Gestión de riesgos

Una guía de aproximación para el empresario

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

2006-2016

TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

INCIBE_PTE_AproxEmpresario_002_GestionRiesgos-2015-v1

Figuras

Tablas

Introducción

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

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

Un hecho común a todos ellos, es que los responsables son conscientes de la existencia de amenazas que suponen un peligro para la consecución de sus objetivos. Dedican esfuerzos y recursos a mantener estos riesgos por debajo de un límite previamente consensuado en sus organizaciones.

Para maximizar los beneficios de dicha gestión y contar con garantías de éxito, los esfuerzos han de ser empleados de forma metódica, estructurada y, sobre todo, siguiendo un proceso de evaluación y mejora continua. Las organizaciones se encuentran en un entorno en cambio constante. Los logros obtenidos ante las amenazas de hoy no suponen ninguna garantía de éxito para las amenazas de mañana.

En esta guía se introducen los conceptos y procesos comunes a toda actividad de gestión de riesgos. La guía mostrará la aplicación de estos conceptos y procesos a la seguridad de la información.

La guía se estructura en los siguientes apartados:

- **Conceptos**
  Los términos básicos utilizados en gestión de riesgos.

- **Gestión de riesgos**
  Actividades para llevar a cabo una gestión de riesgos así como los diferentes roles y responsabilidades.

- **Gestión de riesgos en sistemas de información**
  Se aplican las actividades del apartado anterior al área de sistemas de información.

- **Referencias**
  Listado de enlaces donde encontrar más información sobre de gestión de riesgos.

2 Conceptos

En este apartado se introducen los términos utilizados en la jerga clásica de gestión de riesgos, su comprensión facilitará el resto de la lectura de la guía.

En la actualidad la revisión de algunas de las normas sobre riesgos, en particular las normas ISO, está incorporando nuevos conceptos más generales que los tradicionales, definiendo el riesgo como «incertidumbre en la consecución de los objetivos». Además de la definición se indican los cambios para cada término afectado.

2.1 Activo, amenaza, vulnerabilidad, impacto y probabilidad

- **Activo** Cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del riesgo.
  Este término en las nuevas normas se generaliza para denominarse «fuente de riesgo» siendo el elemento que sólo o con otros puede originar un riesgo.

- **Amenaza** Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.
  En la evolución de las normas este concepto se amplia para denominarse «suceso».

La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos

2 Conceptos

- **Vulnerabilidad** Debilidad que presentan los activos y que facilita la materialización de las amenazas.

- **Impacto o consecuencia** de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad. El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo.
  La consecuencia en las nuevas normas es el resultado de un suceso que afecta a los objetivos.

- **Probabilidad** Es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico de la empresa, o en opiniones de expertos o del empresario (datos subjetivos).
  Este término permanece en la evolución de las normas ISO refiriéndose a un suceso en lugar de a una amenaza.

El siguiente diagrama muestra las relaciones entre estos conceptos:

Ilustración 1 *Activo, amenaza, vulnerabilidad e impacto*

2.2 ¿Cómo se mide el nivel de riesgo?

Como veíamos en el apartado anterior, el **impacto** nos indica las consecuencias de la materialización de una amenaza. El **nivel de riesgo** es una estimación de lo que puede ocurrir y se valora, de forma **cuantitativa**, como el producto del impacto, (consecuencia), asociado a una amenaza (suceso), por la probabilidad de la misma.

Ilustración 2
Cálculo del riesgo

Impacto **x Probabilidad** **= RIESGO**

El impacto, y por tanto el riesgo, se valoran en términos del coste derivado del valor de los activos afectados considerando, además de los daños producidos en el propio activo:

- daños personales
- pérdidas financieras
- interrupción del servicio
- pérdida de imagen y reputación
- disminución del rendimiento

Si bien es posible, y en ocasiones necesario, realizar un análisis **cualitativo**, trabajar con magnitudes económicas facilita a las organizaciones establecer el llamado umbral de riesgo, también llamado «apetito al riesgo»: el nivel máximo de riesgo que la empresa está dispuesta o «se atreve» a soportar. La gestión de riesgos debe mantener el nivel de riesgo siempre por debajo del umbral.

