







# Análisis y Gestión de RIESGOS

[illegible]

# Keren Jodet Castellanos Zapata



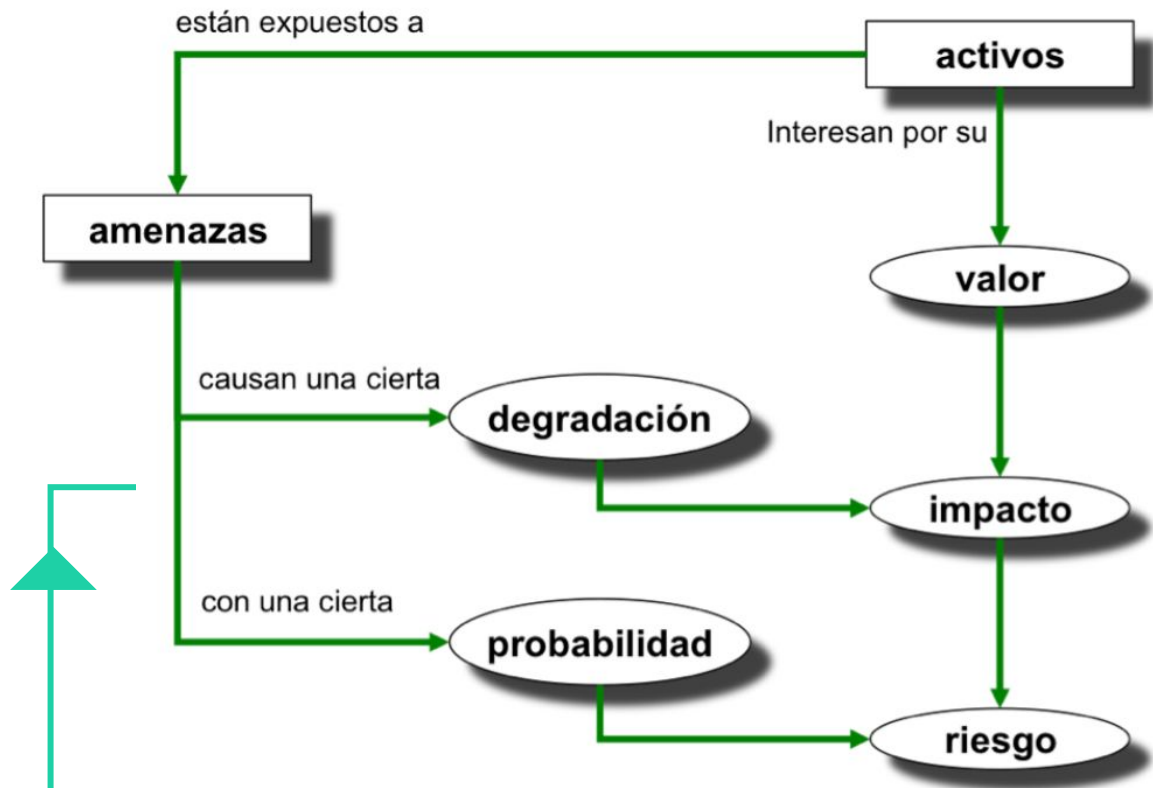


**Análisis de Riesgo**

# Método de análisis de riesgos

El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra).

**Elementos del análisis de riesgos**



# Elementos en el análisis de riesgos

## Amenazas

Las amenazas son cosas que ocurren. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.



## Impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.



## Salvaguardas

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.



