GESTIÓN Y MEDIDAS A ADOPTAR FRENTE A LA FUGA DE INFORMACIÓN

1. INTRODUCCIÓN

- Dentro de una empresa existen bienes intangibles de gran valor. Elementos de información que forman parte de la empresa y que constituyen uno de los aspectos más importantes de la organización. Y en este entorno, más allá de la seguridad física, la seguridad lógica cobra una especial relevancia y por ello requiere una especial atención.

- En efecto, la información se ha convertido en uno de los activos más importantes que posee una empresa. Tal información, en caso de pérdida, sustracción o acceso no consentido por parte de terceros, puede ser empleada con fines indeseados (extorsión, desprestigio, etc.) o, simplemente, utilizada como objeto que se comercializa y vende a escala global en todo tipo de ámbitos y sectores.

- Todo ello está convirtiendo a las fugas de información en una de las mayores amenazas a la que nos enfrentamos en el nuevo mundo conectado en el que vive una empresa como la nuestra, basada en la confianza que los clientes depositan en nosotros.

- En la sociedad actual existen constantes amenazas online, que de manera automatizada (pe., las redes de ordenadores zombies, comúnmente conocidas como botnets), ponen en permanente riesgo la información que tratamos y almacenamos en nuestro despacho, lo que nos obliga a adoptar una serie de medidas de salvaguarda de la responsabilidad legal y deontológica a la que estamos sujetos como profesionales. (INCIBE – Dossier protección de la información).

- Por estos motivos, la ciberseguridad debe ser un elemento indispensable en la estrategia de nuestra empresa: la protección frente a las ciberamenazas (virus, daños informáticos, ataques a páginas web, fraude y robo de identidad online, destrucción de información,...) y el fomento de las medidas de prevención y reacción, son factores esenciales para evitar o minimizar las filtraciones de información y la consecuente pérdida de imagen de nuestro empresa. A lo que habrá que añadir que cualquier incidente en nuestra organización también afectará a terceras personas, como pueden ser otros clientes o proveedores.

- Por eso, la implantación de medidas tecnológicas de ciberseguridad es tan importante. Pero no hay que descuidar la implementación de medidas organizativas que ayuden a la sensibilización, formación, concienciación y educación de todos los miembros de la organización.

- Este último punto es especialmente importante, en tanto en cuanto la información a la que accedemos desde nuestra organización es tratada por personas. Es por ello por lo que son cada vez más habituales los ataques basados en ingeniería social (pe., en casos de suplantación de identidad), cuyo objetivo es engañar al personal de la organización o provocar errores en la gestión interna de la información al objeto de que el ciberataque tenga éxito

2. FUGA DE INFORMACIÓN

La protección de la información se articula en torno al respeto de tres principios básicos: confidencialidad, integridad y disponibilidad.

1.- La confidencialidad implica que la información sea accesible únicamente por el personal autorizado.

2.- La integridad de la información implica que la información sea correcta y esté libre de modificaciones y errores. Hay que tener presente que la información ha podido ser alterada intencionadamente o ser incorrecta, lo que supone un riesgo si estamos basando nuestras decisiones en ella.

3.- La disponibilidad de la información se refiere a que la información esté accesible para las personas o sistemas autorizados, cuando sea necesario.

Llamamos **fuga de información** a la pérdida de la confidencialidad, de forma que personal no autorizado accede a información privilegiada.

En cualquier caso, las consecuencias derivadas de un incidente de fuga de información van a ser siempre negativas: por un lado, en un aspecto tan importante como en la reputación de la empresa, ya que el conocimiento público de la existencia de una filtración de información dañará nuestra imagen, impactando muy negativamente en el negocio y generando desconfianza e inseguridad en los clientes. Y, de otro lado, la publicación de información puede generar consecuencias a terceros: grupos externos de usuarios y otras organizaciones cuyos datos se hayan hecho públicos.

Este aspecto es especialmente importante, por cuanto en relación a los supuestos de fuga de información (los comúnmente conocidos como data breach), en su mayoría terminan con la difusión o publicación de datos de carácter personal (pe. números de tarjetas de crédito, DNI, etc.).

Este es uno de los aspectos más críticos de la gestión de la fuga de información y será también una de las responsabilidades de la organización, de cara a decidir cómo tratar este incidente, tanto desde el punto de vista de cumplimiento de obligaciones legales, como de tratamiento con los medios de comunicación.