Por otro lado, se denomina **coste de protección** al coste que supone para las organizaciones los recursos y esfuerzos que dedican para mantener el nivel de riesgo por debajo del umbral deseado. Las organizaciones deben vigilar de no emplear más recursos de los necesarios para cumplir ese objetivo. En la siguiente gráfica podemos ver como ambos conceptos, riesgo y coste de protección, se relacionan.

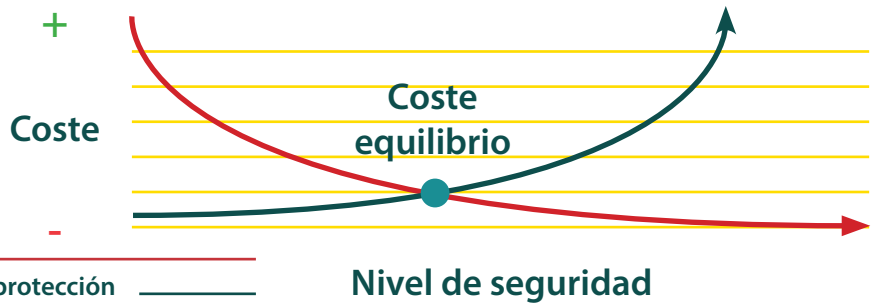


Ilustración 3
Coste de equilibrio

El punto en el que el coste de protección es el adecuado para mantener los riesgos por debajo del umbral fijado de riesgo es el coste de equilibrio. Este punto dependerá del umbral de riesgo de acuerdo con los objetivos de la empresa.

2.3 ¿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** Que consiste en averiguar el nivel de riesgo que la empresa está soportando. Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos.

- **Tratamiento de los riesgos** Para aquellos riesgos cuyo nivel está por encima del umbral deseado la empresa debe decidir cuál es el mejor tratamiento que permita disminuirlos. Esta decisión siempre ha de pasar un filtro económico donde el coste del tratamiento, o coste de protección, no supere el coste de riesgo disminuido.

Ilustración 4
Gestión de riestos

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

- **Evitar o eliminar el riesgo** Por ejemplo sustituyendo el activo por otro que no se vea afectado por la amenaza o eliminando la actividad que lo produce.

- **Reducirlo o mitigarlo** Tomando las medidas oportunas para que el nivel de riesgo se sitúe por debajo del umbral. Para conseguirlo se puede:
  _reducir la probabilidad o frecuencia de ocurrencia: tomando, por ejemplo, medidas preventivas
  _reducir el impacto de la amenaza o acotar el impacto, estableciendo por ejemplo controles y revisando el funcionamiento de las medidas preventivas

- **Transferirlo, compartirlo o asignarlo a terceros** En ocasiones la empresa no tiene la capacidad de tratamiento y precisa la contratación de un tercero con capacidad para reducir y gestionar el riesgo dejándolo por debajo del umbral.

- **Aceptarlo** Se asume el riesgo, bien porque está debajo del umbral aceptable de riesgo bien en situaciones en las que los costes de su tratamiento son elevados y aun siendo riesgos de impacto alto su probabilidad de ocurrencia es baja o porque aun a pesar del riesgo la empresa no quiere dejar de aprovechar la oportunidad que para su negocio supone esa actividad arriesgada.

2 Conceptos

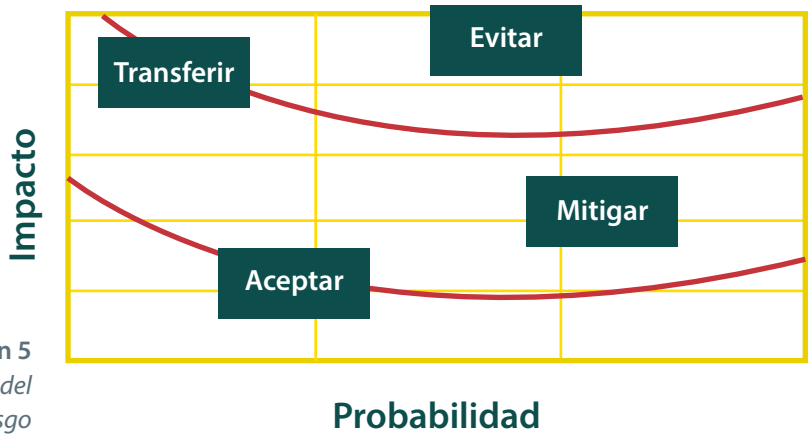


Ilustración 5
Opciones del tratamiento de riesgo

El análisis de riesgos debe ser realizado de forma metódica impidiendo omisiones, improvisaciones o posibles criterios arbitrarios. En la actualidad existen diversas **metodologías y guías de buenas prácticas**, tanto generalistas como especializadas, que pueden ser utilizadas para realizar este análisis. Entre las generalistas destacamos:

