GUÍAS TIC ABOGACÍA ESPAÑOLA: Ciberseguridad

GESTIÓN DE RIESGOS

Una guía de aproximación al Compliance para la Abogacía

Abogacía Española
CONSEJO GENERAL

incibe_

1 INTRODUCCIÓN

2 CONCEPTOS

2.1 - Activo, amenaza, vulnerabilidad, impacto y probabilidad

2.2 - ¿Cómo se mide el nivel de riesgo?

2.3 - ¿Qué hacer con los riesgos?

3 GESTIÓN DEL RIESGO: principios, marco de trabajo y proceso

3.1 - Principios

3.2 - Marco de trabajo

3.2.1 Política de gestión de riesgos

3.3 - Etapas de proceso de gestión de riesgos

3.3.1 Comunicación y consulta

3.3.2 Determinar el contexto

3.3.3 Valoración o apreciación de riesgos

3.3.4 Tratamiento del riesgo

3.3.5 Seguimiento y revisión

4 GESTIÓN DE RIESGOS de seguridad de la información

4.1 - Conceptos

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

4.2.1 Comunicación

4.2.2 Estableciendo el contexto de seguridad de la información

4.2.3 Valorando los riesgos de seguridad de la información

4.2.3.1 Identificando los riesgos

4.2.3.2 Estimando los riesgos

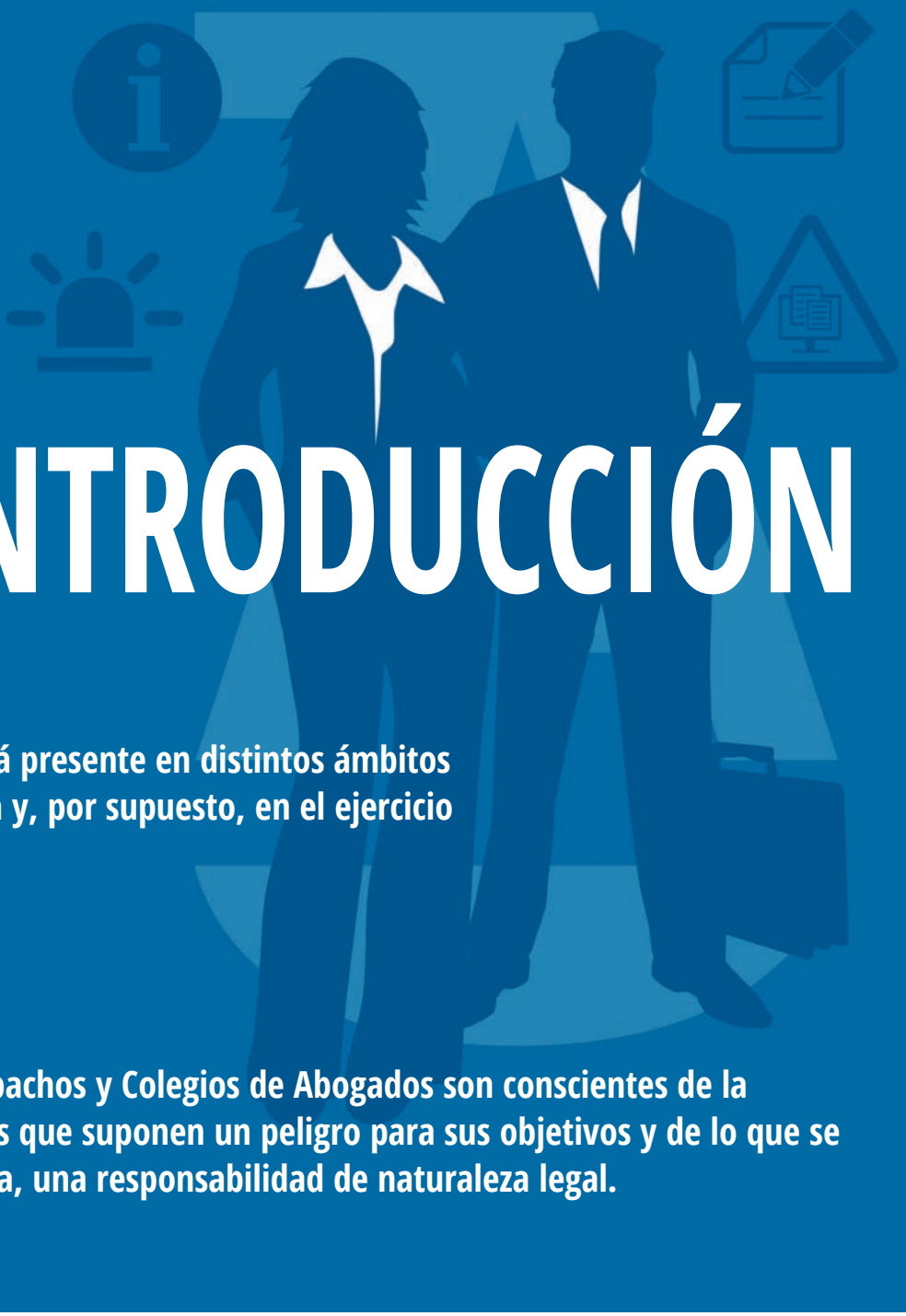
4.2.3.3 Evaluando los riesgos

4.2.4 Tratando y aceptando riesgos de seguridad de la información

4.2.5 Monitorizando los riesgos de seguridad de la información

5 REFERENCIAS

1 INTRODUCCIÓN



La gestión de riesgos está presente en distintos ámbitos de la sociedad y la empresa y, por supuesto, en el ejercicio de la Abogacía.

Los gestores de despachos y Colegios de Abogados son conscientes de la existencia de amenazas que suponen un peligro para sus objetivos y de lo que se deriva, en consecuencia, una responsabilidad de naturaleza legal.

La guía se estructura en los siguientes apartados:

- Conceptos
  - Gestión de riesgos
    - Gestión de riesgos en sistemas de información
      - Referencias

Como es sabido, la gestión de riesgos está presente, con mayor o menor protagonismo, en distintos ámbitos de la sociedad y la empresa y, por supuesto, también en el ejercicio de la Abogacía.

La Abogacía es pieza esencial en el funcionamiento de uno de los poderes del Estado – el Poder Judicial - y en la satisfacción del derecho fundamental a obtener tutela judicial efectiva, lo que nos recuerda la relevancia constitucional de los intereses públicos involucrados en su ejercicio.