En este sentido, y para aquellos supuestos en los que una fuga de información conlleve una fuga de datos personales, el **Reglamento Europeo de Protección de Datos** contiene una serie de previsiones y obligaciones para el responsable del tratamiento.

En efecto, los **Considerandos 85 a 87 y los artículos 33 y 34**, recogen la obligación para el responsable del tratamiento de que, tan pronto como éste tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, deberá, sin dilación indebida, y a más tardar 72 horas después de que haya tenido constancia de ella, notificar tal violación de seguridad a la autoridad de control competente, a menos que el responsable pueda demostrar la improbabilidad de que la citada violación entrañe un riesgo para los derechos y libertades de las personas físicas afectadas (pe., porque tales datos iban cifrados o porque se han adoptado medidas ulteriores eficaces que garanticen que ya no existe tal riesgo). Es lo que se conoce como Data Breach Notification.

Además de tal notificación, el responsable del tratamiento de los datos objeto de la fuga (en este caso, el despacho) deberá comunicar al interesado, sin dilación indebida, la violación de la seguridad de sus datos personales en caso de que ésta pueda entrañar un alto riesgo para sus derechos y libertades.

Tal notificación deberá realizarse respetando el contenido mínimo establecido en el artículo 34 del citado Reglamento europeo. Esta comunicación es importante al objeto de que las personas afectadas por la fuga de sus datos estén informados del incidente y de los datos que han sido sustraídos, a fin de que puedan tomar las acciones oportunas para su seguridad, tales como el cambio de contraseñas, la revocación de números de tarjetas, ser especialmente cautelosos con eventuales accesos a sus cuentas de correo, etc.

Además, se debe proporcionar algún canal para que los afectados puedan mantenerse informados sobre la evolución del incidente y las distintas recomendaciones que pueda realizar la organización a los afectados, con el objetivo de minimizar las consecuencias.

En relación a la competencia para conocer este tipo de situaciones, **la Agencia Española de Protección de Datos (AEPD) es la autoridad estatal encargada de velar por el cumplimiento de la normativa sobre protección de datos.** Sus funciones son garantizar y tutelar el derecho fundamental a la protección de datos de carácter personal de los ciudadanos.

2.1. ORIGEN Y MOTIVOS

El **origen de las amenazas** que provocan las fugas de información puede ser tanto externo como interno.

a) Origen interno: dentro de este punto incluimos las fugas de información ocasionadas por empleados propios de la empresa, ya sea de forma inconsciente (por desconocimiento o por error) o dolosa (en el caso de empleados de la propia organización que voluntariamente facilitan el acceso o revelan tal información a terceros sin autorización, lo que comúnmente se conoce por *"insider"*).

b) Origen externo: en este grupo incluimos amenazas que provienen de fuera de nuestra organización y que tienen por objetivo acceder de manera ilícita a información confidencial. Entre estos supuestos podemos destacar, por ejemplo:

- **El hackitivismo:** terceros que quieren mostrar su desacuerdo con la actividad que realiza el despacho o los clientes a los que defiende.
- **La venganza de clientes descontentos** o de antiguos empleados.
- **El robo de información confidencial:** el acceso no consentido a información privilegiada de clientes o relacionada con expedientes concretos por parte de organizaciones criminales, o ciberdelincuentes que persiguen sustraer datos confidenciales buscando una ventaja competitiva o la obtención de beneficio económico.
- **El ataque de terceros** que simplemente buscan el daño ala imagen del despacho.
- **Otros cuyo objetivo es realizar actividades de competencia desleal.**

2.2. CAUSAS Y PREVENCIÓN

En la mayoría de los casos, las fugas de información implican la ausencia o ineficiencia de algún tipo de medida o de procedimiento de seguridad, implementados para evitar este tipo de incidentes. Esta carencia de medidas conlleva un inadecuado control sobre la información que se maneja, lo que hace aumentar de forma significativa la probabilidad de que se produzca un incidente que lleve consigo una fuga de información.

Las causas principales de las fugas de información (y por tanto el carácter de las medidas preventivas que se deberán adoptar) pueden ser clasificadas en dos grupos estrechamente relacionados: aquellas que pertenecen al ámbito organizativo y aquellas que hacen referencia al ámbito técnico.

a) Dentro de las causas organizativas.

- Uno de los primeros errores que se comete durante la protección de la información es la **falta de clasificación** de la misma. Esta clasificación se puede realizar en base a su nivel de confidencialidad y en función de diversos parámetros como el valor que tiene para la organización, el impacto que puede generar su filtración, su nivel de sensibilidad o si se trata de información personal o no.