- COSO [1], organización americana dedicada a la creación de guías y marcos de trabajo en el ámbito de la gestión de riesgos empresariales.
- ISO 31000:2009 [2], norma global, no certificable, que aporta metodología, principios y directrices en materia de gestión de riesgos.

Específicas para gestión de riesgos de seguridad de la información:

- MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [3] creada por el Ministerio de Administraciones Públicas español.
- ISO / IEC 27005: 2008 (E) [11] norma que aporta directrices para la gestión de riesgos de seguridad de la información.
- NIST SP - 800-30 [4], metodología creada en este caso por el gobierno norteamericano.

Cada empresa puede elegir una metodología o una guía de buenas prácticas a seguir o bien definir una propia que esté acorde con su idiosincrasia.

3 Gestión del riesgo: principios, marco de trabajo y proceso

En este apartado se describe el proceso y las actividades necesarios para llevar a cabo la gestión de riesgos de acuerdo a la norma ISO 31000:2009 [2].

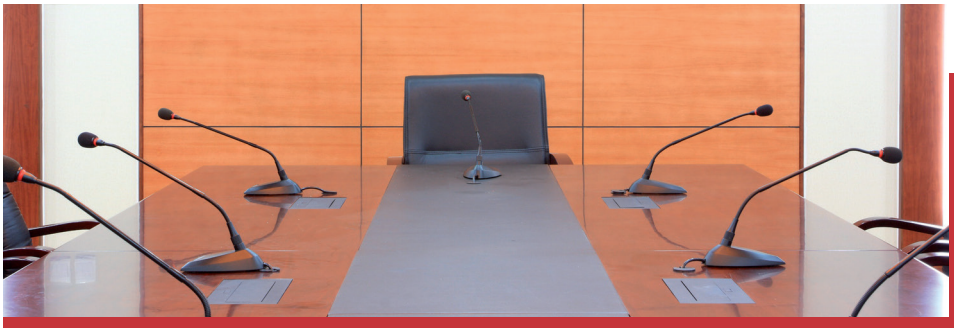
3.1 Principios

Estos son los principios básicos que debe cumplir la gestión de riesgos si queremos que cumpla su cometido:

- proteger el valor, es decir, contribuir a la consecución de los objetivos y la mejora del desempeño
- ser una parte integral de todos los procesos de la empresa
- formar parte de la toma de decisiones
- tratar explícitamente la incertidumbre
- ser sistemática, estructurada y oportuna
- basarse en la mejor información disponible
- adaptarse, alineándose con el contexto interno y externo y con los perfiles del riesgo
- integrar factores humanos y culturales
- ser trasparente y participativa
- ser dinámica, iterativa y responde a los cambios
- facilitar la mejora continua

3.2 Marco de trabajo

Como en toda actividad, el compromiso de la dirección es básico para llevarla a cabo con éxito. En la gestión de riesgos no es diferente, ha de estar plenamente integrada en los procesos de la empresa y requiere un compromiso fuerte y sostenido de la dirección así como del establecimiento de una rigurosa planificación estratégica, un marco de trabajo. Este «marco de trabajo» ha de ser objeto de seguimiento y revisión periódica que permitan medir el progreso y adaptarse a los cambios del entorno, tomando las decisiones oportunas para la mejora continua.