Como ejemplos de riesgos a los que se enfrenta la profesión, y que deben ser correctamente gestionados, encontramos algunos de los siguientes:

• **Riesgos de carácter laboral,** que afectan a la organización del despacho o sociedad desde la que se desempeña la actividad de la Abogacía.

• **Riesgos corporativos y de proyectos,** que acompañan a las actividades de asesoramiento y defensa propios de la profesión, y que se reflejan en la necesidad de contar con un seguro de responsabilidad civil.

• **Riesgos de naturaleza deontológica,** derivados de las obligaciones de buenas prácticas a las que están sometidos los abogados.

• **Riesgos financieros,** que afectan a la actividad económica que se desarrolla durante el ejercicio de la profesión.

• **Riesgos de seguridad de la información,** provenientes de la gestión de información personal y confidencial de nuestros clientes (no solo datos de carácter personal o privado, sino también información financiera, de

terceros, etc), que encuentran reflejo en las obligaciones de diligencia y secreto a las que se refieren el Estatuto General de la Abogacía Española y el Código Deontológico de la Abogacía, como veremos más adelante. Pero ya el artículo 1.4 del Estatuto General de la Abogacía recoge un principio general fundamental relacionado con este aspecto, cuando dice que los abogados deben ser personas de reconocida honorabilidad y, en consecuencia han de observar una trayectoria de respeto a las leyes, a los principios rectores y valores superiores de la Abogacía, a las normas deontológicas y a las buenas prácticas profesionales.

Un hecho común a todos ellos, es que los gestores de despachos y Colegios de Abogados son conscientes de la existencia de amenazas que suponen un peligro para la consecución de sus objetivos y de lo que se deriva, en consecuencia, una responsabilidad de naturaleza legal. Debe ser, por tanto, objetivo de los responsables de estas organizaciones el dedicar esfuerzos y recursos para mantener estos riesgos por debajo de un límite previamente consensuado que no exceda de lo razonable.

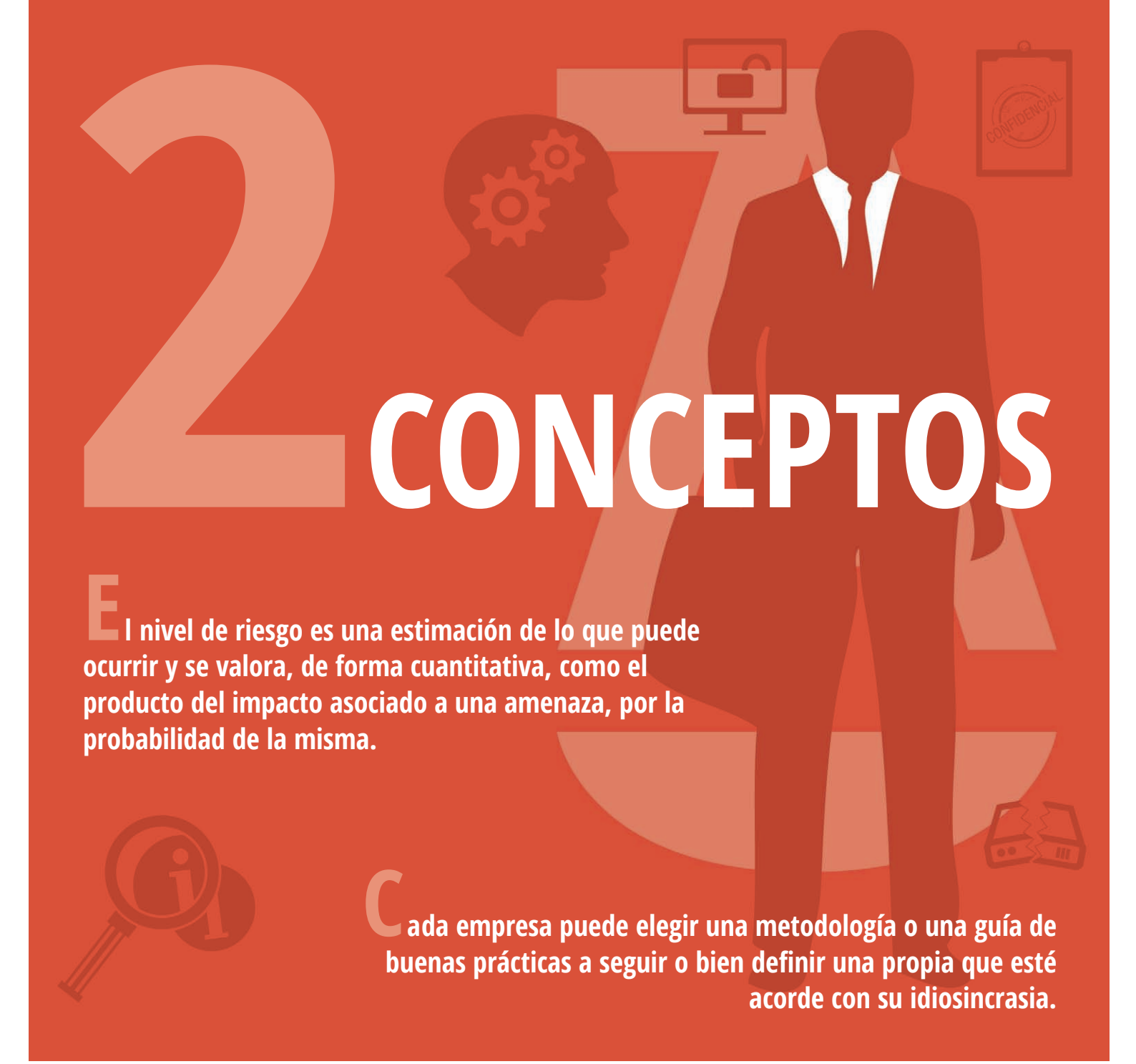
Para maximizar los beneficios de dicha gestión y contar con garantías de éxito, los esfuerzos han de ser empleados de forma metódica, estructurada y, sobre todo, siguiendo un proceso de evaluación y mejora continua. Los despachos y Colegios se encuentran en un entorno de cambio constante, por lo que los logros obtenidos frente a los riesgos de hoy no suponen ninguna garantía de éxito para las amenazas de mañana, especialmente en un ámbito como el de la ciberseguridad, en el que los avances de la tecnología convierten en vulnerables los sistemas otrora impenetrables.

En esta guía se introducen los conceptos y procesos comunes a toda actividad de gestión de riesgos en organizaciones jurídicas. La guía mostrará la aplicación de estos conceptos y procesos a la seguridad de la información para la Abogacía y sus instituciones.