Si se desconoce el valor de la información que trata la organización, no será posible diseñar ni implementar las medidas de protección adecuadas.

- Otro de los errores suele ser la **falta de delimitación del ámbito de difusión** de la información. Una correcta delimitación del alcance de tal información nos permitirá establecer el perímetro dentro del cual podrá ser difundida la información y su nivel de confidencialidad.

Disponer de estos recursos es fundamental para poder determinar quién debe conocer la información y qué tipo de acciones puede realizar sobre esta. Esto se conoce como principio del mínimo conocimiento.

- La **falta de conocimiento y formación** son otra de las causas más comunes de la fuga de información. Esta circunstancia facilita la producción de errores por parte de los empleados, quienes, por un lado, deben utilizar los recursos que la empresa pone a su disposición de forma responsable y diligente (como es el caso de los servicios en la nube, los dispositivos móviles, el correo electrónico, las redes sociales o la simple navegación por Internet); pero, de otro lado, también debe disponer de ciertos conocimientos y formación en materia de ciberseguridad, siendo responsabilidad de la organización proporcionar a su plantilla y colaboradores la formación necesaria de manera que el empleado pueda desempeñar su función de forma segura.

- Otra causa organizativa es la **ausencia de procedimientos** y de pautas u obligaciones para los trabajadores en el ámbito de ciberseguridad. El establecimiento de políticas que indiquen al usuario claramente cuáles son los límites dentro de los cuales deberán desempeñar su actividad y por otro lado, los procedimientos para aquellas actividades de especial importancia o riesgo, disminuirán el riesgo de que se produzca una fuga de información.

- Por último, también la **inexistencia de acuerdos de confidencialidad** con la plantilla es un elemento que fomenta la producción de fugas de datos. Es importante solicitar por escrito la conformidad de los empleados con normas internas de esta naturaleza, como pueden ser la política de confidencialidad o de seguridad, entre otras, de manera que el futuro empleado, acepte por escrito las políticas y condiciones de privacidad y seguridad aplicables a la organización.

a) Dentro de las causas organizativas,

- Uno de los primeros errores que se comete durante la protección de la información es la **falta de clasificación** de la misma. Esta clasificación se puede realizar en base a su nivel de confidencialidad y en función de diversos parámetros como el valor que tiene para la organización, el impacto que puede generar su filtración, su nivel de sensibilidad o si se trata de información personal o no.

Si se desconoce el valor de la información que trata la organización, no será posible diseñar ni implementar las medidas de protección adecuadas.

- Otro de los errores suele ser la **falta de delimitación del ámbito de difusión** de la información. Una correcta delimitación del alcance de tal información nos permitirá establecer el perímetro dentro del cual podrá ser difundida la información y su nivel de confidencialidad.

Disponer de estos recursos es fundamental para poder determinar quién debe conocer la información y qué tipo de acciones puede realizar sobre esta. Esto se conoce como principio del mínimo conocimiento.

- La **falta de conocimiento y formación** son otra de las causas más comunes de la fuga de información. Esta circunstancia facilita la producción de errores por parte de los empleados, quienes, por un lado, deben utilizar los recursos que la empresa pone a su disposición de forma responsable y diligente (como es el caso de los servicios en la nube, los dispositivos móviles, el correo electrónico, las redes sociales o la simple navegación por Internet); pero, de otro lado, también debe disponer de ciertos conocimientos y formación en materia de ciberseguridad, siendo responsabilidad de la organización proporcionar a su plantilla y colaboradores la formación necesaria de manera que el empleado pueda desempeñar su función de forma segura.

- Otra causa organizativa es la **ausencia de procedimientos** y de pautas u obligaciones para los trabajadores en el ámbito de ciberseguridad. El establecimiento de políticas que indiquen al usuario claramente cuáles son los límites dentro de los cuales deberán desempeñar su actividad y por otro lado, los procedimientos para aquellas actividades de especial importancia o riesgo, disminuirán el riesgo de que se produzca una fuga de información.

- Por último, también la **inexistencia de acuerdos de confidencialidad** con la plantilla es un elemento que fomenta la producción de fugas de datos. Es importante solicitar por escrito la conformidad de los empleados con normas internas de esta naturaleza, como pueden ser la política de confidencialidad o de seguridad, entre otras, de manera que el futuro empleado, acepte por escrito las políticas y condiciones de privacidad y seguridad aplicables a la organización.

b) Dentro de las causas técnicas podemos destacar:

- El **código malicioso o *malware*** (pe. los troyanos), es una de las principales amenazas, siendo el robo de información uno de sus objetivos más comunes. El *malware* está muchas veces diseñado utilizando técnicas que permiten mantener oculto su código en un sistema, mientras recoge y envía información, lo que dificulta su localización.