Este "marco de trabajo" ha de ser objeto de seguimiento y revisión periódica

3 Gestión del riesgo: principios, marco de trabajo y proceso

Para conseguir una buena gestión del riesgo el marco de trabajo definido ha de:

- comprender la empresa y su contexto
- establecer una **política de gestión de riesgos**
- identificar autoridades y competencias
- definir la integración en los procesos de negocio como plan estratégico para que sea relevante, eficaz y eficiente
- proporcionar los recursos necesarios:
  _personas, formación
  _procesos y procedimientos
  _métodos y herramientas
- establecer mecanismos de comunicación interna y externa

Este marco de trabajo se implementará definiendo un calendario y estrategia de implementación y revisión que permita:

- establecer y desarrollar los objetivos
- aplicar la política y el proceso
- cumplir con la legislación y normativa
- organizar la formación y la comunicación y consulta a los interesados

Hay que definir un calendario y estrategia de implementación y revisión del marco de trabajo

3 Gestión del riesgo: principios, marco de trabajo y proceso

3.2.1 Política de gestión de riesgos

El establecimiento de una política de gestión de riesgos en la que se indiquen con claridad los objetivos y se materialice el compromiso de toda la empresa va a ser clave para una gestión de riesgos eficaz. La política tratará estas cuestiones:

- motivos para llevar a cabo la gestión de riesgos
- relación con otras políticas de la empresa
- responsabilidades y rendición de cuentas en el proceso de gestión de riesgos
- recursos disponibles
- medición del desempeño
- compromiso de revisión del marco de trabajo y de la política

3.3 Etapas del proceso de gestión de riesgos

En el proceso de gestión de riesgos se distinguen las siguientes actividades:

Ilustración 6 *Proceso de gestión de riesgos (fuente: ISO 31000:2009)*

3 Gestión del riesgo: principios, marco de trabajo y proceso

3.3.1 Comunicación y consulta

Esta actividad es la primera y abarca todas las siguientes pues se ha de realizar en todas las etapas. En ella se fomenta la participación y se coordinan las actuaciones de todas las partes implicadas, tanto internas como externas, en la gestión de riesgos.

3.3.2 Determinar el contexto

Es esencial que la gestión de riesgos se integre tanto con el resto de áreas de la empresa como con su entorno externo. Por tanto hay que determinar los condicionantes tanto internos como externos que definen el marco de trabajo. A nivel interno se tendrán en cuenta: la cultura, recursos, procesos y objetivos del negocio. A nivel externo se consideran diferentes aspectos relativos al entorno social, económico o legislativo.

Como resultado de esta fase se establecen:

- los objetivos de la gestión de riesgo
- los criterios que se emplearán para la evaluación de los riesgos, el método a utilizar en el establecimiento de probabilidades, así como las magnitudes de los impactos
- el alcance de la gestión de riesgos, los roles y la asignación de responsabilidades

3.3.3 Valoración o apreciación de riesgos

Una vez definido el contexto se han de valorar los riesgos. En esta etapa se determinan los riesgos que van a ser controlados por medio de su identificación, análisis y evaluación. Todos aquellos riesgos que no sean identificados quedarán como riesgos ocultos o no controlados. Se realizan en esta fase las siguientes actividades:

- **Identificación del riesgo**, cuyo objetivo es búsqueda, reconocimiento y descripción de todos los posibles puntos de peligro tanto internos como externos; para cada uno de ellos se determinará su impacto y probabilidad
  - esta fase responde a las siguientes preguntas:
    - *¿qué puede pasar?*
    - *¿cuándo y dónde?*
    - *¿cómo y por qué?*

3 Gestión del riesgo: principios, marco de trabajo y proceso

- **Análisis del riesgos** es la etapa en la cual se califican cada uno de los riesgos identificados tanto de forma cuantitativa (valorando su impacto) como cualitativa (importancia relativa) para priorizar nuestros esfuerzos de forma no arbitraria. En esta actividad también se persigue comprender cómo se desarrollan los riesgos, estudiando sus causas y consecuencias, así como evaluando la eficacia de los diferentes medios de control implantados en la empresa.
  - Se mide el nivel de riesgo según la fórmula ***Riesgo = Impacto x Probabilidad***, valorando las consecuencias y la probabilidad de cada riesgo.

- **Evaluación del riesgo**, cuyo objetivo es determinar prioridades en el uso de los recursos a emplear en la gestión de riesgos. En esta fase se amplía la calificación del análisis anterior incluyendo valoraciones en términos de estrategia de negocio que permitan establecer qué riesgos son aceptables y cuáles no.

