gustaría definir lo que es una amenaza. Según el ISO/IEC 27001, una amenaza **es una situación que desencadena en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de los activos de información**.

Otra definición de acuerdo al [*INCIBE*](https://www.incibe.es/), nos dice que una amenaza es **toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información**, es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestro sistema.

Entonces, si partimos desde la definición, **cualquier cosa que pueda afectar la operación principal de una organización, sea cual sea, debe considerarse una amenaza.**

Ya teniendo esto claro, ahora tenemos que definirlas para la empresa, y esto depende mucho de la actividad principal del negocio. Una vez que se cuenta con [**el listado de activos de la organización**](https://blog.easysec.com.mx/2021/10/inventario-de-activos.html), así como la categorización de cada uno de ellos, se puede proceder a realizar el listado de amenazas.

## **¿Cómo definir las amenazas de seguridad en tus activos informáticos?**

Existen metodologías como la **MAGERIT** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), que te ayudan en este proceso, pero lo explicaré de otra forma.

Primero, tienes que saber que existen distintos tipos de amenazas, por ejemplo:

* Desastres naturales, como terremotos, inundaciones, tsunamis, incendios forestales.
* Desastres de origen industrial, como incendios, fallas en los sistemas de comunicación, electricidad o aplicaciones.
* Errores humanos no intencionales.
* Ataques intencionales o maliciosos.
* [Malware](https://blog.easysec.com.mx/2022/08/que-es-el-malware-y-como-funciona.html), [suplantación de identidad](https://blog.easysec.com.mx/2021/08/que-es-la-suplantacion-de-identidad.html), manipulación, repudio, robo, divulgación de información, denegación de servicio, etc.

Como podrás darte cuenta, **las amenazas no son únicamente informáticas**, ya que **pueden provenir de** [**personas dentro**](https://blog.easysec.com.mx/2019/11/insiders.html) **o fuera de la organización**, e incluso eventos ajenos a ella.

Ahora que conoces algunas amenazas, puedes darte una idea de las que pueden afectar a los activos más críticos de tu empresa y así es como se pueden definir, listando todo lo que se nos ocurra, claro en conjunto con un equipo, ya que será más fácil debido a que no todos tienen la misma perspectiva.

Te recomiendo que dentro del proceso de definición de amenazas se incluyan gerentes, directores y especialistas de cada área de tu organización, pero principalmente las que tengan que ver con los activos críticos.

Un ejemplo para que quede más claro es el siguiente: Supongamos que tenemos una página de comercio electrónico donde a diario tu empresa vende miles de productos siendo el servidor de alojamiento y la página como tal, los activos más críticos.

### **¿Qué amenazas podrían poner en riesgo el activo o servidor de comercio electrónico?**

* El servidor podría sufrir daño físico por falta de mantenimiento.
* El servidor podría sufrir un daño lógico por falta de mantenimiento.
* La información contenida podría ser modificada por usuarios con acceso.
* Puede sufrir un ataque informático por falta de controles de seguridad.
* Podría sufrir una infección de malware.
* Pueden ser manipulados los datos del servidor.
* Pueden conectarse los administradores a través de un escritorio remoto.
* Podría perderse la disponibilidad por una falla con el enlace de internet.
* Podrían perder disponibilidad por una falla de energía eléctrica.
* Puede perder disponibilidad al recibir miles de peticiones que no pueda procesar.
* Podría un terremoto sepultar el servidor bajo los escombros perdiendo disponibilidad.

Existen muchas más amenazas que podrías agregar a la lista, pero esto solo es un ejemplo sencillo para que puedas tener una mejor idea de cómo se realiza.

Una vez detectadas las amenazas que podrían poner en riesgo a nuestros activos críticos, será más sencillo evaluar qué controles de seguridad tecnológicos, políticas y planes implementar para disminuir la probabilidad de que alguna de ellas se materialice y afecte la operación del negocio.