- El **acceso no autorizado a sistemas e infraestructuras** es otro de los principales riesgos a evitar. Gran parte de estos accesos no autorizados se podrían evitar si los sistemas y aplicaciones estuvieran convenientemente actualizados. La actualización se considera parte fundamental de una buena gestión y de responsabilidad corporativa, puesto que aporta mayor seguridad y denota un trabajo de mejora continua que redunda en beneficio de la aplicación y, por extensión, del usuario.

- La **generalización del uso de servicios en la nube** para el almacenamiento de todo tipo de información puede llevar a la percepción de que en la nube nuestra información está segura, cuando lo cierto es que no sólo depende de eso. El nivel de seguridad que tiene depende de la robustez de las contraseñas de los propios usuarios y de su formación en ciberseguridad.

- El **uso de las tecnologías móviles para el trabajo diario** (conocido por *Bring Your Own Device* o *BYOD*) almacenando en ellos información de la empresa -en ocasiones crítica-, han llevado a la generalización de medidas como el uso de herramientas de cifrado de la información o el uso de VPN (redes privadas virtuales) en las comunicaciones. Sin embargo, si la información almacenada en los dispositivos es realmente crítica, deben intensificarse las políticas y medidas de seguridad a implementar. En todo caso, y aunque parezca una obviedad, las medidas de seguridad deben haberse tomado con anterioridad al incidente, porque una vez este ocurre hay poco margen de maniobra.

2.3. ¿CÓMO PODEMOS MITIGAR LA FUGA DE INFORMACIÓN?

Visto que el factor humano es uno de los principales motivos de fugas de información, es muy importante llevar a cabo campañas de concienciación en materia de ciberseguridad dentro del despacho, sin perjuicio de que podamos hacerlas extensivas a terceros con los que mantengamos relaciones comerciales o profesionales, tales como proveedores, colaboradores u otro personal externo.

Además conviene **desarrollar y mantener actualizadas políticas claras y completas de acceso a la información,** debiéndonos asegurar de que son bien conocidas por todos los miembros de la organización y, en su caso, terceros ajenos a la misma que deban acceder a información del despacho en base a algún tipo de relación contractual. En relación a este extremo, es importante que la organización siga el principio del mínimo privilegio, el cual se traduce en que un usuario sólo debe tener acceso a aquella información de carácter sensible estrictamente necesaria para desempeñar sus funciones diarias. Dicho de otro modo, nadie de la organización deberá tener permiso de acceso a información que no necesite por razón de su cargo o funciones.

Dentro de esta imprescindible labor de prevención, es importante conocer los productos y servicios que la industria de ciberseguridad ofrece, muchas veces de forma gratuita, para mitigar esta amenaza. Por citar algunos, podemos destacar aquellos destinados a la gestión del ciclo de vida de la información (ILM, del inglés *Information Life-cycle Management*), productos para el control de dispositivos externos, u otros destinados específicamente a evitar la fuga de información (DLP, del inglés *Data Loss Prevention*).

No obstante la implantación de medidas preventivas técnicas y organizativas, sigue existiendo la posibilidad de que se produzca un incidente de seguridad relacionado con la información que se maneja en el despacho. Por eso, además de estar continuamente implementando nuevas medidas de protección, siempre debemos estar preparados por si se produce tal incidente: disponer de un plan de riesgos adecuado, de un programa de *compliance* y de haber implementado medidas tecnológicas apropiadas son actuaciones esenciales de cara a dificultar la producción de incidentes, a minimizar su impacto dentro de la organización, y a graduar eventuales responsabilidades legales y deontológicas que nos pudieran afectar.

Aun así, **¿qué debemos hacer si se produce una fuga de información en nuestra empresa?**

En los apartados siguientes se desarrollarán los diferentes aspectos relacionados con la gestión del incidente una vez se haya producido, ya que hay que gestionar las posibles consecuencias del impacto de la fuga de información, tanto sobre la organización como sobre otros actores externos.

Las consecuencias que pueden derivarse de un incidente de fuga de información deben preocupar, y mucho, a las empresas.

La adecuada gestión de incidentes de esta naturaleza pasa por comprender sus posibles consecuencias, ya que sin ello no será posible diseñar una estrategia adecuada para poder tomar las decisiones e implantar las medidas adecuadas para gestionar y minimizar el impacto del incidente, una vez hubiera llegado a producirse.

Determinar las consecuencias y el impacto de un incidente de fuga de información es una tarea muy compleja que depende de muchos factores. En el siguiente apartado vamos a analizar algunos de esos factores, que servirán de base para poder determinar el posible nivel de impacto.

3.1. ESTIMACIÓN DEL IMPACTO

Las eventuales consecuencias derivadas de un incidente de fuga de información pueden agruparse en las siguientes categorías, que están relacionadas entre sí y pueden darse conjuntamente:

a) Daños reputacionales: se genera un impacto muy negativo de la imagen de nuestra empresa, lo que lleva aparejado la pérdida de confianza de clientes y proveedores.

b) Consecuencias regulatorias: un incidente de esta naturaleza puede derivar en sanciones de distinta entidad, tanto civiles, penales o administrativas, en ocasiones de elevado importe.

c) Consecuencias económicas: estrechamente relacionadas con las anteriores se encuentran aquellas que suponen un impacto negativo a nivel económico, con una disminución de la inversión, negocio, etc.

En el ámbito de la ciberseguridad, no es cierto que las empresas grandes estén más expuestas al riesgo. Las consecuencias de una fuga de información no dependen tanto del tamaño o área de especialización de una empresa, sino de la criticidad de la información que maneje. Por eso es tan importante atender al tipo de información que se maneja dentro de la organización:

-**Información confidencial o restringida:** entendida como aquella información que consideremos crítica para los procesos de nuestra entidad. Por ejemplo: datos de nuestros clientes y de los procedimientos que les afecten, datos de contabilidad, datos de los propios trabajadores, etc.

-**Información no confidencial:** a estos efectos se considera aquella información cuya revelación y divulgación impactaría en la imagen de la empresa, pero el peso del impacto económico será menor.

Otro de los factores que definen el escenario es el tipo de datos que se han podido ver afectados. A estos efectos podemos diferenciar:

-**Datos de carácter personal:** cualquier dato que identifique o que pueda ser asociado a una persona identificada. Su divulgación o difusión pueden conllevar sanciones para la organización que ha sufrido el incidente.

-**Otros datos:** aquellos que no son datos de carácter personal, como por ejemplo, información técnica u operativa, secretos comerciales, etc.

En base a estos factores podemos tener una aproximación que nos ayude a determinar las posibles consecuencias de un incidente. Y, a partir de ahí, adoptar las medidas técnicas u organizativas adecuadas para remediarlo.

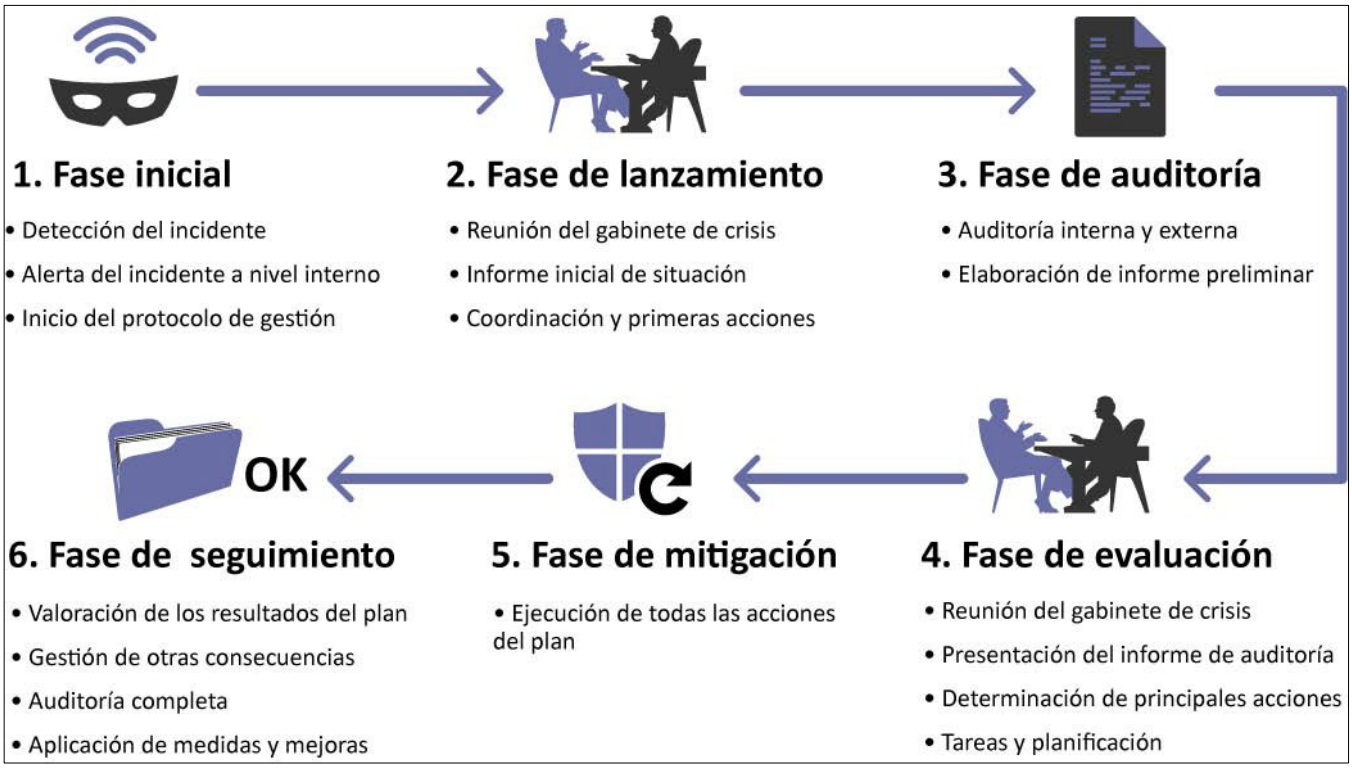
Para obtener una escala de valor de las consecuencias será necesario contar con una valoración objetiva tanto de los factores antes expuestos como de otros aspectos, siguiendo un procedimiento de análisis de riesgos. Para ello, deberemos tener en cuenta el activo a proteger de la fuga de información, la amenaza, la probabilidad de que ocurra y el impacto, aspectos estos que nos permitirán obtener el dato real de riesgo.

d) Otras consecuencias: en este apartado se incluyen aquellas que pueden suponer un impacto negativo en otros ámbitos como, entre otros, el político, diplomático, institucional o gubernamental.

Al ser tantos los aspectos y situaciones que confluyen en la producción de este tipo de incidente, su gestión requiere una combinación de aptitudes que eviten una mala gestión del mismo. Tengamos presente que un tratamiento inadecuado de un incidente de este tipo podría provocar el efecto contrario al deseado, magnificando su impacto negativo a todos sus niveles.

El **Plan para la gestión** de los incidentes de fuga de información que se propone a continuación recoge los principales puntos y aspectos a tener en cuenta por parte de un despacho de abogados que quiera reforzar su capacidad de prevención y reacción ante un incidente de estas características.

La gravedad del incidente y el contexto en el que se produzca hará que los diferentes pasos a seguir deban adaptarse al escenario específico en el que se produzcan.



4.1. FASE INICIAL

Los momentos inmediatamente posteriores a la detección de una fuga de información son especialmente críticos. Una rápida y adecuada gestión en las primeras fases puede suponer una eficaz reducción del impacto del incidente y una minimización de sus efectos.

Excepto en el caso de pérdida de dispositivos o terminales, la propia naturaleza del incidente hace que en la mayoría de las ocasiones aquél no sea detectado ni identificado hasta que la información se filtra, haciéndose pública a través de Internet o de cualquier otro medio.

Por este motivo, uno de los mayores retos a los que se enfrentan las organizaciones es conseguir la **detección temprana del incidente.** A estos efectos, una práctica que puede ser de utilidad es la constante monitorización online (incluyendo la *deep web* en la medida de los posible) de cualquier publicación que pueda afectar a nuestra entidad, para de este modo poder tomar el control de la situación lo antes posible.

Una vez que hayamos tenido conocimiento del incidente deberemos **informar internamente de la situación,** activando el protocolo de actuación que tengamos diseñado en nuestra organización para la gestión de esos casos. Dentro de la información que compartamos con las personas de nuestra organización responsables de gestionar este tipo de incidentes, es importante incidir en la prudencia y confidencialidad, redirigiendo al interlocutor previamente designado cualquier duda o pregunta que pueda surgir, tanto desde los propios empleados como de terceros. Además, se deberá informar a los últimos responsables de nuestra empresa de la activación del procedimiento de gestión de ciberincidentes.