3.3.4 Tratamiento del riesgo

A continuación se identifican y evalúan las opciones existentes de tratamiento de cada uno de los riesgos que sea necesario tratar según se determinó en la fase anterior. Algunas de las opciones de tratamiento son, como vimos en apartados anteriores (apartado 2.3): evitarlo, reducirlo o mitigarlo, transferirlo o compartirlo y aceptarlo.

3.3.5 Seguimiento y revisión

Para conseguir una mejora continua se supervisa «lo que está ocurriendo» en la práctica y se realizan las correcciones que fuera preciso. También se ha de evaluar el propio sistema de gestión, detectando posibles deficiencias y oportunidades de mejora. La revisión de los cambios del entorno está incluida en esta etapa, realimentando la fase de determinación del contexto.

Para conseguir una mejora continua se supervisa «lo que está ocurriendo» en la práctica y se realizan las correcciones que fuera preciso

4 Gestión del riesgos de seguridad de la información

En la sociedad actual, inmersa en la llamada revolución digital, las compañías son conscientes del protagonismo de la **información** en sus procesos productivos.

Esta revolución ha cambiado también las relaciones con clientes, proveedores, organismos oficiales, donde Internet juega un importante papel como medio de comunicación. Este medio, por su naturaleza libre y de bajo coste, ha permitido interconectar a las personas y a las empresas entre sí rompiendo las barreras geográficas y habilitando en gran medida la llamada globalización de la economía y de la sociedad.

Las empresas acostumbradas a dedicar recursos para gestionar los riesgos de sus procesos productivos, deben también preocuparse y asignar recursos para la gestión de los riesgos asociados a su información y a las infraestructuras que la soportan.

4.1 Conceptos

En términos de gestión de riesgos de seguridad de la información, el **activo** a proteger es la **información** de la compañía. Hablamos tanto de información «digital» contenida en nuestros sistemas de información como aquella contenida en cualquier otro soporte como por ejemplo el papel. También tenemos que tener presente que la gestión debe ocuparse de todo el ciclo de vida de la información y no sólo de su explotación, considerando etapas como la de captura o destrucción de la información.

La información es el activo principal pero también debemos considerar: infraestructura informática, equipos auxiliares, redes de comunicaciones, instalaciones y personas.

Cuando hablamos de seguridad de la información hablamos de protegerla de riesgos que puedan afectar a una o varias de sus tres principales propiedades:

- **Confidencialidad** La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
- **Integridad** La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.
- **Disponibilidad** La información debe estar siempre accesible para aquellos que estén autorizados.

Ilustración 7 *Dimensiones de la seguridad de la información*

4 Gestión del riesgo: de seguridad de la información

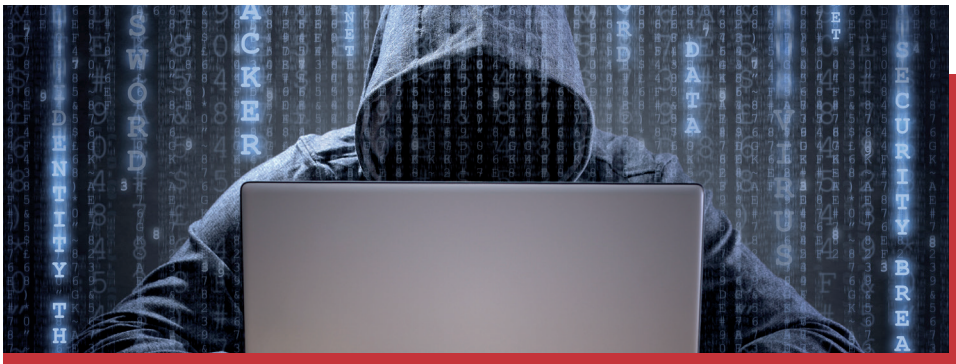
Las **amenazas** a las que se enfrenta la información de nuestras organizaciones pueden ser muy variadas, a modo de ejemplo:

- **de origen natural:** inundaciones, terremotos, incendios, rayos
- fallos de la infraestructura auxiliar: fallos de suministro eléctrico, refrigeración, contaminación...
- **fallos de los sistemas informáticos y de comunicaciones:** fallos en las aplicaciones, hardware o equipos de transmisiones
- **error humano:** errores accidentales o deliberados de las personas que interactúan con la información, por ejemplo:
  _acciones no autorizadas como uso de software o hardware no autorizados
  _funcionamiento incorrecto por abuso o robo de derechos de acceso o errores en el uso, falta de disponibilidad, etc
  _información comprometida por robo de equipos, desvelado de secretos, espionaje, etc