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



El nivel de riesgo es una estimación de lo que puede ocurrir y se valora, de forma cuantitativa, como el producto del impacto asociado a una amenaza, por la probabilidad de la misma.

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.

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

- Evitar o eliminar el riesgo
- Reducirlo o mitigarlo
- Transferirlo
- Aceptarlo

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[1].

2.1 Activo, amenaza, vulnerabilidad, impacto y probabilidad

- **Activo:** cualquier recurso de la organización ("fuente de riesgo") necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un perjuicio. 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, entre los cuales se encuentra la información que compone los expedientes, es importante para la evaluación de la magnitud del riesgo.

- **Amenaza:** circunstancia desfavorable (o "suceso", en terminología de las normas ISO) que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

- **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 (también en los objetivos) se suele estimar en un porcentaje de degradación que afecta al valor del activo, donde el 100% sería la pérdida total del activo.

- **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).

[1]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.

El siguiente diagrama muestra las relaciones entre estos conceptos:

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.

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 (continuidad del negocio)**
- **Pérdida de imagen y reputación**
- **Disminución del rendimiento**

"Umbral de riesgo"

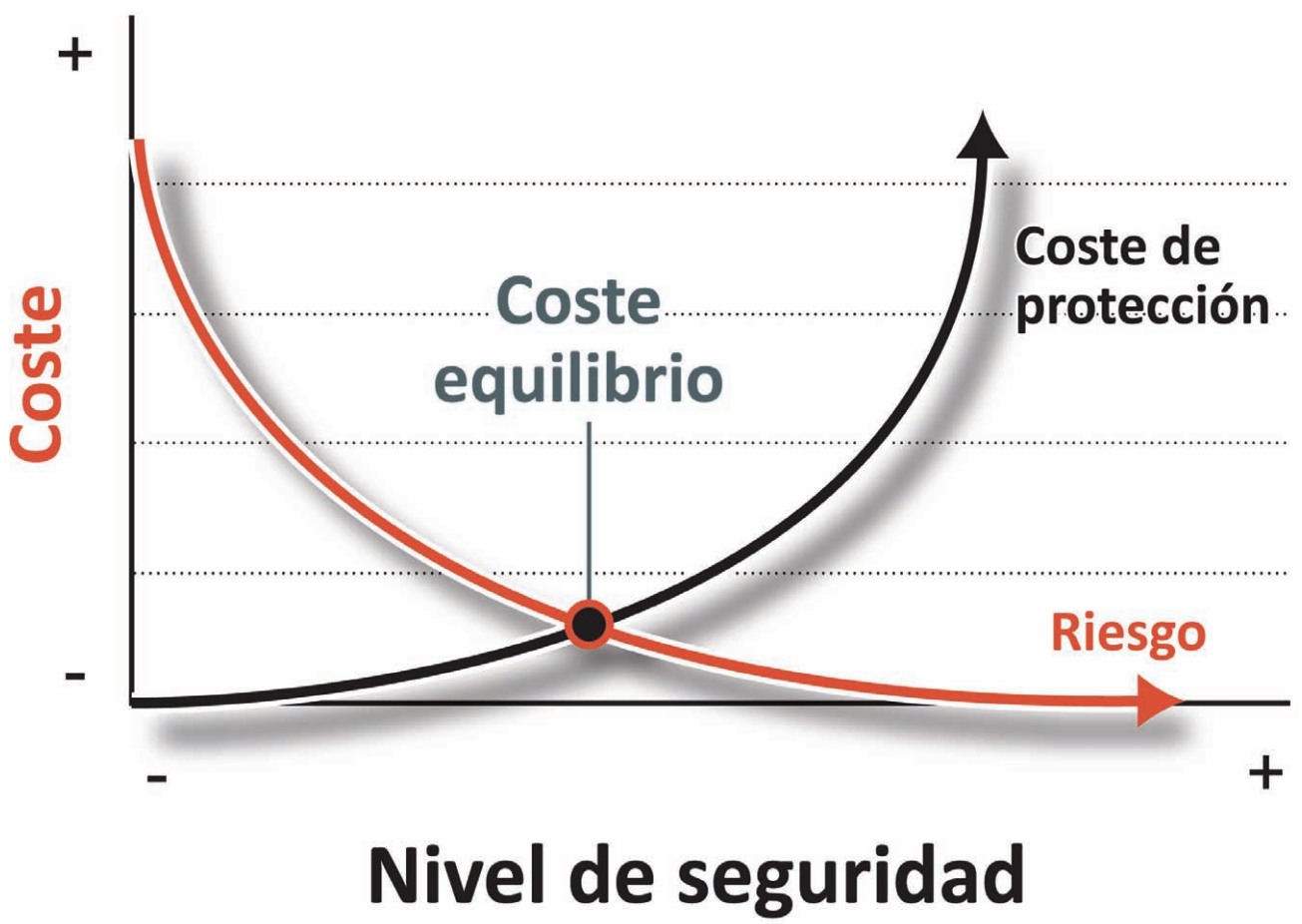
Si bien es posible -y en ocasiones necesario- realizar un análisis cualitativo, trabajar con magnitudes económicas facilita a las organizaciones establecer el llamado **umbral de riesgo**. Esto es: el **nivel máximo de riesgo que la empresa está dispuesta o asume soportar. La gestión de riesgos debe mantener el nivel de riesgo siempre por debajo del umbral**, y es un elemento fundamental de valoración para las compañías de seguros que ofrecen servicios de cobertura para los profesionales de la Abogacía y a sus instituciones.

Por otro lado, se denomina c**oste 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 velar por que no se inviertan 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.

"Nivel máximo de riesgo que la empresa está dispuesta o asume soportar"

"La gestión de riesgos debe mantener el nivel de riesgo siempre por debajo del umbral fijado"

"La gestión de riesgos debe mantener el nivel de riesgo siempre por debajo del umbral fijado"



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 y actividad de la organización.

2.3 ¿Qué hacer con los riesgos?

Las actividades dirigidas a 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 durante 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 para 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.

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 (p.e., no conectando a Internet determinados ordenadores que contienen información confidencial o sensible de nuestros clientes).

