# **Fáciles pasos a seguir para un Análisis de riesgo de Seguridad**

# 

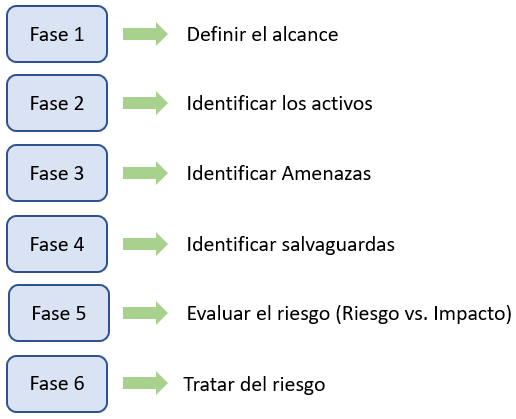
# Hoy en día es primordial realizar un análisis de riesgo de [seguridad](https://www.a2secure.com/) en las empresas para definir proyectos e iniciativas de seguridad de la información y a su vez para cumplir con varias normativas de seguridad, como la GDPR y PCI DSS. Para cumplir con ello, se deben tomar en consideración varios factores a la hora de iniciar un análisis de riesgo, escogiendo la mejor metodología para que sea un proceso fácil y factible.

En primer lugar, se debe pensar en crear un Plan Director de Seguridad, donde se detallen los diferentes proyectos de seguridad de la información, destinado a reducir los riesgos desde una evaluación inicial y mitigar algún tipo de posibles incidentes de ciberseguridad.

Luego de ello, debemos escoger entre los dos tipos de análisis de riesgo:

* **Cualitativos:** la prioridad de cada riesgo será calculada en base a diferentes variables como: probabilidad de ocurrencia, frecuencia de ocurrencia, disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, entre otros. Este método de análisis de riesgos es uno de los más utilizado en la toma de decisiones en proyectos empresariales, los empleados se apoyan en su juicio, experiencia e intuición para la toma de decisiones.
* **Cuantitativos:** se realizan sobre riesgos que han sido catalogados como prioritarios durante la etapa de análisis cualitativo. Este proceso asignará un valor numérico.

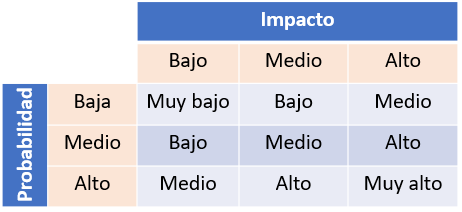
Cabe destacar que dependiendo de la metodología escogida para realizar el análisis de riesgo, existen diferentes fases o etapas a realizar, sin embargo, en este blog señalamos un conjunto de las fases más comunes que son utilizadas en los análisis de riesgo.



1. **Definir el Alcance:** en esta primera fase se debe definir el alcance del estudio. Es una tarea bastante importante ya que de ello se seleccionarán las áreas estratégicas para mejorar la seguridad en los sistemas, procesos y elementos dentro del alcance del Plan Director de Seguridad. *Por ejemplo:* Realizar un Análisis de riesgo en el entorno PCI DSS o análisis de riesgo sobre los procesos de Desarrollo.
2. **Identificación de activos:** se debe definir los activos involucrados en el estudio, por ejemplo: Hardware, software, sistemas de comunicación, aplicaciones, instalaciones, personal, proveedores, servicios subcontratados, entre otros.
3. **Identificación de amenazas:** se deben identificar las amenazas a las que se encuentran expuestos cada uno de ellos. El catálogo es sumamente amplio, pero se debe enfocar para cada caso, *por ejemplo:* si se quiere evaluar las amenazas dirigidas a un servidor físico, se puede considerar daños por fuego, por agua, averías de origen físico o lógicos, errores del administrador, denegación de servicios, robo de equipos, entre otros.
4. **Identificación de las salvaguardas:** En esta fase se debe estudiar las características de nuestros activos para buscar los puntos más vulnerables y conseguir una posible solución para solventar los riesgos a los que se encuentran expuestos y/o limitar el daño causado. *Por ejemplo:* Si se encuentran con servidores que tienen el software desactualizado y no tienen antivirus instalado, entonces debe considerarse como salvaguardas: actualizar el software del servidor, configurar el servidor para alertas a las nuevas actualizaciones e instalar un antivirus.
5. **Evaluación del riesgo:** Ya teniendo las primeras cuatro fases detalladas anteriormente, podremos calcular el riesgo, en base a la probabilidad de que la amenaza se materialice y el impacto que pueda causar en el negocio.

Para calcular el riesgo si decidimos realizarlo por el **método cuantitativo** se calculará multiplicando los factores: Riesgo = Probabilidad x Impacto.

En cambio, si consideramos realizar el análisis de riesgo por el **método cualitativo** se usará la siguiente matriz de riesgo:



Para esta evaluación se debe tomar en cuenta las vulnerabilidades y salvaguardas existentes. *Por ejemplo:* Existe una caída de un Firewall principal el cual puede causar una afectación e impacto importante para el negocio, sin embargo, si se tiene un backup o firewall redundante se puede indicar un impacto “medio” ya que con el firewall redundante no se verá afectado el servicio y no impactara el negocio.

1. **Tratar el riesgo:** Con el riesgo ya calculado se deben solventar y/o tratar los riesgos que superen el límite establecido por nosotros en el Plan Director De Seguridad. Por ejemplo: tratar los riesgos con valor mayor a 5 para los métodos cualitativos, o atacar los riesgos superiores a “Medio” si trabajamos con el método cuantitativo. Para tratar el riesgo existen 4 estrategias a seguir:
2. **Transferir el riesgo a un tercero:** *por ejemplo*: se contrata a un proveedor de servicio para procesar los datos de tarjetas de clientes.
3. **Eliminar el riesgo:** *por ejemplo:* eliminar todos los datos de tarjetas de clientes del entorno estudiado si no es estrictamente necesario.
4. **Asumir el riesgo:** *por ejemplo*: implementar una base de datos y segmentar la red es muy costoso por lo que se asume el riesgo. Asumir el riesgo siempre debe estar documentado.
5. **Implantar medidas para mitigar los riesgos:** se debe implantar una serie de proyectos para mitigar el riesgo de cada activo. *Por ejemplo:* se debe realizar escaneos de seguridad externos/internos trimestralmente en el entorno estudiado para solventar las vulnerabilidades.

Cabe destacar que los análisis de riesgo son de suma importancia para las empresas por la información que nos proporciona y también por las medidas de mitigación que se presentan para [mejorar la seguridad de nuestra empresa.](https://www.a2secure.com/)

Para finalizar se invita a las diferentes empresas a realizar este proyecto y mantener un equilibrio entre el coste, la importancia del activo para la empresa y el nivel del riesgo.

Fuente: [Fáciles pasos a seguir para un Análisis de riesgo de Seguridad | A2Secure](https://www.a2secure.com/blog/faciles-pasos-a-seguir-para-un-analisis-de-riesgo-de-seguridad/)