Las **vulnerabilidades** frente a las cuales se debe proteger a los sistemas de información y a la información que tratan, dependen en gran medida de la naturaleza de los mismos; podemos decir que es un factor **intrínseco** a nuestros activos. Estas pueden depender del hardware, del software, las redes, el personal, el edificio o las infraestructuras o la organización. Algunos ejemplos son:

- equipamiento informático susceptible a variaciones de temperatura o humedad
- sistemas operativos que por su estructura, configuración o mantenimiento son más vulnerables a algunos ataques
- localizaciones que son más propensas a desastres naturales como por ejemplo inundaciones o que están en lugares con variaciones de suministro eléctrico
- aplicaciones informáticas, que por su diseño, son más inseguras que otras
- personal sin la formación adecuada, ausente o sin supervisión

Gran parte de estos factores son difíciles o muy caros de erradicar y las organizaciones tienen que convivir con ellos tomando medidas que reduzcan el impacto de sus amenazas.



Las vulnerabilidades pueden depender del hardware, del software, las redes, el personal, el edificio, la organización...

Gestión del riesgo:
de seguridad de la información

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

Análogamente a lo que veíamos en el capítulo anterior 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

- ***Se recomienda la lectura del siguiente contenido del portal:***
- ***«Sigue el camino del análisis de riesgos» (infografía) [5]***

4.2.1 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.

Estas acciones de comunicación son importantes para:

- identificar los riesgos
- valorarlos en función de las consecuencias para el negocio y la probabilidad de que ocurran
- comprender la probabilidad y consecuencias de los riesgos
- establecer prioridades para el tratamiento de riesgos
- informar y contribuir a que se involucren las áreas interesadas
- monitorizar la efectividad del tratamiento de los riesgos
- revisar con regularidad el proceso y su monitorización
- concienciar a la plantilla y a la dirección sobre estos riesgos y su forma de mitigarlos

4.2.2 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; el primero sea más rápido pero menos preciso que el segundo. Además sirve para ser conscientes de las leyes que se deben cumplir, -LOPD y LSSI 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.

Así quedarán definidos los **criterios** para:

- evaluación de riesgos:

_*cuáles son los activos de información críticos.*
_*la importancia de los mismos en cuanto a disponibilidad, integridad y confidencialidad.*
_*el valor estratégico de los procesos de información del negocio.*

- niveles de clasificación de los impactos
- escalas de aceptación de riesgos

Por último se define el **ámbito** y los límites de esta gestión, es decir a qué parte de la organización afecta, que procesos, que oficinas o que parte de la estructura.

4.2.3 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

4.2.3.1 *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:

_*información: estratégica, de carácter personal o que esté sujeta a legislación que la proteja, esencial para el desarrollo del negocio, de difícil o muy costosa reposición, etc*
_*actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc*

- De soporte:

_*hardware: PC, portátiles, servidores, impresoras, discos, documentos en papel*
_*software: sistemas operativos, paquetes, aplicaciones, ...*
_*redes: conmutadores, cableado, puntos de acceso, ...*
_*personal: usuarios, desarrolladores, responsables, ...*
_*edificios, salas, y sus servicios*
_*estructura organizativa: responsables, áreas, contratistas, ...*

Después de tener una relación con todos los activos se han de **conocer las amenazas** que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc. En el apartado anterior se mencionan algunos ejemplos.

4 Gestión del riesgo: de seguridad de la información

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?

Posiblemente ya se hayan tomado algunas medidas para contrarrestar estas amenazas. Es importante tenerlas en cuenta para no duplicar esfuerzos, analizar si son efectivas y si aún se utilizan o no.

Al llegar aquí tendremos, un listado de activos, sus amenazas y las medidas que ya se han tomado. A continuación revisaremos las vulnerabilidades que pueden aprovechar las amenazas y causar daños a nuestros activos de información. Existen distintos métodos para analizar **amenazas** por ejemplo:

- entrevistas con usuarios y cuestionarios
- inspección física
- uso de herramientas para el escaneo automatizado

Para cada una de las amenazas analizaremos las **vulnerabilidades** que puede explotar. La norma ISO 27005 [11] incluye un anexo con ejemplos de vulnerabilidades y amenazas que puede servir de apoyo en esta tarea.

