

Ciberseguridad - Continuidad del negocio



1 - Introducción a la gestión de riesgo



- 1.1 Introducción la gestión de riesgo
- 1.2 Activo, amenaza, vulnerabilidad, impacto y probabilidad
- 1.3 ¿Cómo se mide el nivel de riesgo?
- 1.4 ¿Qué hacer con los riesgos?
- 1.5 El proceso de gestión de riesgos de seguridad de la información
- 1.6 Recomendaciones y bibliografía



Introducción al contenido



1.1 Introducción la gestión de riesgo

La gestión de riesgos está presente, con mayor o menor protagonismo, en distintos ámbitos de la sociedad y la empresa. Los siguientes son algunos ejemplos de la gestión de riesgos:

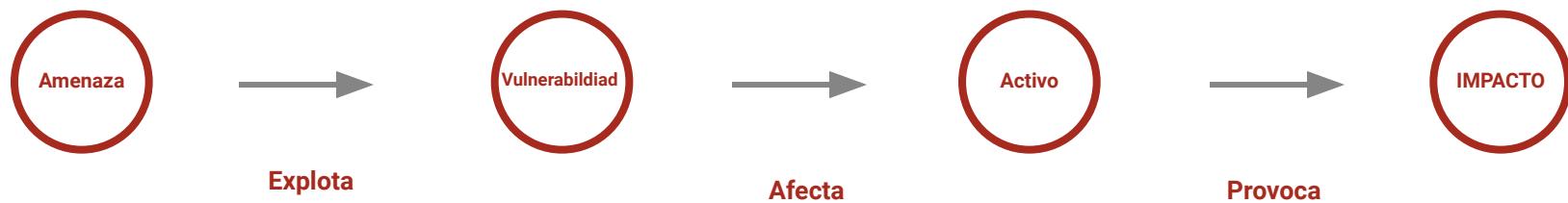
- ... laborales
- ... alimentarios
- ... bancarios, financieros
- ... corporativos, de proyectos
- ... medioambientales
- ... de seguridad de la información



1.2 Activo, amenaza, vulnerabilidad, impacto y probabilidad



1.2 Activo, amenaza, vulnerabilidad, impacto y probabilidad



1.3 ¿Cómo se mide el nivel de riesgo?

$$\text{Riesgo} = \text{Activo} \times \text{Amenaza} \times \text{Vulnerabilidad}$$



1.4 ¿Qué hacer con los riesgos?

Las actividades cuyo objetivo es mantener el riesgo por debajo del umbral fijado se engloban en lo que se denomina Gestión del riesgo. Las organizaciones que decidan gestionar el riesgo para su actividad deberán realizar dos grandes tareas:

- Análisis de riesgo
- Tratamiento de riesgo



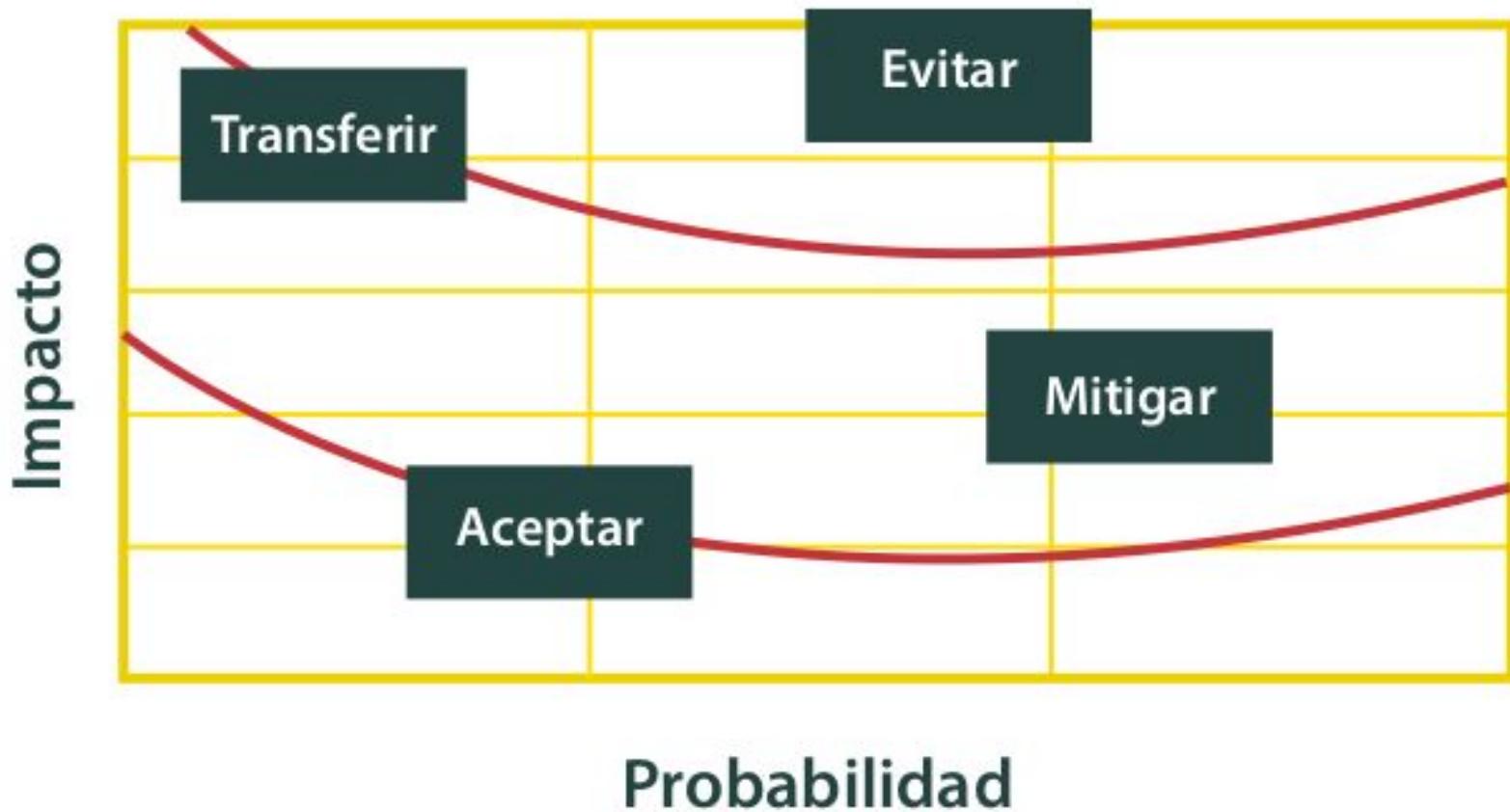
1.4 ¿Qué hacer con los riesgos?

Para el tratamiento de riesgos las empresas cuentan, entre otras, con las siguientes opciones:

- Evitar o eliminar el riesgo
- Reducirlo o mitigarlo
- Transferirlo, compartirlo o asignarlo a terceros
- Aceptarlo



1.4 ¿Qué hacer con los riesgos?



1.5 El proceso de gestión de riesgos de seguridad de la información

La gestión de riesgos de seguridad de la información es un proceso que consiste en:

- Comunicación
- Establecimiento del contexto
- Valoración del riesgo
- Tratamiento del riesgo y aceptación del riesgo
- Revisión y monitorización



1.5 El proceso de gestión de riesgos de seguridad de la información

Comunicación

Durante todo el proceso las acciones de comunicación se sucederán para mantener informada a la dirección y a la plantilla. Igualmente se recibirá información de los procesos y los interesados.

Con estas acciones se consigue difundir la información necesaria para conseguir el consenso de los responsables y los afectados por las decisiones que se tomen.



1.5 El proceso de gestión de riesgos de seguridad de la información

Estableciendo el contexto de seguridad de la información

En esta fase, en función del contexto, se definen los criterios básicos para la gestión de riesgos de seguridad de la información. Por ejemplo, se ha de decidir si se va a utilizar un enfoque global o un enfoque detallado. Además sirve para ser conscientes de las leyes que se deben cumplir, -LOPD y GDPR por ejemplo-, así como requisitos de contratos con terceros y normativa aplicable. Las distintas áreas implicadas harán valer sus expectativas, los recursos disponibles y cómo valoran las posibles consecuencias de los riesgos.



1.5 El proceso de gestión de riesgos de seguridad de la información

Valorando los riesgos de seguridad de la información

Esta es la fase central de la gestión de riesgos. Consta a su vez de:

- Identificación
- Análisis
- Evaluación



1.5 El proceso de gestión de riesgos de seguridad de la información

Valorando los riesgos de seguridad de la información

Identificando los riesgos

Para la evaluación de riesgos de seguridad de la información en primer lugar se han de identificar los activos de información. En general estos pueden ser de dos tipos:

Primarios

De soporte



1.5 El proceso de gestión de riesgos de seguridad de la información

Valorando los riesgos de seguridad de la información

Identificando los riesgos

Para valorar los daños estas son algunas de las preguntas:

- ¿qué valor tiene este activo para la empresa?
- ¿cuánto cuesta su mantenimiento?
- ¿cómo repercute en los beneficios de la empresa?
- ¿cuánto valdría para la competencia?
- ¿cuánto costaría recuperarlo o volverlo a generar?
- ¿cuánto costó adquirirlo o su desarrollo?
- ¿a qué responsabilidades legales o contractuales nos enfrentamos si se ve comprometido?



1.5 El proceso de gestión de riesgos de seguridad de la información

Valorando los riesgos de seguridad de la información

Estimando los riesgos

En la fase de establecimiento del contexto se determinaron una serie de criterios que serán las directrices de la estimación de riesgos. Son los que servirán para medir las consecuencias o impacto de la pérdida de confidencialidad, integridad y disponibilidad de los activos.



1.5 El proceso de gestión de riesgos de seguridad de la información

Valorando los riesgos de seguridad de la información

Estimando los riesgos

Estos criterios se concretan en escalas para valorar:

- pérdidas financieras
- costes de reparación o sustitución
- interrupción del servicio
- pérdida de reputación y confianza de los clientes
- disminución del rendimiento
- infracciones legales o ruptura de condiciones contractuales
- pérdida de ventaja competitiva
- daños personales



1.5 El proceso de gestión de riesgos de seguridad de la información

Valorando los riesgos de seguridad de la información *Estimando los riesgos*

Rango impacto / Descripción	Descripción	Pérdidas financieras	Pérdida del activo(s)	Reputación e imagen	Disminución de rendimiento
5 Catastrófico	> 6 % del presupuesto	Total	Mayor que un mes	Alta y muy extendida	> 50 % de variación en los indicadores
4 Desastroso	6% del Presupuesto	Muy gran impacto	De una semana a un mes	Media y muy extendida	25-50 % variación en los indicadores
3 Serio	2% del presupuesto	Gran impacto	De un día a una semana	Media y poco extendida	10-25% variación en los indicadores
2 Menor	1% del presupuesto	Impacto menor	½ día o 1 día	Baja y muy extendida	5-10 % variación en los indicadores
1 Insignificante	< 0,5 % del presupuesto	Casi sin impacto	Menor de ½ día	Baja y poco extendida	Hasta 5% variación en los indicadores

1.5 El proceso de gestión de riesgos de seguridad de la información

Valorando los riesgos de seguridad de la información

Evaluando los riesgos

Una vez se han valorado las consecuencias o impactos y la probabilidad de los incidentes para los activos del ámbito elegido, se ha de realizar el producto de ambos para calcular los riesgos. Los resultados obtenidos se compararán con los criterios de aceptación de riesgo.

La siguiente tabla muestra un ejemplo de un mapa de calor con el que comparar las valoraciones realizadas. Situaremos cada riesgo en la tabla, antes y después de considerar cómo han afectado las medidas que ya se habían puesto en marcha.



1.5 El proceso de gestión de riesgos de seguridad de la información

Valorando los riesgos de seguridad de la información

Evaluando los riesgos



1.5 El proceso de gestión de riesgos de seguridad de la información

Tratando y aceptando riesgos de seguridad de la información

En esta fase se seleccionarán la opción de tratamiento adecuada (evitar, reducir o mitigar, transferir o aceptar) para cada uno de los riesgos de la lista. Para elegir las opciones, o una combinación de ellas, se considerará no sólo la valoración obtenida para cada riesgo sino también el coste del tratamiento. Por ejemplo será mejor evitar algún riesgo que mitigarlo si el coste es muy alto.

Se preferirán las opciones que aporten una reducción considerable del riesgo de la forma más económica. El nivel de tolerancia de riesgo se establece en base a **criterios de coste-beneficio**.



1.5 El proceso de gestión de riesgos de seguridad de la información

Tratando y aceptando riesgos de seguridad de la información

Coste-Beneficio

El coste del tratamiento es muy superior a los beneficios.

El coste del tratamiento es adecuado a los beneficios.

El coste del tratamiento por terceros es más beneficioso que el tratamiento directo.

El nivel de riesgo está muy alejado del nivel de tolerancia.

Tratamiento

Evitar el riesgo, por ejemplo, dejando de realizar esa actividad.

Reducir o mitigar el riesgo: seleccionando e implementando los controles o medidas adecuadas que hagan que se reduzca la probabilidad o el impacto.

Transferir el riesgo, por ejemplo, contratando un seguro o subcontratando el servicio.

Retener o aceptar el riesgo sin implementar controles adicionales. Monitorizarlo para confirmar que no se incrementa.



1.5 El proceso de gestión de riesgos de seguridad de la información

Tratando y aceptando riesgos de seguridad de la información

Para reducir o mitigar los riesgos se realizan estas acciones:

- instalar productos o contratar servicios
- establecer controles de seguridad
- mejorar los procedimientos
- cambiar el entorno
- incluir métodos de detección temprana
- implantar un plan de contingencia y continuidad
- realizar formación y sensibilización



1.5 El proceso de gestión de riesgos de seguridad de la información

Tratando y aceptando riesgos de seguridad de la información

El resultado de esta fase se concreta en un **plan de tratamiento de riesgos**, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado. A este plan se añadirá una relación de **riesgos residuales**, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

Adicionalmente se incluye en algunos modelos una etapa de **aceptación del riesgo** para garantizar que la dirección es consciente de los riesgos residuales. Esta situación es importante cuando se decide posponer la implantación de medidas o rechazarla por motivos económicos.



1.5 El proceso de gestión de riesgos de seguridad de la información

Monitorizando los riesgos de seguridad de la información

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios.

Los riesgos no son estáticos y pueden cambiar de forma radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte lo siguiente:



1.5 El proceso de gestión de riesgos de seguridad de la información

Monitorizando los riesgos de seguridad de la información

- nuevos activos o modificaciones en el valor de los activos
- nuevas amenazas
- cambios o aparición de nuevas vulnerabilidades
- aumento de las consecuencias o impactos
- incidentes de seguridad de la información



1.5 El proceso de gestión de riesgos de seguridad de la información

Monitorizando los riesgos de seguridad de la información

De forma análoga se revisará el propio proceso de gestión de riesgos para adecuarlo al contexto. Esta revisión afecta entre otros a:

- las categorías de activos
- los criterios de evaluación de riesgos
- los niveles de clasificación de los impactos
- las escalas de aceptación de riesgos
- los recursos necesarios



1.6 Recomendaciones y bibliografía

- Haga un inventario de activos
- Califique sus activos y agreguele un valor
- Identifique las amenazas
- Esté atento a las vulnerabilidades y sea consciente de su riesgo, las mismas pueden surgir frecuentemente.
- Como resultado de la gestión de riesgos tenemos identificados los riesgos y su forma de tratarlos. Este es un buen punto de partida para gestionar la seguridad de la información en la empresa de forma amplia, planificando las distintas actuaciones de forma que estén organizadas en el tiempo y alineadas con la estrategia del negocio.
- La gestión de riesgos es el proceso central para poner en marcha un Plan director de seguridad de la información. En este plan se definen y priorizan, en base a una evaluación de riesgos, los proyectos que se hayan de implantar para reducir los riesgos a que está expuesta la empre



Bibliografía

- EEUU, COSO Committee of Sponsoring Organizations of the Treadway Commission (2015)
● «Guidance», <<http://www.coso.org/guidance.htm>>
- ISO, INTERNATIONAL STANDARIZATION ASSOCIATION (2009) «ISO 31000:2009 Risk management – Principles and guidelines»,
<<http://www.iso.org/iso/ES/home/standards/iso31000.htm>>
- Gobierno de España – ADMINISTRACIÓN ELECTRÓNICA (2012), MAGERIT V3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,
<http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_MetodoLog/pae_Magerit.html#.VVBX5WP-soco>
- EEUU NIST, National Institute of Standards and Technology (2012), «Special Publication 800-30 Rev.1», Guide for conducting risk assessment, Computer Security Division Information Technology Laboratory,
<<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>>
- ISO (2013) “ISO 27001:2013 Information security management systems - Requirements”,
<<http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>>
- ISO27000.es: el portal de la ISO27001 en español <<http://www.iso27000.es/>>
- ISO 27005:2011 Information technology - Security techniques - Information security risk management» <http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742>