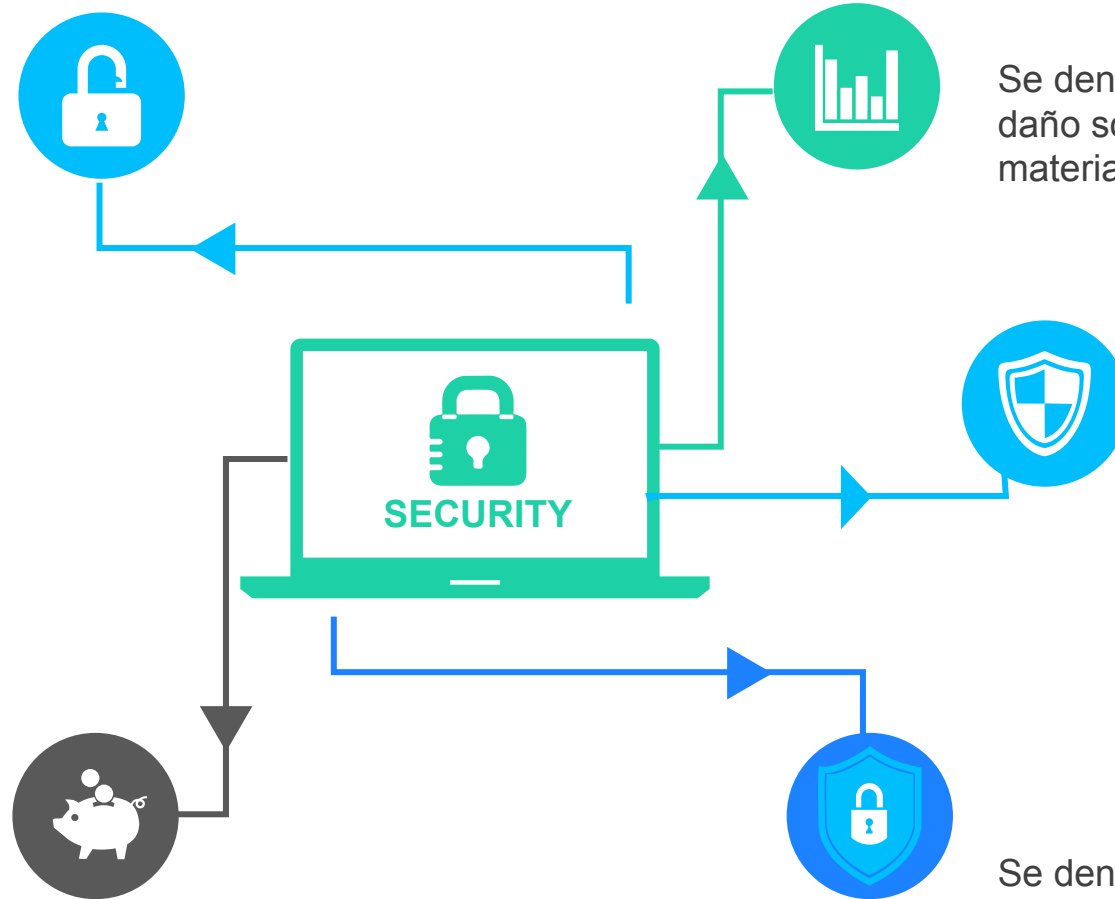
## Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.



## Riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema.



# Tareas del análisis de riesgos

# Caracterización de Activos

- Identificación de los activos
- Dependencias entre activos
- Valoración de los activos

# Caracterización de Amenazas

- Identificación de las amenazas
- Valoración de las amenazas

# Caracterización de Salvaguardas

- Identificación de las salvaguardas pertinentes
- Valoración de las salvaguardas

## Estimación del estado de Riesgo

- Estimación del impacto
- Estimación del riesgo



# Caracterización de los activos



Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

El resultado de esta actividad es el informe denominado “modelo de valor”.

Sub-tareas:

- Identificación de los activos
- Dependencias entre activos
- Valoración de los activos

# Caracterización de las amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

El resultado de esta actividad es el informe denominado “mapa de riesgos”.

Sub-tareas:

- Identificación de las amenazas
- Valoración de las amenazas





# Caracterización de las salvaguardas

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.



El resultado de esta actividad se concreta en varios informes:

- declaración de aplicabilidad
- evaluación de salvaguardas
- insuficiencias (o vulnerabilidades del sistema de protección)

Sub-tareas:

- Identificación de las salvaguardas pertinentes
- Valoración de las salvaguardas



# Estimación del estado de riesgo

Esta actividad procesa todos los datos recopilados en las actividades anteriores para

- realizar un informe del estado de riesgo: estimación de impacto y riesgo
- realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas

Sub-tareas:

- Estimación del impacto
- Estimación del riesgo





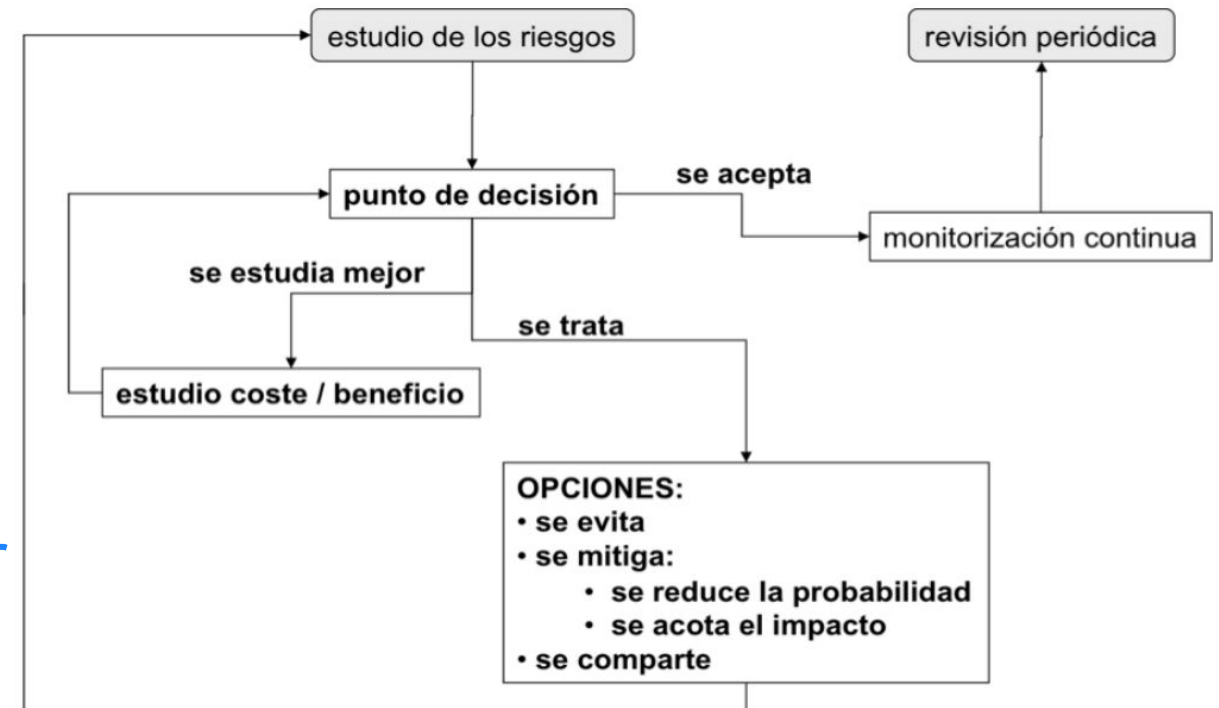
# Gestión de Riesgo

# Proceso de gestión de riesgos

El resultado del análisis es sólo un análisis. A partir de él disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados=, de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.

A partir de aquí, las decisiones son de los órganos de gobierno de la Organización que actuarán en 2 pasos:

- paso 1: evaluación
- paso 2: tratamiento



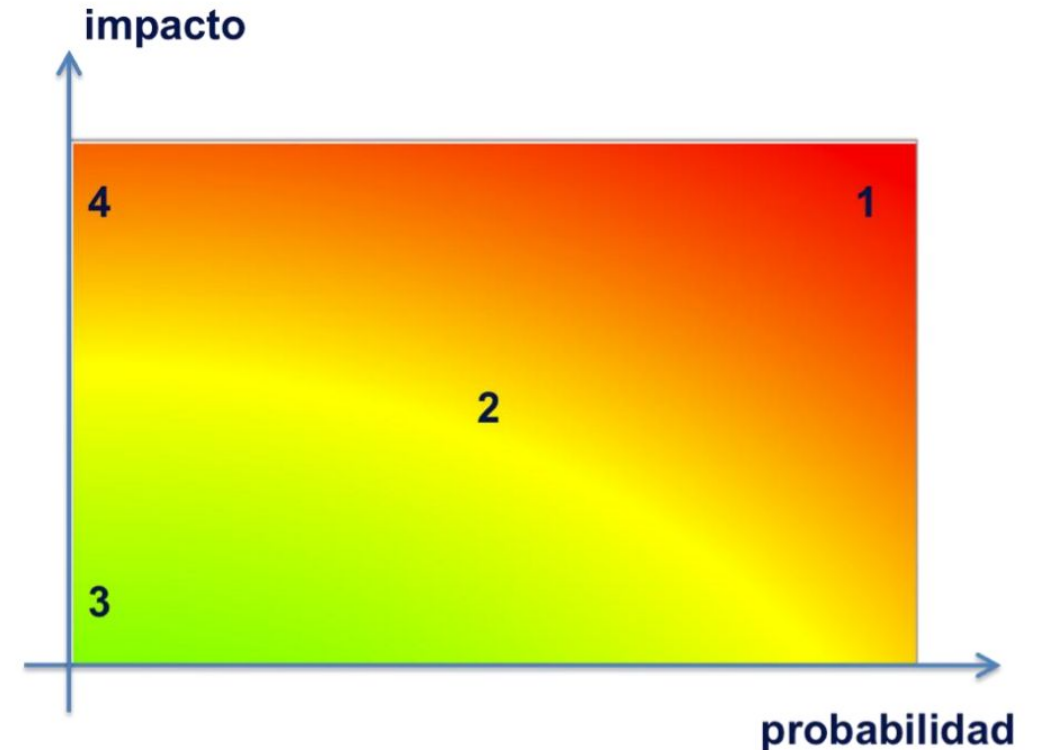
**Decisiones de tratamiento de los riesgos**



# Tratamiento de los riesgos

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

- zona 1 – riesgos muy probables y de muy alto impacto.
- zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.
- zona 3 – riesgos improbables y de bajo impacto.
- zona 4 – riesgos improbables pero de muy alto impacto.



Tratamientos por:

- Eliminación
- Mitigación
- Compartición
- Financiación

# Tratamiento del riesgo: eliminación

La eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable.

Esta opción puede tomar diferentes formas:

- Eliminar cierto tipo de activos, y emplear otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos, etc.
- Reordenar la arquitectura del sistema (el esquema de dependencias en nuestra terminología) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas. Por ejemplo: segregar redes, desdoblar equipos para atender a necesidades concretas, alejando lo más valioso de lo más expuesto, etc.



# Tratamiento del riesgo: mitigación



La mitigación del riesgo se refiere a una de dos opciones:

- reducir la degradación causada por una amenaza (a veces se usa la expresión ‘acotar el impacto’)
- reducir la probabilidad de que una amenaza de materializa

En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas. En términos de madurez de las salvaguardas: subir de nivel.

# Tratamiento del riesgo: eliminación



Tradicionalmente se ha hablado de ‘transferir el riesgo’. Como la transferencia puede ser parcial o total, es más general hablar de ‘compartir el riesgo’.

Hay dos formas básicas de compartir riesgo:

- Riesgo cualitativo: se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades.
- Riesgo cuantitativo: se comparte por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias.



# Tratamiento del riesgo: financiación

Cuando se acepta un riesgo, la Organización hará bien en reservar fondos para el caso de que el riesgo se concrete y haya que responder de sus consecuencias. A veces se habla de 'fondos de contingencia' y también puede ser parte de los contratos de aseguramiento. Normalmente esta opción no modifica nada del sistema y nos vale el análisis de riesgos disponible.

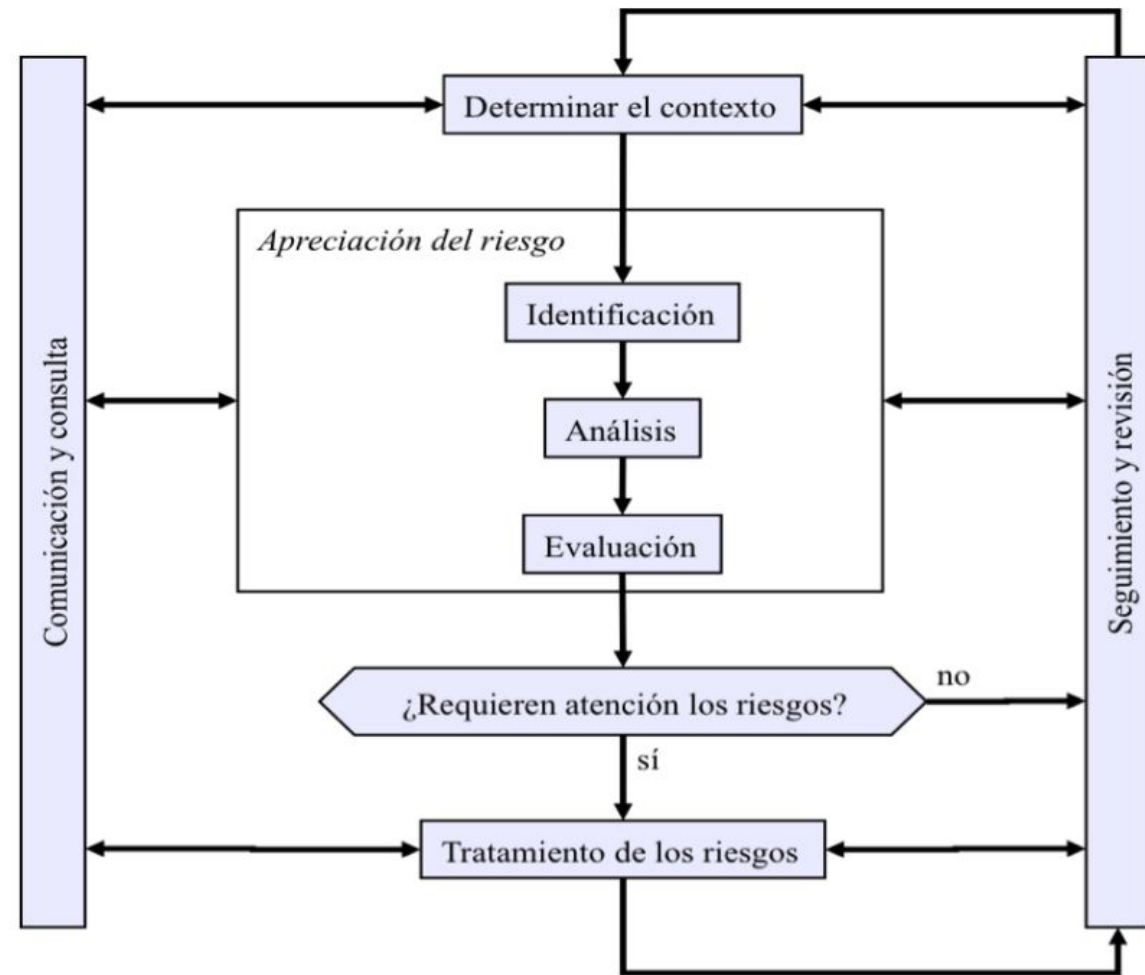
Los órganos de gobierno han adoptado una propuesta de tratamiento

- evitar el riesgo
- prevenir: mitigar la probabilidad de que ocurra
- mitigar el impacto si ocurriera
- compartir el riesgo con un tercero
- asumir el riesgo



# Proceso de gestión de riesgos

- Se definen los roles y responsabilidades respecto de la gestión de riesgos.
- Se establece el contexto de gestión de riesgos.
- Se establecen los criterios de valoración de riesgos y toma de decisiones de tratamiento.
- Se interpretan los riesgos residuales en términos de impacto en el negocio o misión de la Organización.
- Se identifican y valoran las opciones de tratamiento de los riesgos residuales.



# Contexto de gestión de riesgos

Hay que identificar el entorno en cuanto competencia y posicionamiento respecto de la competencia.

Hay que identificar el contexto interno en el que se desenvuelve la actividad de la Organización: política interna, compromisos con los accionistas y con los trabajadores o sus representantes.

La identificación del contexto en el que se desarrolla el proceso de gestión de riesgos debe ser objeto de una revisión continua para adaptarse a las circunstancias de cada momento.



# Criterios de valoración de riesgos



Hay que establecer reglas y/o criterios para tomar decisiones de tratamiento:

- umbrales de impacto
- umbrales de probabilidad
- umbrales combinados de impacto y probabilidad
- umbrales de nivel de riesgo
- impacto en la reputación de la Organización o de las personas responsables
- impacto en la posición de competencia
- impacto comparado con otras áreas de riesgo: financiero, regulatorio, medioambiental, seguridad industrial, etc
- combinaciones o concurrencia de riesgos que pudieran tener un efecto combinado
- amenazas especialmente sensibles



# Formas de reducir los riesgos



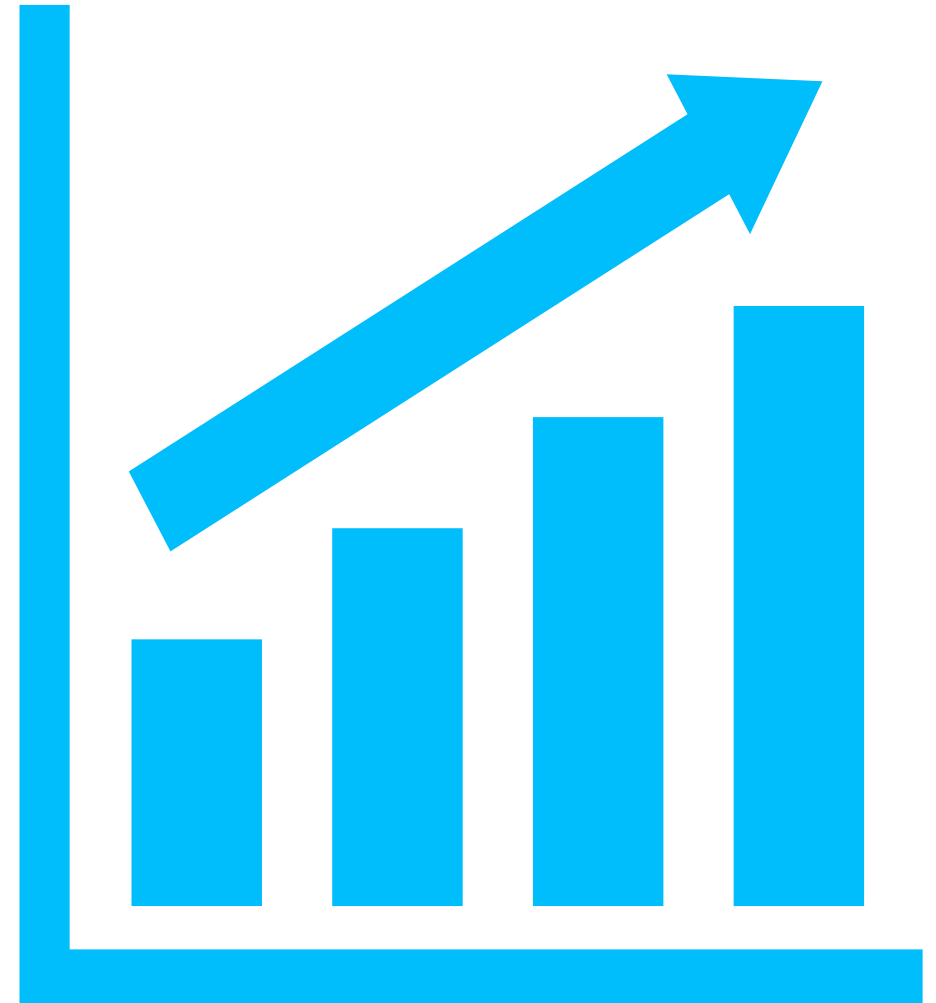
Hay múltiples formas de reducir el riesgo:

- eliminar el riesgo eliminando sus causas: información tratada, servicios prestados, arquitectura del sistema,
- reducir o limitar el impacto
- reducir la probabilidad de que la amenaza ocurra
- en el caso de amenazas derivadas de defectos de los productos (vulnerabilidades técnicas): reparar el producto (por ejemplo, aplicar los parches del fabricante)
- implantar nuevas salvaguardas o mejorar la calidad de las presentes
- externalizar partes del sistema
- contratar seguros de cobertura

# Seguimiento en gestión de riesgos

El análisis de los riesgos es un ejercicio formal, basado en múltiples estimaciones y valoraciones que pueden no compaginarse con la realidad. Es absolutamente necesario que el sistema esté bajo monitorización permanente. Los indicadores de impacto y riesgo potenciales son útiles para decidir qué puntos deben ser objeto de monitorización.

Y debe estar preparado un sistema de detección de posibles incidentes (en base a indicadores predictivos) así como un sistema de reacción a incidentes de seguridad.



# Servicios subcontratados



Cuando dependemos de terceros es especialmente importante conocer el desempeño de nuestros proveedores, tanto con un buen sistema de reporte, escalado y resolución de los incidentes de seguridad, como en el establecimiento de indicadores predictivos. Del análisis de dependencias realizado durante el análisis de riesgos, tenemos información de en qué medida y en qué dimensiones de seguridad dependemos de cada proveedor externo.

De esta información se sigue qué elementos debemos monitorizar para asegurarnos que satisfacen nuestros requisitos de seguridad

# ¿QUÉ ES LA GESTIÓN DE RIESGOS?

BENEFICIOS, TIPOS Y ETAPAS



CONDUCE TU EMPRESA





*¡Gracias!*