Finalmente se han de concretar las **consecuencias**, es decir, cómo estas amenazas y vulnerabilidades afectan a la disponibilidad, integridad y confidencialidad de los activos de información.

Las distintas metodologías y herramientas proporcionan listados que sirven de orientación a la hora de identificar activos, amenazas y vulnerabilidades.

4.2.3.2

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. 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

Esta tabla muestra un posible ejemplo de estos criterios:

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 enl os indicadores
1	Insignificante	< 0,5 % del presupuesto	Casi sin impacto	Menor de ½ día	Baja y poco extendida	Hasta 5% variación en los indicadores

Tabla 1 *Ejemplo de niveles de clasificación de los impactos de un incidente*

La estimación puede realizarse con distinta profundidad o nivel de detalle. Los métodos para realizarla incluyen estimaciones cualitativas y cuantitativas o una combinación de ambas. Suele realizarse una estimación cualitativa inicial para identificar los riesgos que precisan una estimación cuantitativa.

4 Gestión del riesgo: de seguridad de la información

En la estimación cualitativa se califican las potenciales consecuencias y la probabilidad según niveles (alto, medio, bajo) subjetivos. En la cuantitativa se utiliza una escala con valores numéricos, apoyándose en datos de distintas fuentes por ejemplo incidentes del pasado, experiencia previa, estudios, etc.

Se recomienda la lectura de los siguientes contenidos del portal:
- ***«Fácil y sencillo: análisis de riesgos en 6 pasos» [6]***
- ***«Plan director de seguridad» [7], en particular el área de descargas con plantillas y hojas de verificación .***

Además de medir las posibles consecuencias se ha de estimar la **probabilidad de que ocurran los incidentes**. También en este caso se utilizan técnicas cualitativas y cuantitativas que consideran:

- estadísticas de los incidentes en el pasado, de estudios o del sector
- factores geográficos o estacionales (temperatura, inundaciones, ...)
- motivaciones de los posibles atacantes (atractivo de los datos que se manejan, clima laboral, ...)
- vulnerabilidades existentes
- medidas que ya se han tomado y su resultado

Como resultado tendremos la valoración de las consecuencias y su probabilidad, con las que podremos estimar el nivel del riesgo.

Además de medir las posibles consecuencias se ha de estimar la probabilidad de que ocurran los incidentes

4 Gestión del riesgo: de seguridad de la información

4.2.3.3 *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 como han afectado las medidas que ya se habían puesto en marcha.

Casi seguro	5	5	10	15	20	25
Muy probable	4	4	8	12	16	20
Posible	3	3	6	9	12	15
Improbable	2	2	4	6	8	10
Muy improbable	1	1	2	3	4	5
Probabilidad	x	1	2	3	4	5
	Impacto	**Insignificante**	**Menor**	**Serio**	**Desastroso**	**Catastrófico**

Tabla 2 *Estimación del producto «probabilidad x impacto» para evaluar riesgos*

Este tipo de tablas también servirá para estimar qué tratamiento dar a cada riesgo. Por ejemplo los riesgos en la zona roja serían inaceptables pero los de la zona blanca podemos elegir soportarlos. Estos criterios nos ayudarán en la fase siguiente.

4.2.4 Tratando y aceptando riesgos de seguridad de la información

Como resultado de la etapa anterior tendremos una lista ordenada de riesgos o una tabla como la del ejemplo con su posición. Ahora debemos elegir qué hacer con cada uno de ellos en virtud de su valoración y de los criterios establecidos. Es decir, tendremos que situar la «línea roja» de nuestro umbral o nivel de tolerancia al riesgo.

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**.

Gestión del riesgo:
de seguridad de la información

Coste-Beneficio	Tratamiento
El coste del tratamiento es muy superior a los beneficios.	**Evitar el riesgo**, por ejemplo, dejando de realizar esa actividad.
El coste del tratamiento es adecuado a los beneficios.	**Reducir o mitigar el riesgo**: seleccionando e implementando los controles o medidas adecuadas que hagan que se reduzca la probabilidad o el impacto.
El coste del tratamiento por terceros es más beneficioso que el tratamiento directo.	**Transferir el riesgo, por ejemplo**, contratando un seguro o subcontratando el servicio.
El nivel de riesgo está muy alejado del nivel de tolerancia.	**Retener o aceptar el riesgo** sin implementar controles adicionales. Monitorizarlo para confirmar que no se incrementa.