Finalmente hay que recordar que si la fuga de información conlleva datos personales, el Reglamento Europeo de Protección de Datos recoge que el responsable del tratamiento tiene la obligación de notificar la violación de seguridad a la Agencia Española de Protección de Datos en las 72 horas siguientes a haber tenido conocimiento de que se ha producido la misma. Además deberá notificar al interesado si ésta entraña un alto riesgo para sus derechos y libertades. De aquí la importancia de activar rápidamente el protocolo interno de gestión del incidente.

4.2. FASE DE LANZAMIENTO

Una vez se activa el protocolo interno de gestión del incidente, el primer paso es el de convocar a los miembros del comité o gabinete de crisis, entendido como aquel equipo de gestión responsable de tomar las decisiones durante este proceso.

Mantener la calma y actuar coordinada y organizadamente es fundamental para evitar decisiones incorrectas o que pueden provocar consecuencias negativas adicionales.

Será necesario contar como mínimo con un responsable con capacidad de decisión, ya sea personal propio de la empresa o externo, que se encargará de la gestión y coordinación de la situación. Cuanto más cerca esté el responsable del gabinete del máximo responsable de la empresa, más efectiva será la gestión.

En cualquier caso, **todas las decisiones y las actuaciones relacionadas con el incidente deberán ser tomadas y coordinadas por el gabinete de crisis.** Es fundamental evitar actuaciones por libre o que no hayan sido definidas y consensuadas por el gabinete, y dejar constancia de las mismas en cada momento.

4.3. FASE DE AUDITORÍA

Una vez se han iniciado los pasos anteriores, daría comienzo la fase de obtención de información sobre el incidente. Para ello, **será necesario iniciar una auditoría interna**, con el objetivo de determinar con exactitud y en el menor tiempo posible lo siguiente:

a)Determinar la cantidad (tamaño en disco, número de registros, etc.) de información que ha podido ser sustraída.

b)Establecer el tipo de datos que contiene la información que ha podido ser sustraída. Debe prestarse especial atención si se han filtrado datos de carácter personal y de qué nivel, ya que esto podrá accionar una serie de actuaciones específicas, de conformidad con la normativa sobre protección de datos.

c)Determinar si la información pertenece a la nuestra empresa o es externa, es decir, si se trata de información exclusivamente interna o que hace referencia o afecta a organizaciones o personas terceras de fuera de la empresa, con especial consideración a los datos de nuestros clientes.

d)Establecer y acotar la causa principal de la filtración, en el sentido de determinar si tiene un origen técnico o humano. Si el origen es técnico, hay que identificar los sistemas que están afectados o en los cuales se ha producido la brecha. Si es de origen humano, deberá iniciarse el proceso para identificar cómo y cuándo se ha producido la fuga y quiénes han sido los responsables de esa fuga de información.

Además de la auditoría interna, **también es necesario realizar una auditoría externa.** El objetivo de ésta será conocer el tamaño, gravedad y nivel de difusión de la filtración en el exterior de la organización. Hay que distinguir entre aquella información que haya sido sustraída de la información que se ha hecho pública, ya que no son necesariamente lo mismo. Al menos es necesario:

a)Determinar el alcance de la publicación de la información sustraída (dónde se ha publicado, cuántos potenciales accesos ha podido tener, etc.). Este punto es crítico para poder cerrar la brecha de seguridad y mitigar la difusión de la información sustraída.

b)Establecer qué información se ha hecho pública y determinar la cantidad (tamaño en disco, número de registros, etc.) de la información filtrada en el exterior de la organización.

c)Recoger las noticias y otros contenidos que hayan aparecido en los medios de comunicación, así como en otros medios en Internet sobre el incidente.

d) Conocer las reacciones que se están produciendo en relación con el incidente.

En esta fase, **el tiempo de reacción es crítico.** De forma orientativa es recomendable conocer la mayor parte de los puntos anteriores en un plazo no superior a 12 horas, desde el momento en que se ha conocido el incidente.

En cualquier caso, y sin perjuicio de la gravedad del incidente y de otros factores, reducir los tiempos es fundamental, pero sin perder de vista que debe primar la obtención de información fiable y no meras hipótesis o suposiciones.

4.4. FASE DE EVALUACIÓN

Con la información recopilada se podrá iniciar el proceso de valoración del incidente, así como sus posibles consecuencias e impacto. Para ello es recomendable establecer las tareas a emprender, así como una planificación detallada para cada una de ellas.

Se debe considerar que al tratarse de una evaluación inicial **las tareas se diseñan en función de la información disponible,** que puede ser incompleta. Por otro lado, también hay que tener en cuenta la ventana de tiempo de respuesta disponible, puesto que se debe actuar conagilidad.

Dentro de las principales tareas que será necesario llevar a cabo se encuentran lassiguientes:

- Actuaciones para **cortar la filtración** y evitar nuevas fugas de información.
- Tareas de **revisión de la difusión** de la información **y mitigación** de la misma, en especial si ésta contiene datos de carácter personal o se trata de información confidencial.
- Tareas de **actuación con los afectados** por la fuga de información, ya sean internos o externos.
- Tareas para la **mitigación de las consecuencias legales:** posibles incumplimientos de normativa en materia de protección de datos de carácter personal o de otra normativa. También aquellas tareas encaminadas a la preparación de toda la información necesaria ante posibles denuncias por los afectados, otras organizaciones, etc.
- Tareas para la **determinación de las consecuencias económicas,** que puedan afectar a la organización y su posible mitigación.
- Tareas a acometer en los **activos de la organización afectados,** y su alcance, en relación con los activos de información, infraestructuras, personas, etc.
- Planificación del **contacto y coordinación con fuerzas y cuerpos de seguridad,** denuncia y otras actuaciones, en caso de ser necesario.
- Planificación de **comunicación e información del incidente,** tanto a nivel interno como externo, a medios de comunicación, y afectados, en caso de ser necesario.

Este conjunto básico de acciones compondrán el **plan de emergencia** diseñado para el incidente de fuga de información. Su ejecución deberá de estar completamente coordinada y supervisada en todo momento por el gabinete de crisis.

En función del escenario y los recursos de la organización, las acciones indicadas anteriormente podrán realizarse de forma simultánea o secuencial. En cualquier caso, establecer la prioridad de las tareas será responsabilidad del gabinete de crisis.

4.4. FASE DE MITIGACIÓN

Esta fase se centra en tratar de **reducir la brecha de seguridad y evitar que se produzcan nuevas fugas de información.** Por este motivo, en algunos casos puede ser necesario desconectar un determinado terminal, servicio o sistema de Internet. Ante esta situación debe primar el objetivo de mitigar la fuga de información en el menor tiempo posible. Más adelante se aplicarán medidas más adecuadas o menos drásticas que la desconexión, pero siempre garantizando la seguridad.

El siguiente paso se centrará en minimizar la difusión de la información sustraída, en especial si se encuentra publicada en Internet. Por este motivo, se contactará con los sitios que han publicado información, con los motores de búsqueda y se solicitará su retirada, en especial si se trata de información sensible o protegida por el secreto profesional o la LOPD.

Junto con el paso anterior, si se considera necesario, se llevará acabo la comunicación pertinente a los medios. Los medios de comunicación pueden aportar un mecanismo muy eficaz para hacer llegar tranquilidad a los afectados. Como se indicó anteriormente, debe de existir un único punto de contacto exterior desde la organización para evitar descoordinación.

En caso de existir personas afectadas por la fuga de información, por ejemplo, si se han filtrado datos personales de terceros, como de clientes nuestros, deberá seguirse el procedimiento de notificación y comunicación que contempla el Reglamento Europeo de Protección de Datos, así como seguir las indicaciones y protocolos que establezca el organismo de control español, en este caso la Agencia Española de Protección de Datos

También **se pondrá el incidente en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado** (Policía Nacional y Guardia Civil) o de la Fiscalía de cibercriminalidad informática, a través de la presentación de una denuncia y otras acciones que puedan derivarse de la coordinación o la solicitud de información por parte de las fuerzas y cuerpos de seguridad.

Hay que tener en cuenta, además, la necesidad de informar a otros organismos que puedan tener competencias en este tipo de incidentes, como es el caso de la Agencia Española de Protección de Datos, en el caso de datos de carácter personal, y el CERT de Seguridad e Industria (CERTSI) en cualquier otro caso.

4.6. FASE DE SEGUIMIENTO

Una vez completadas las principales acciones del plan, se procederá a **evaluar el resultado y la efectividad de las acciones realizadas**, en relación con las consecuencias y su impacto.

Además, en caso de ser necesario, se deberá hacer frente a otros aspectos que hayan podido generarse durante la fase de mitigación del incidente, como puedan ser consecuencias legales, económicas, reputacionales y similares.

Durante esta fase también se iniciará el proceso de estabilización de la situación generada por el incidente. Se comenzará con un proceso de valoración global del mismo, que supondrá una auditoría más completa a partir de la cual se puedan diseñar e implantar medidas definitivas para evitar nuevas fugas y restablecer el normal funcionamiento de los servicios e infraestructuras que pudieran haberse visto afectadas.