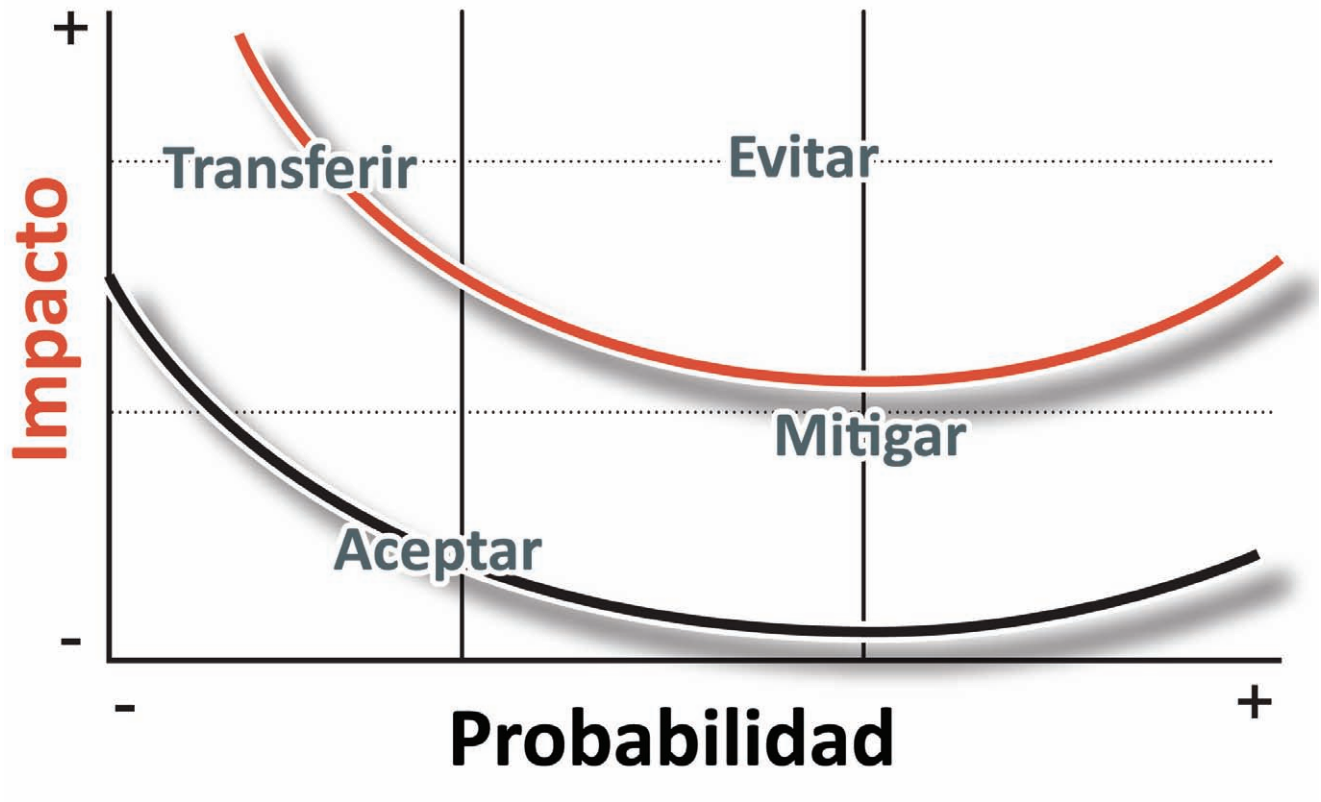
• **Reducirlo o mitigarlo:** tomando las medidas oportunas para que el nivel de riesgo se sitúe por debajo del umbral. Para conseguirlo se puede:

– ***Reducir la probabilidad o frecuencia de ocurrencia:*** tomando, por ejemplo, medidas preventivas (p.e., instalando medidas de seguridad físicas y lógicas).

– ***Reducir el impacto de la amenaza o acotar el impacto***, estableciendo por ejemplo controles y revisando el funcionamiento de las medidas preventivas (p.e., realizando auditorías de seguridad periódicas).

• **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 porque los costes de su tratamiento son elevados y aun siendo riesgos de impacto alto su probabilidad de ocurrencia es baja; o porque aún a pesar del riesgo la empresa no quiere dejar de aprovechar la oportunidad que para su negocio supone esa actividad arriesgada.



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:

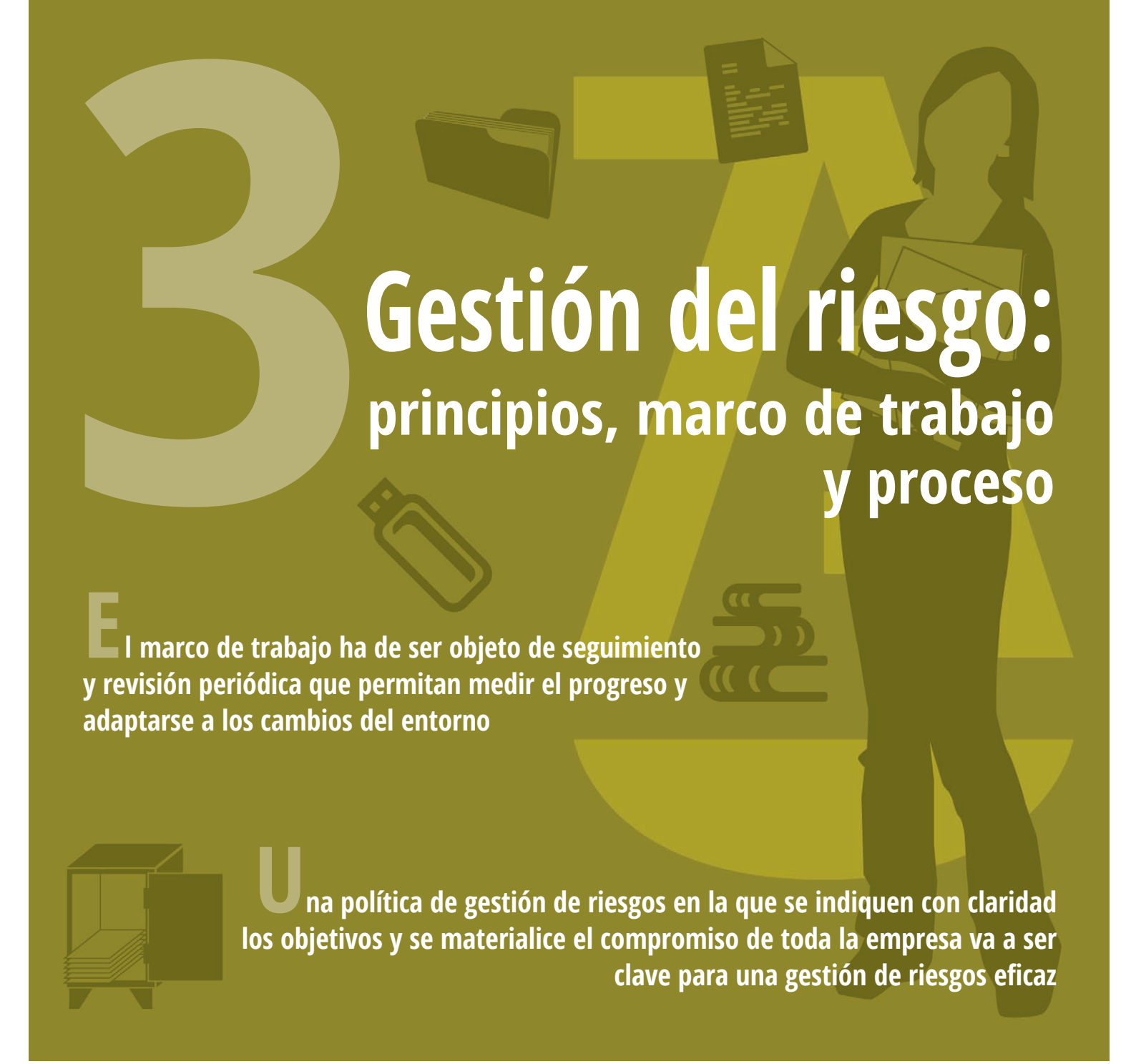
- **COSO:** organización americana dedicada a la creación de guías y marcos de trabajo en el ámbito de la gestión de riesgos empresariales. [1]
- **ISO 31000:2009:** norma global, no certificable, que aporta metodología, principios y directrices en materia de gestión de riesgos. [2]

Específicas para gestión de riesgos de seguridad de la información:

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

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



El marco de trabajo ha de ser objeto de seguimiento y revisión periódica que permitan medir el progreso y adaptarse a los cambios del entorno

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

Se califican cada uno de los riesgos identificados de forma:

- Cuantitativa (valorando su impacto)
- Cualitativa (importancia relativa)

Para priorizar nuestros esfuerzos de forma no arbitraria

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.

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

- **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

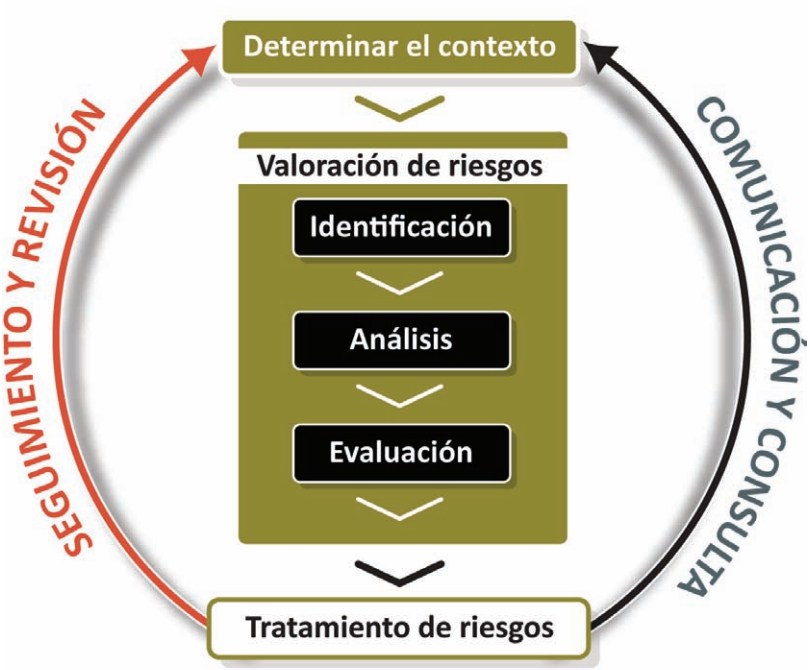
3.2.1 Política de gestión de riesgos

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:



3.3.1 Comunicación y consulta

Esta actividad es la primera a abordar, 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 organización como con su entorno externo. Por tanto hay que determinar los condicionantes internos y 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 debe procederse a valorar los riesgos.

En esta etapa se determinan los riesgos que deben ser controlados, lo que se hará a través de su identificación, análisis y evaluación. Aquellos otros riesgos que no sean identificados quedarán como riesgos ocultos o no controlados.

Se realizan en esta fase las siguientes actividades:

- **Identificación del riesgo:** tiene por objetivo la identificación y descripción de todos los posibles puntos de peligro tanto internos como externos, tras lo cual se determinará su impacto y probabilidad.

– Esta fase responde a las siguientes preguntas:

¿Qué puede pasar?

¿Cuándo y dónde?

¿Cómo y por qué?

- **Análisis de riesgos:** esta 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:** su 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.

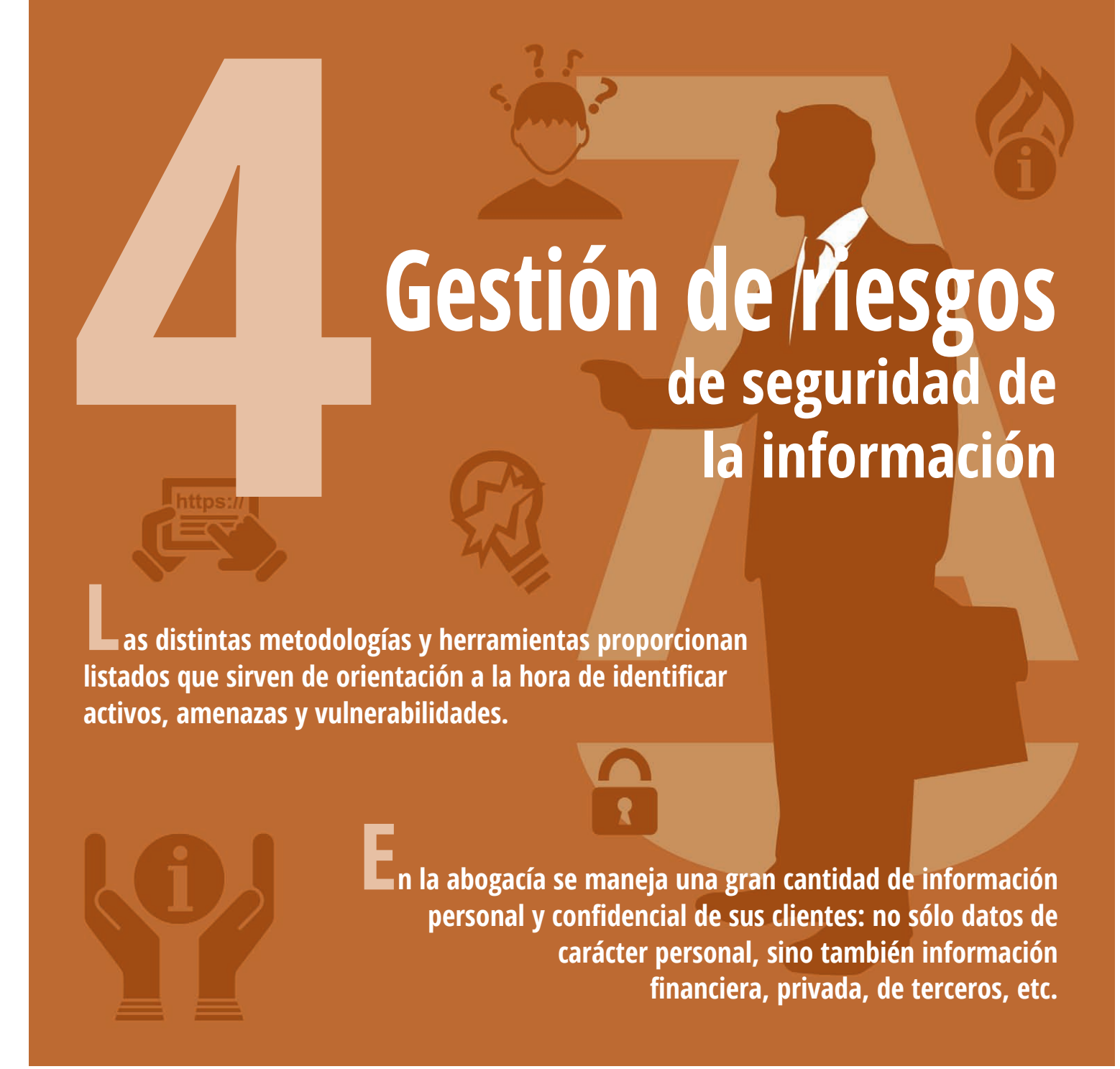
3.3.4 Tratamiento del riesgo

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 debe supervisar la realidad de lo que está ocurriendo, contrastando con nuestras previsiones, para poder realizar 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.

4 Gestión de riesgos de seguridad de la información



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

En la abogacía se maneja una gran cantidad de información personal y confidencial de sus clientes: no sólo datos de carácter personal, sino también información financiera, privada, de terceros, etc.

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

En la sociedad digital actual las compañías son conscientes del protagonismo de la información en sus procesos productivos. Muy en particular **en el sector de la Abogacía, donde se maneja una gran cantidad de información personal y confidencial de sus clientes: no sólo datos de carácter personal, sino también información financiera, privada, de terceros, etc.**

Esta revolución ha cambiado también las relaciones con clientes, proveedores y organismos oficiales, con Internet como protagonista. 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 debemos 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 obtención, almacenamiento, fin de vida útil y destrucción de la información.

Aunque la información es el activo principal a proteger, no debemos olvidar otros aspectos, tales como: la 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.

Seguridad de la información:

"Confidencialidad"

hablamos de protegerla de riesgos que

"Integridad"

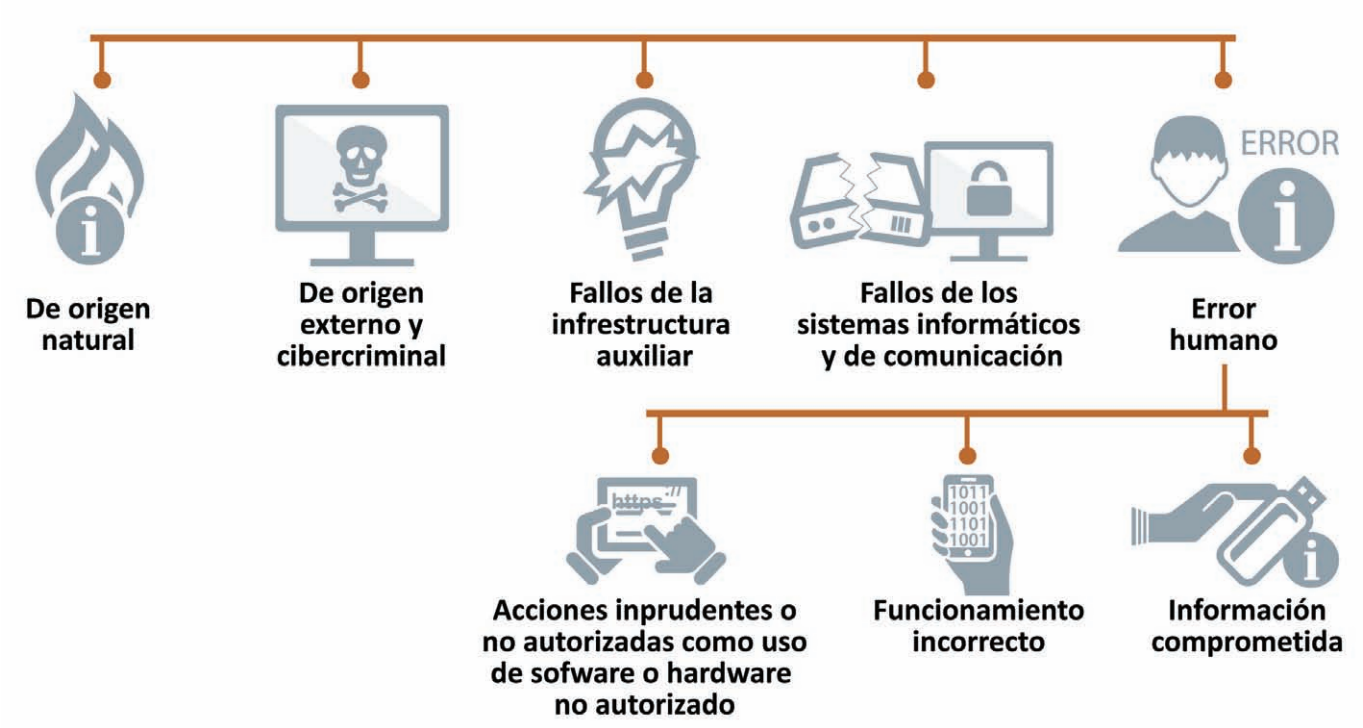
puedan afectar a una o varias de sus tres

"Disponibilidad"

principales propiedades:

Amenazas

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…
- **De origen externo y cibercriminal**: ciberataques, instalación de malware, conexión a redes de bots, etc.
- **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 imprudentes o no autorizadas como uso de software o hardware no autorizados*** (pe. Servicios en la nube que no cumplen con las medidas de seguridad apropiadas para albergar datos de un determinado nivel de protección de su confidencialidad)

  – ***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.

Vulnerabilidades

Las **vulnerabilidades** de las que 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.

Tales vulnerabilidades pueden afectar al hardware, al software, a las redes, al personal, al edificio o a las infraestructuras u 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.
- **Utilización de terminales personales,** sin las debidas medidas de protección adecuadas al nivel de criticidad de la información almacenada (BYOD).

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.

Además de todo ello, cabe recordar que, por sus particularidades, la Abogacía está sometida a normas legales y deontológicas, que hacen necesario que estos profesionales inviertan medidas de seguridad específicas para proteger sus activos.

Así, por ejemplo, en relación a este extremo encontramos una serie de preceptos que nos afectan directamente:

– **El Estatuto General de la Abogacía Española**, aprobado por **Real Decreto 658/2001, de 22 de junio**, establece una serie de normas dirigidas a proteger la libertad y la independencia del abogado, pero también impone una serie de obligaciones relacionadas con la gestión de riesgos informáticos a los que se enfrenta el abogado durante su ejercicio.

Entre las principales obligaciones, y con tal de salvaguardar el principio de confianza del cliente en su abogado (también citado en el artículo 4 y 5 del código deontológico), es fundamental la obligación de secreto de las comunicaciones, deber y derecho primordial de la Abogacía, mencionada en el **artículo 32.1**, cuando señala que "de conformidad con lo establecido por el artículo 437.2 de la Ley Orgánica del Poder Judicial, los abogados deberán guardar secreto de todos los hechos o noticias que conozcan por razón de cualquiera de las modalidades de su actuación profesional […]". También el **artículo 34:**

> *e) se refiere al deber de confidencialidad cuando señala como obligación de los colegiados la de "mantener como materia reservada las conversaciones y correspondencia habidas con el abogado o abogados contrarios, con prohibición de revelarlos o presentarlos en juicio sin su previo consentimiento".*

– Esta obligación de secreto aparece mencionada de nuevo en el **artículo 42.1**, según el cual:

> *"son obligaciones del abogado para con la parte por él defendida, además de las que se deriven de sus relaciones contractuales, el cumplimiento de la misión de defensa que le sea encomendada con el máximo celo y diligencia y guardando el secreto profesional".*

– Tales obligaciones se incluyen en un deber superior, que es la obligación de diligencia que debe regir toda actividad del abogado, incluyendo la adopción de medidas técnicas adecuadas para desarrollar su labor, a la que se refiere el **artículo 42.2** del propio Estatuto del modo siguiente:

> *"el abogado realizará diligentemente las actividades profesionales que le imponga la defensa del asunto encomendado, ateniéndose a las exigencias técnicas, deontológicas y éticas adecuadas a la tutela jurídica de dicho asunto y pudiendo auxiliarse de sus colaboradores y otros compañeros, quienes actuarán bajo su responsabilidad".*

– Todas estas obligaciones confluyen en la responsabilidad que asumen estos profesionales a la luz de las obligaciones ahí contempladas, tal y como recoge el **artículo 78** del Estatuto:

> *"1. Los abogados están sujetos a responsabilidad penal por los delitos y faltas que cometan en el ejercicio de su profesión.*
>
> *2. Los abogados en su ejercicio profesional, están sujetos a responsabilidad civil cuando por dolo o negligencia dañen los intereses cuya defensa les hubiere sido confiada, responsabilidad que será exigible conforme a la legislación ordinaria ante los Tribunales de Justicia, pudiendo establecerse legalmente su aseguramiento obligatorio".*

– Eso implica una obligación de cobertura de riesgo adecuada, tal y como ya menciona el código deontológico de la Abogacía en su **artículo 21**, cuyo **apartado 1** establece que:

> *"el abogado deberá tener cubierta, con medios propios o con el recomendable aseguramiento, su responsabilidad profesional, en cuantía adecuada a los riesgos que implique".*

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:

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**, y se podrá constituir un "comité de crisis" que coordine y asuma la responsabilidad en caso de tener que enfrentarse a un incidente de seguridad informático.

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

"Enfoque global o un enfoque detallado"

En esta fase 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.

"Las leyes que se deben cumplir"

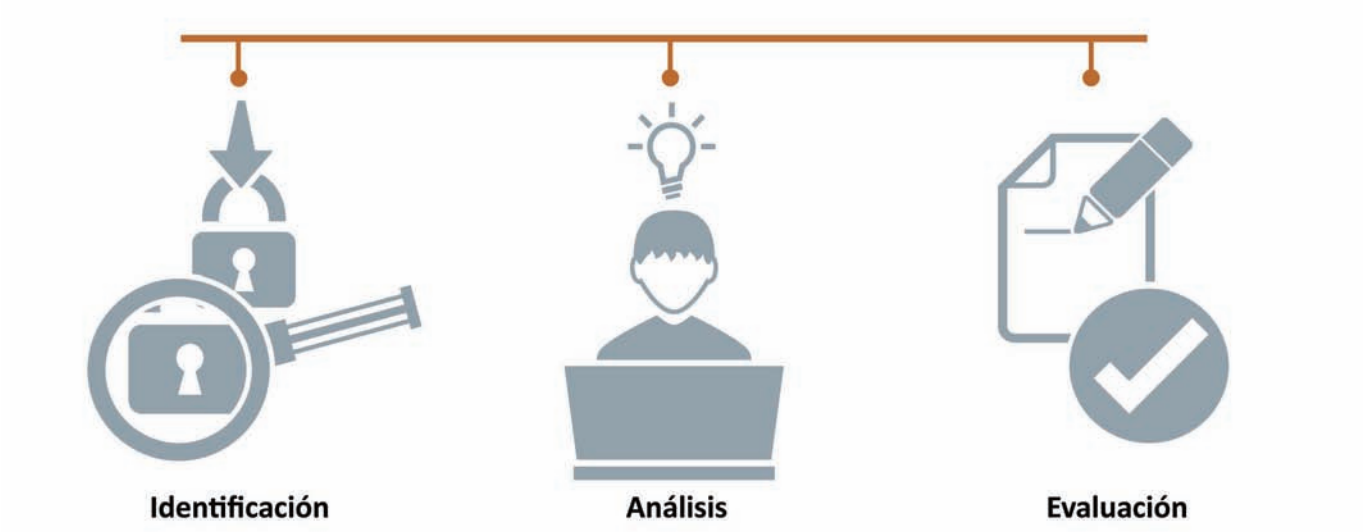
Tras este análisis deben quedar definidos los criterios para:

- **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, qué procesos, qué oficinas o qué 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:



4.2.3.1 Identificando los riesgos

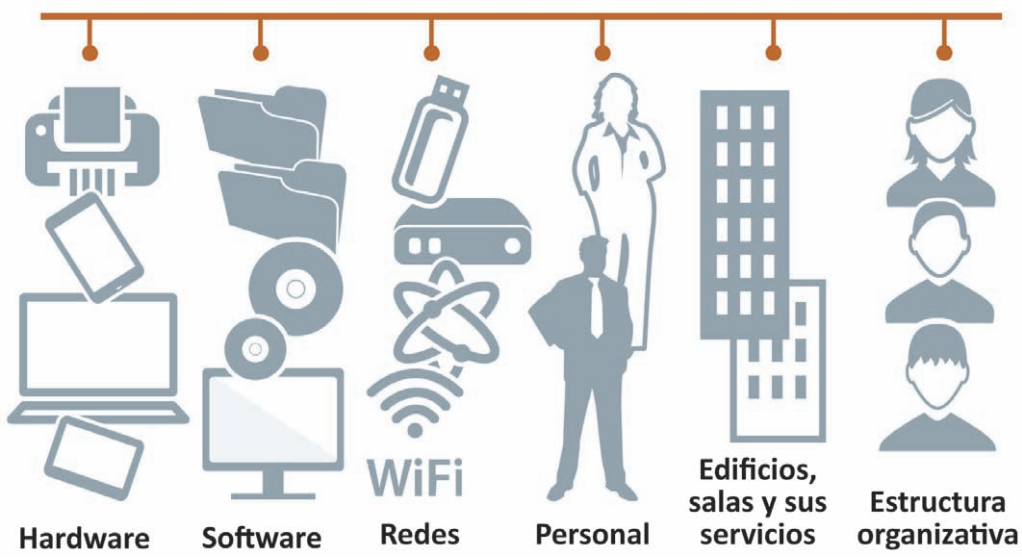
Para la evaluación de riesgos de seguridad de la información en primer lugar se han de identificar los activos de información. En general estos pueden ser de dos tipos:

- ***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, etc.*

– ***Redes:*** *conmutadores, cableado, puntos de acceso, etc.*

– ***Personal:*** *usuarios, desarrolladores, responsables, etc.*

– ***Edificios, salas y sus servicios***

– ***Estructura organizativa:*** *responsables, áreas, contratistas, etc.*

Después de obtener una relación de todos los activos disponibles en nuestra organización, habrá que **identificar y conocer las amenazas** susceptibles de causar daños en la información, los procesos y los soportes.

"Identificar y conocer las amenazas"

"Valoración de los daños"

Con tal de ser eficaces en la tarea de identificación de las amenazas y **la valoración de los daños** que pueden producir, es recomendable contrastar la información de que disponemos con los propietarios de los activos, usuarios, expertos, etc. En el apartado anterior se mencionan algunos ejemplos.

En lo que respecta a la valoración de los daños, estas serán algunas de las preguntas que deberemos formularnos:

¿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.

Llegados a este punto dispondremos de un listado de activos, sus amenazas y las medidas que ya se han tomado. Eso nos va a permitir revisar las vulnerabilidades que pueden ser aprovechadas para causar daños a nuestros activos de información. Existen distintos métodos para analizar amenazas, como por ejemplo:

- ***Entrevistas con usuarios y cuestionarios***
- ***Inspección física***
- ***Uso de herramientas para el escaneo automatizado***

Para cada una de las amenazas habrá que realizar un análisis de aquellas vulnerabilidades que pueden ser explotadas. La norma ISO 27005 [11] incluye un anexo con ejemplos de vulnerabilidades y amenazas que puede servir de apoyo en esta tarea.

Finalmente hay que 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

"Medir las consecuencias o impactos"

En la fase de establecimiento del contexto se determinaron una serie de criterios que serán las directrices que podemos seguir para la estimación de los riesgos a los que se enfrentan nuestros activos.

Tales criterios 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 que permitan valorar:

Esta tabla muestra un posible ejemplo de estos criterios:

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

Los métodos para realizar tal ejercicio incluyen estimaciones cualitativas y cuantitativas o una combinación de ambas. Inicialmente suele realizarse una estimación cualitativa que permita identificar los riesgos que precisan una estimación cuantitativa.

En la estimación cualitativa se califican las potenciales consecuencias, así como su probabilidad, aplicando una graduación por niveles (alto, medio, bajo). 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.

Además de medir las posibles consecuencias debe asimismo estimarse 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
- ***Actores 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

El objetivo es obtener una valoración clara de las consecuencias y de su probabilidad, de manera que podamos realizar una estimación del nivel del riesgo lo más exacta posible.

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, queda 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	–	1	2	3	4	5
	Impacto	Insignificante	Menor	Serio	Desastroso	Catastrófico

“Estimar qué tratamiento dar a cada riesgo”

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.

Coste-beneficio	Tratamiento
El coste es muy superior a los beneficios	**Evitar el riesgo**, por ejemplo, dejando de realizar esa actividad
El coste 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 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

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.

"Aceptación del riesgo"

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:

- ***N*uevos activos o modificaciones en el valor de los activos**
- ***N*uevas amenazas**
- ***C*ambios o aparición de nuevas vulnerabilidades**
- ***A*umento de las consecuencias o impactos**
- ***I*ncidentes 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:

- ***L*as categorías de activos**
- ***L*os criterios de evaluación de riesgos**
- ***L*os niveles de clasificación de los impactos**
- ***L*as escalas de aceptación de riesgos**
- ***L*os 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.

“Poner en marcha un Plan director de seguridad de la información”

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://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf> [consulta: 12/05/2015]

[5] INCIBE Protege tu empresa - Blog (2014) «Sigue el camino del análisis de riesgos» <https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Sigue_camino_analisis_riesgo> [consulta: 12/05/2015]

[6] INCIBE - Protege tu empresa - Blog (2014) «Fácil y sencillo: análisis de riesgos en 6 pasos» <https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/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/empresas/que_te_interesa/Plan_director_de_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/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/nueva_version_iso27001> [consulta: 12/05/2015]

[13] Código Deontológico Abogacía

[14] Estatuto General de la Abogacía Española

GUÍAS TIC ABOGACÍA ESPAÑOLA: Ciberseguridad

GESTIÓN DE RIESGOS

Una guía de aproximación al Compliance para la Abogacía

Abogacía Española
CONSEJO GENERAL

incibe_

www.abogacia.es

@RedAbogacia @Abogacia_es