Tabla 3 *Ejemplo criterios para el tratamiento de riesgos*

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

Los controles son medidas de protección para reducir el riesgo. La norma ISO 27001:2013 [8] en su anexo A incluye una lista de controles -no exhaustiva- de aplicación a la mayoría de empresas.

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.

4.2.5 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:

- 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

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

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 empresa.

Se recomienda la lectura del siguiente contenido del portal:
«Plan director de seguridad» [7]

5 Referencias

1 EEUU, COSO Committee of Sponsoring Organizations of the Treadway Commission (2015) «Guidance», <http://www.coso.org/guidance.htm> [consulta: 12/05/2015]

2 ISO, INTERNATIONAL STANDARIZATION ASSOCIATION (2009) «ISO 31000:2009 Risk management – Principles and guidelines», <http://www.iso.org/iso/ES/home/standards/iso31000.htm> [consulta: 12/05/2015]

3 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#.VVBx5WPsoco> [consulta: 12/05/2015]

4 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> [consulta: 12/05/2015]

5 INCIBE Protege tu empresa - Blog (2014) «Sigue el camino del análisis de riesgos» <https://www.incibe.es/protege-tu-empresa/blog/sigue-camino-analisis-riesgos> [consulta: 12/05/2015]

6 INCIBE - Protege tu empresa - Blog (2014) «Fácil y sencillo: análisis de riesgos en 6 pasos» <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo> [consulta: 12/05/2015]

7 INCIBE - Protege tu empresa - ¿Qué te interesa? (2014), «Plan director de seguridad» <https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad> [consulta: 12/05/2015]

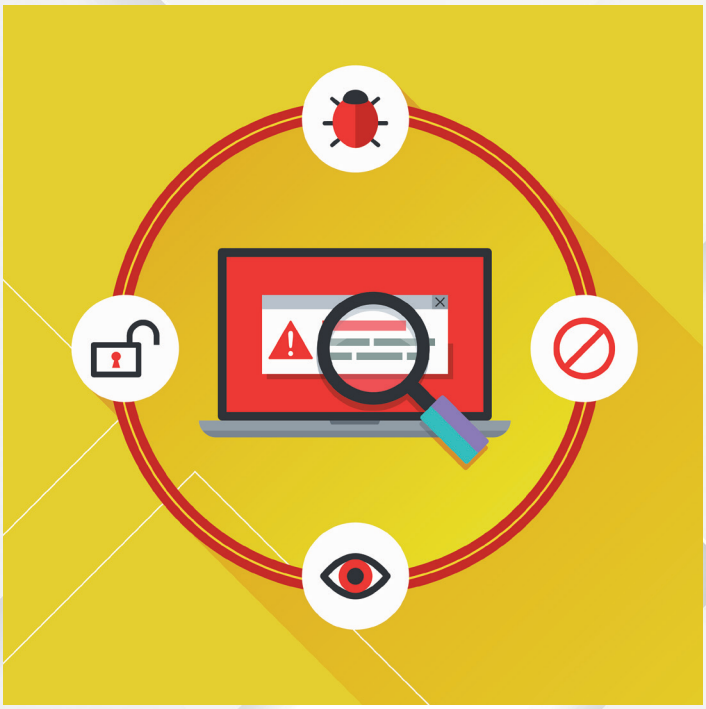
8 ISO (2013) "ISO 27001:2013 Information security management systems - Requirements", <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> [consulta: 12/05/2015]

9 ISO27000.es: el portal de la ISO27001 en español <http://www.iso27000.es/>

10 ISMS FORUM SPAIN: Asociación española para el fomento de la seguridad de la información <https://www.ismsforum.es/>

11 ISO (2011) «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>

12 INCIBE Protege tu empresa - Blog (2013) «Nueva versión ISO/IEC 27001:2013» <https://www.incibe.es/protege-tu-empresa/blog/nueva-version-iso27001> [consulta: 12/05/2015]



GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL