GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

GUÍA

GESTIÓN DE FUGA DE INFORMACIÓN

mayo 2012

ÍNDICE

1. INTRODUCCIÓN

Desde que Francis Bacon acuño la expresión “la información es poder” han pasado más de 400 años y sin embargo en el momento actual es cuando esta frase parece haber cobrado mayor sentido. La información se ha convertido en el activo más importante que posee cualquier organización, es moneda de cambio e instrumento de fuerza y presión, otorga ventaja a quien la posee, y hay toda una industria en torno a la gestión, tratamiento y por supuesto, protección de la información. Sin duda, vivimos en la «Sociedad de la Información».

En el año 2010 se produjo, la que está considerada hasta la fecha, como la mayor filtración de información de la historia. *Wikileaks*, una organización sin ánimo de lucro, publicó un total de 250.000 (cables) comunicaciones que se habían realizado entre el Departamento de Estado Estadounidense y sus embajadas repartidas por todo el mundo. Las consecuencias no se hicieron esperar.

Este incidente supuso la confirmación de algo que ya se sabía: la gran dificultad de mantener la confidencialidad de la información, evitando filtraciones, pero también puso de manifiesto que **ninguna organización está a salvo**, incluidas aquellas que pertenecen al ámbito gubernamental o dedicadas a alguna de las múltiples ramas o ámbitos de la seguridad, que lógicamente se suponen preparadas, ya que disponen de procedimientos, herramientas y personal entrenado para manejar información considerada sensible y confidencial. Pero, como ha quedado demostrado, la seguridad 100% no existe y en última instancia, la información es manipulada por personas, y como se suele decir en seguridad «el usuario es el eslabón más débil de la cadena».

Wikileaks es un ejemplo perfecto de cómo una fuga de información puede tener consecuencias imprevisibles y un enorme impacto mediático, tal y como ocurrió en este caso, debido a la naturaleza de la información filtrada y el ámbito al que pertenecía. El daño fue tremendo, y puso en jaque al gobierno americano que tuvo que realizar importantes esfuerzos para minimizar el impacto y las consecuencias.

Aunque el incidente de *Wikileaks* estableció un antes y un después, el problema de la fuga de información existe desde que los humanos manejan información. **La fuga de información tiene una componente social y humana muy importante**. Detrás de una buena parte de los incidentes de fuga de información se esconden motivaciones personales, o simples errores, entre otras.

La masificación del uso de las tecnologías y su integración en todos los ámbitos y estamentos de la sociedad han creado un escenario en el que por un lado, cada vez se gestiona mayor cantidad de información y por otro, se ha convertido en un activo crítico de las organizaciones y los usuarios. Además las tecnologías posibilitan un tratamiento de la información sin precedentes y a nivel global, de manera que es transmitida, procesada, copiada o almacenada con una rapidez y eficacia impensable hace algunos años, sumado al hecho de que es posible llevar a cabo dichas acciones, desde múltiples tipos de dispositivos, en cualquier lugar y en cualquier momento.

La computación en la nube o los dispositivos móviles son una de las últimas expresiones de la tecnología que están potenciando una propiedad de la información, que ha convertido en un autentico reto mantener la su confidencialidad: **la ubicuidad**.

Es precisamente esta propiedad la que entraña los mayores riesgos para la confidencialidad de la información, ya que hace **más difícil definir límites geográficos, físicos o lógicos del ámbito de utilización y protección de la información**. Por otro lado, el valor que ha tomado la información como arma de desprestigio, herramienta de presión o elemento de valor que se comercializa y vende a escala global en todo tipo de ámbitos y sectores, están convirtiendo a la fuga de información en uno de las mayores amenazas para la seguridad, puesto que detrás de este tipo de incidentes se sitúan motivaciones muy poderosas, como el beneficio económico o el daño de imagen.

En la actualidad la industria de seguridad ofrece un buen número de soluciones de seguridad en forma de productos y servicios, entre los que destacan aquellos destinados a la gestión del ciclo de vida de la información (ILM) o los que están destinados específicamente a evitar la fuga de información (DLP). La prevención de la fuga de información es un negocio en auge.

Por desgracia en este tipo de incidentes la prevención no es suficiente, puesto que las consecuencias de la fuga de información pueden ser muy negativas y con un elevado nivel de dispersión, pudiendo afectar a otras organizaciones o incluso usuarios. Las organizaciones se suelen centrar en exceso en la prevención, dejando a un lado la gestión del incidente. Esto supone que en caso que finalmente se produzca la fuga de información, no se toman las decisiones adecuadas o no se dispone de un procedimiento básico que sirva de guía y que permita minimizar adecuadamente el impacto y evitar un empeoramiento de la situación.

Teniendo en cuenta lo anterior, desde INTECO-CERT hemos querido dedicar una guía a la gestión de la fuga de información desde el punto de vista de la gestión del incidente, es decir, cuando ya se ha producido y hay que gestionar las posibles consecuencias.

A través de esta guía básica esperamos ofrecer información de utilidad a las organizaciones y las empresas, de manera que puedan tomar las mejores decisiones, con el objetivo de minimizar las consecuencias y el impacto de un incidente de fuga de información sobre la organización y sobre otros actores externos.

2. EL PROBLEMA

2.1. INTRODUCCIÓN

La protección de la información hace referencia a la protección de tres propiedades principales: confidencialidad, integridad y disponibilidad. La fuga de información es la pérdida de la primera, es decir, la pérdida de la confidencialidad, de forma que: información que a priori no debería de ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, termina siendo visible o accesible para otros.

Como cualquier otro incidente de seguridad, la fuga de información tiene un origen y unas causas principales. Por otro lado, si el incidente finalmente tiene éxito, tendrá consecuencias que afectarán por un lado a la propia organización, pero también podrán tener impacto sobre grupos externos de usuarios y otras organizaciones.

El impacto y las consecuencias posteriores a un incidente de fuga de información, es uno de los aspectos que mayor preocupación despierta en las organizaciones, puesto que la filtración de información puede dañar su imagen pública y en el caso de las empresas, puede suponer un impacto negativo para el negocio, además de generar desconfianza e inseguridad en el público en general y generar otras consecuencias a terceros, como en el caso de que la información filtrada haga referencia a usuarios o clientes.

Por otro lado, la fuga de información es un tipo de incidente difícil de ocultar, puesto que su propia naturaleza y las motivaciones que se sitúan detrás de estos incidentes suelen terminar en muchas ocasiones con la difusión del suceso en Internet. La enorme velocidad a la que se propaga la información en la Red y la gran cantidad de medios disponibles para llevar a cabo dicha propagación, son factores que no ayudan a la hora de contener una posible filtración.

Además de los problemas más evidentes derivados de la fuga de información, hay otras consecuencias que pueden tener un impacto significativo, incluso a nivel económico. Actualmente existen un conjunto de normativas que ponen especial énfasis en el uso y tratamiento de datos de carácter personal por parte de las organizaciones, las empresas y los ciudadanos. Dichas normativas prevén sanciones tanto de tipo económico, si se trata de empresas, como de tipo administrativo, para las administraciones, en caso que el tratamiento de los datos no se ajuste a la ley, y en este supuesto entran las fugas de datos, ya que en muchas ocasiones, estos incidentes terminan con la difusión o publicación de datos de carácter personal.

Precisamente el temor a las posibles sanciones, es en ocasiones, uno de los principales motivos para la ocultación de un incidente. 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 si se hace público, a quién se debe de informar y en qué orden, así como otros aspectos relativos a la comunicación del suceso a los medios.

2.2. ORIGEN Y MOTIVACIÓN

En los primeros años de la informática, la fuga de información se relacionaba principalmente con los accesos no autorizados de origen externo, a sistemas u ordenadores, implicando, en ocasiones, la sustracción o el robo de información, pero las consecuencias por aquel entonces eran muy limitadas si las comparamos con el impacto que puede llegar a tener hoy día.

Con el tiempo, las amenazas evolucionaron y también cambiaron algunos paradigmas de la seguridad. La frase «el enemigo está dentro» se popularizó hace ya unos años cuando los incidentes de seguridad cuyo origen estaba en el interior de las propias organizaciones comenzaron a aumentar. Dicho aumento cambió la percepción y el concepto de protección, puesto que hasta entonces las medidas de seguridad se centraban en crear barreras para proteger a las organizaciones de las amenazas externas.

Actualmente, el origen de las amenazas puede ser tanto externo como interno. En el caso del origen interno, el empleado, se ha convertido en uno de los principales focos de todo tipo de incidentes de seguridad. El descontento, la venta de secretos industriales o información privilegiada para la obtención de beneficio económico, la venganza, el daño a la imagen, o la creación de una nueva empresa con parte de los activos de información de otra, son algunos de los principales motivos detrás de una buena parte de los incidentes de seguridad de fuga de información. Pero no todos los incidentes de este tipo tienen una motivación específica. En ocasiones, también están relacionados con la falta de conocimiento, formación o sencillamente errores.

Desde el punto de vista externo del origen de la fuga de información, el mapa de las amenazas externas ha cambiado enormemente en la última década, con la aparición de nuevos jugadores en el escenario de la seguridad: organizaciones criminales, activistas o terroristas, han tomado Internet y la han convertido en un verdadero campo de batalla, en el que se desarrollan todo tipo de estrategias con diversos objetivos, como conseguir beneficio económico, llevar a cabo acciones de protesta y daño de imagen, o sabotajes a instalaciones industriales.

2.3. CAUSAS

En cualquier incidente de seguridad siempre existen elementos o mecanismos que hacen posible, facilitan y ayudan al éxito de un incidente de seguridad. Las causas en relación con la fuga de información pueden ser clasificadas en dos grupos principales, por un lado aquellas que pertenecen al **ámbito organizativo** y por otro, aquellas que hacen referencia a **al ámbito técnico**.

La mayoría de las causas, organizativas o técnicas, por lo general, implican la ausencia de algún tipo de medida de seguridad, procedimiento, herramienta, etc. La ausencia supone la falta de control y esta aumenta de forma significativa la probabilidad de que se produzca un incidente de fuga de información.

2.3.1. Causas organizativas

Una gestión deficiente, la falta de formación y buenas prácticas, la ausencia de políticas y procedimientos o la no aplicación de mecanismos de disuasión, son causas habituales y suficientes para facilitar o desencadenar un incidente de fuga de información.

Uno de los primeros errores que se comete en relación con la protección de la información es la falta de una clasificación de la información en base a su nivel de confidencialidad, en función de diversos parámetros, como son el valor que tiene para la organización, el impacto público que puede generar su difusión, 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 y seleccionar las medidas de protección adecuadas. Por otro lado, el ámbito de difusión, permite establecer el perímetro dentro del cual podrá ser difundida la información y junto con el nivel de confidencialidad, hará posible determinar quien debe de conocer la información y qué tipo de acciones puede realizar sobre esta.

Los errores o la falta de conocimiento y formación son otra de las causas más comunes de la fuga de información. Por un lado, el empleado debe utilizar los recursos que la organización pone a su disposición de forma responsable, como en el caso del uso del correo electrónico, la navegación Web u otros servicios y por otro lado, debe disponer de ciertos conocimientos y formación en relación con su actividad diaria, siendo responsabilidad de la organización proporcionar la información y la formación necesaria de manera que el empleado pueda desempeñar su función adecuadamente.

Además de las buenas prácticas y la formación es necesario contar con procedimientos y establecer el conjunto de pautas y obligaciones para los trabajadores en el ámbito de la seguridad, mediante el establecimiento de políticas que indiquen 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, de manera que se sigua un proceso controlado y las tareas se realicen de la forma más segura posible.

Además de la formación, las buenas prácticas y las políticas, es necesario ir un paso más allá, con el objetivo de incorporar un **nivel adicional de disuasión**, a la hora de evitar prácticas indebidas o actividades malintencionadas dentro de las organizaciones.

En este sentido, cada vez es más habitual que durante el proceso de contratación de un empleado, se solicite por escrito la conformidad con diversas normas internas, como la política de confidencialidad o de seguridad, entre otras, de manera que el futuro empleado, deja por escrito la aceptación de las condiciones correspondientes.

No es lo mismo leer un documento, que leerlo y posteriormente firmarlo. El sentido y las consecuencias en ambos casos son muy distintos. Por otro lado, hoy día, las empresas y las organizaciones cuentan con legislación que les permite establecer límites legales a las actividades de sus trabajadores y que pueden ser utilizadas como mecanismos de disuasión para evitar un uso malintencionado de los recursos y la información.

La disuasión es una herramienta muy potente si se utiliza adecuadamente y en el contexto correcto, informando a los trabajadores, pero sobre todo, dejando claro que la organización ha establecido medidas para prevenir, y en caso de que suceda un incidente, tomar la iniciativa poniendo en marcha las acciones correspondientes.

2.3.2. Causas técnicas

El código malicioso o malware, se ha convertido en una de las principales amenazas, siendo uno de sus objetivos más comunes el robo de información. La revolución de las tecnologías móviles y el aumento de los trámites y transacciones on-line, han venido acompañadas de un importante incremento del código malicioso y de su peligrosidad, debido a que en su mayoría, está destinado al fraude y a la obtención de beneficio económico.

Uno de los mayores peligros del código malicioso, es que permite automatizar una buena parte del proceso relacionado con la fuga de información y además, el diseño de muchos de estos programas, incluye técnicas que permiten mantener oculto el código en un sistema, mientras recoge y envía información.

El acceso no autorizado a sistemas e infraestructuras es otra de las causas detrás del robo de información. Ya sea como parte de una campaña de desprestigio, con el acceso no autorizado a una página web de una organización con cierta relevancia pública, o con motivo de sustraer información sobre secretos industriales, los accesos no autorizados han vuelto a la palestra de los incidentes de seguridad más peligrosos y están mostrando el deficiente nivel de seguridad que tienen muchas aplicaciones y portales Web en Internet.

En relación con lo anterior es importante indicar que los sistemas y aplicaciones precisan de actualizaciones y revisiones constantes. Hace años, muy pocas aplicaciones eran actualizadas regularmente, incluidos los sistemas operativos. Hoy día, cualquier aplicación, dispone de actualizaciones regulares y **contar con un servicio de actualizaciones se considera parte fundamental de una buena aplicación**, puesto que aporta mayor seguridad y denota un trabajo de mejora continua, que redunda en beneficio para la aplicación y por extensión, para el usuario.

En la práctica es difícil separar las causas organizativas y técnicas, puesto que cada vez están más relacionadas, debido al uso intensivo de las tecnologías de la información dentro de las organizaciones para cualquier actividad, incluida la gestión de la seguridad, pero aún así, es importante diferenciarlas, de cara a diseñar medias y detectar vulnerabilidades y mejoras.

3. LAS CONSECUENCIAS

3.1. ESCENARIOS

Las consecuencias de un incidente de fuga de información preocupan enormemente a las empresas y las organizaciones. Un incidente que se hace público, puede causar un importante daño de imagen o mermar la confianza de los clientes de la entidad, lo que puede llegar a afectar a su negocio.

Comprender las posibles consecuencias es un aspecto esencial y necesario para la gestión de incidentes de fuga de información. A través del estudio de las posibles consecuencias, es posible diseñar una estrategia, de forma que en caso que finalmente se produzca un incidente de fuga de información, sea posible tomar las decisiones adecuadamente, minimizando el impacto, ya sea sobre la propia organización o incluso sobre terceros, ya sean clientes, usuarios o sobre otras organizaciones.

Para comprender algunas de las consecuencias de un incidente de fuga de información, vamos a describir distintos escenarios que están basados en incidentes reales, de los cuales se ha suprimido información que no es relevante para al propósito del apartado.

Tomemos como primer escenario: el caso de una entidad bancaria que sufrió una fuga de información que supuso la filtración de datos de sus clientes, que incluían números de cuentas bancarias y otra información. El origen de la filtración parece ser que fue interno, a través de un empleado de la propia entidad.

Es evidente que la imagen pública de la entidad quedo dañada y su credibilidad afectada, pero también hubo consecuencias externas, ya que se vieron expuestos datos de clientes, que una vez conocieron la filtración, pudieron tomar acciones legales contra la propia entidad, a tenor, de la ley de protección de datos personales que aplique en aquel país o de otra legislación.

Por otro lado, el impacto de la información revelada, en el caso de los clientes afectados tuvo otras consecuencias derivadas de la revelación de cuentas no declaradas, lo que originó una posterior investigación por las autoridades fiscales correspondientes, ante la posible evasión de impuestos.

Un prototipo de un conocido dispositivo de un importante fabricante de tecnología apareció en un bar y posteriormente fue vendido a un portal especializado en noticias de tecnología. El origen del incidente parece ser que fue interno, un empleado dejó olvidado el prototipo en el establecimiento.

En este caso, el impacto es completamente distinto al caso anterior, e incluso, la aparición de este supuesto prototipo pudo generar más expectativas en los posibles compradores del producto final, pero en cualquier caso, la filtración proporcionó información sensible a sus competidores, que pudieron utilizarla en su beneficio, antes de que el producto definitivo saliera al mercado.

Aparecen en la basura miles de informes médicos, que al parecer provenían de un centro de salud. El origen de la fuga parece ser que fue interno.

Afortunadamente, alguien los encontró y pasaron a estar custodiados. España cuenta con una legislación relativa a protección de datos, conocida como Ley Orgánica de Protección de Datos (LOPD) y una agencia, la Agencia Española de Protección de Datos encargada de velar por el cumplimiento de esta. Debido a la gravedad del caso, y tratándose de datos de carácter personal que además contenían datos médicos, la Agencia Española de Protección de Datos, junto con los cuerpos y fuerzas de seguridad correspondiente, así como los organismos con competencias, llevaron a cabo una investigación.

Las consecuencias en este caso son de carácter fundamentalmente legal, ya que este tipo de incidentes suele conllevar sanciones y por supuesto, otras actuaciones a nivel interno en la propia entidad. En este sentido hay que aclarar, que no es lo mismo que se trate de una entidad pública o privada, puesto que el impacto económico debido a una posible sanción es bien distinto, además de otras consecuencias, como la imagen pública, que tendrán un impacto muy diferente en cada caso.

A diferencia del incidente anteriormente comentado, relativo a la entidad bancaria, los datos de los expedientes no fueron difundidos, lo que limita de forma importante las posibles consecuencias. Si no hay afectados por la revelación de la información, no deberían, a priori producirse otras consecuencias, como denuncias por parte de los afectados.

Un grupo activista, filtro datos personales relativos al director de una organización gubernamental estadounidense y su familia, como medida de represalia por el cierre de un portal de descargas en Internet. En este caso, la fuga se originó en el exterior.

En este caso nos encontramos ante un incidente de fuga de información muy distinto a los anteriores, puesto que aunque se filtran dato personales, van dirigidos a una persona y su familia, no a un colectivo de usuarios. Por otro lado, la motivación parece ser la venganza, dirigida no contra la entidad sino contra una persona de la misma, en este caso el director. Las consecuencias afectan sobre todo a la persona de la cual se filtraron los datos.

Además en este escenario, el incidente se produjo en un país que no cuenta con una normativa de protección de datos de carácter personal como ocurre en España y en la Unión Europea. Lógicamente se producirá una investigación para determinar donde se produjo la brecha de seguridad, pero posiblemente no haya consecuencias legales de ningún tipo, salvo que consigan identificar a los culpables.

Una plataforma de juegos on-line sufre un robo de datos personales que incluye datos bancarios. La fuga se produce varias veces, ante la aparente dificultad de cerrar la brecha de seguridad. Se ven afectados usuarios de todas partes del mundo.

Nos encontramos ante un caso particular, por un lado se trata de un robo de datos personales, que incluye información bancaria. Esto supone un importante riesgo para los usuarios. Por otro lado, afecta a usuarios a nivel global, es decir, de distintos países. Hasta aquí no es muy distinto de otros incidentes de fuga de información, pero en este caso se da

una situación que es importante destacar, puesto que la plataforma es atacada en varias ocasiones y se producen varios accesos no autorizados, lo que termina dañando gravemente la imagen de la compañía que la gestiona, ante la aparente imposibilidad de contener o cerrar la brecha de seguridad.

La magnitud del robo de datos fue considerable y el impacto mediático muy importante. Por otro lado, tuvo consecuencias tanto a nivel económico, como legales, ya fuera por denuncias relativas a una posible negligencia por parte de la compañía, debido a la gestión del incidente.

Una agencia gubernamental del ámbito de la seguridad nacional, sufre un acceso no autorizado que tiene como consecuencia la sustracción de cientos de documentos confidenciales. Debido al nivel de confidencialidad de los datos sustraídos, la fuga es considerada muy grave.

Tal y como se ha comentado antes, las consecuencias de una fuga de datos de una organización que pertenezca a la administración son muy distintas de aquellas que pueden afectar a una empresa. Tomando el caso que se ha descrito arriba, las consecuencias en este caso, son todavía más distintas si cabe, en sentido que se trata de una organización gubernamental y perteneciente al ámbito de la seguridad nacional.

Las consecuencias en este caso tienen un impacto a otros niveles completamente distintos, ya que se trataría de una fuga de información que podría afectar a la seguridad nacional de una nación. Las consecuencias de un incidente de este tipo tendrían que ver con el daño de imagen y credibilidad de la organización afectada, pero las causas más importantes serían de tipo externo a la organización, por ejemplo, si se ha sustraído información relativa a infraestructuras críticas o sistemas de defensa.

Los casos que se han descrito dan una idea muy general de las posibles consecuencias que puede llegar a tener un incidente de fuga de información, ya sea sobre la propia organización en la cual se ha producido la fuga, o incluso sobre las personas u otras organizaciones o ámbitos.

Lo cierto es que determinar las posibles 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, los cuales servirán de base de cara a establecer las consecuencias y el posible nivel de impacto.

3.2. ESTIMACIÓN DEL IMPACTO

Se entiende por impacto el conjunto de las consecuencias que se derivan de un incidente, en el ámbito que nos ocupa, de un incidente de fuga de información. A partir de los ejemplos vistos en el apartado anterior queda patente la gran diversidad de escenarios posibles y lo distintas que pueden ser las consecuencias, que podríamos separar en varias categorías principales:

- **Daño de imagen**. Son aquellas consecuencias que generan impacto negativo en la imagen de la compañía o de la organización y que además generan pérdida de confianza.
- **Consecuencias legales**. Son aquellas consecuencias que se enmarcan en el ámbito legal, que podrían conllevar sanciones económicas o administrativas.
- **Consecuencias económicas**. Son aquellas que afectan o suponen un impacto negativo a nivel económico, en forma de sanciones, disminución de la inversión, negocio, etc.
- **Otras consecuencias**. Son aquellas que afectan o supone un impacto negativo en ámbitos muy diversos, como por ejemplo, el ámbito político, diplomático, institucional, o gubernamental, entre otros. En general se trata de consecuencias que no están englobadas en los otros tres tipos.

En realidad es difícil separar las consecuencias anteriores, puesto que en la mayoría de los casos están íntimamente relacionadas y por otro lado, es difícil que se den consecuencias de un único tipo para un incidente. Por lo general, las consecuencias suelen ser una combinación de las anteriores, cada una con un peso distinto en función del escenario.

Dicho escenario estará definido por un conjunto de factores que en parte, determinarán el peso final que tendrán las consecuencias y en su conjunto, determinarán el impacto global del incidente sobre la organización y su entorno.

Uno de los factores que definen el escenario es el tipo de organización en la cual se ha producido la fuga de información, es decir, si se trata de una organización que pertenece a la administración o si se trata de una empresa o una organización privada. Analizando las consecuencias, se puede establecer que el peso de las distintas consecuencias (legales, económicas o de imagen) es muy distinto en cada caso:

- **Organizaciones del sector público**. En el caso de las organizaciones pertenecientes a la administración, el posible daño e imagen es un factor que cobra importancia desde un punto de vista político o gubernamental. Las consecuencias económicas, como las sanciones debidas a incumplimiento de la legislación, son ciertamente limitadas, por ejemplo, en el caso de una fuga de información de datos de carácter personal, las sanciones a las organizaciones pertenecientes a la administración (como norma general), no son de tipo económico, aunque sí que es

cierto que se podrían producir casos en los cuales, los afectados denunciarán (proceso ordinario) y finalmente se estableciera algún tipo de indemnización.

- **Organizaciones del sector privado**. Es evidente que las organizaciones que pertenecen al sector privado están mucho más ligadas a posibles efectos o consecuencias de carácter económico. A diferencia de las administraciones, el sector privado si está expuesto a sanciones económicas. Por otro lado, un incidente puede suponer la pérdida de confianza de los inversores o de sus clientes, lo que también puede tener consecuencias muy significativas sobre su negocio y su actividad.

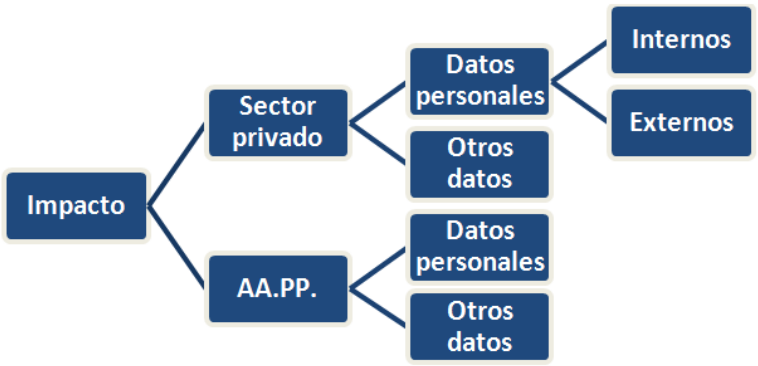
Otro de los factores que tienen especial importancia en un escenario de fuga de información, es la naturaleza de la información, en especial, la tipología de los datos sustraídos o filtrados. En este sentido, podemos establecer una clasificación muy sencilla, diferenciando entre:

- **Datos de carácter personal**. Aquellos datos relativos a terceros físicos y que permiten identificar a una persona, ya sea de forma directa o indirecta (…). Los datos de carácter personal son muy amplios, pero en cualquier caso, lo fundamental es que hacen referencia a ciudadanos y son considerados “sensibles”. Su divulgación o difusión, pueden conllevar sanciones para la organización que ha sufrido el incidente.
- **Otros datos**. Serán aquellos que no son datos de carácter personal, generalmente relacionados con terceros jurídico, información técnica u operativa.

Además de diferenciar entre información que contiene datos de carácter personal o no, también es importante establecer si dicha información hace referencia al interior o al exterior de la organización. Hay que tener en cuenta que no es lo mismo que se filtren datos de personas u organizaciones externas a la organización, como por ejemplo datos de clientes, a que se filtren datos de los propios trabajadores. Las consecuencias pueden ser muy distintas. Por tanto, además de la clasificación anterior tenemos también:

- **Datos internos**. Son aquellos datos relativos que proporcionan o hacen referencia a la propia organización.
- **Datos externos**. Son aquellos datos relativos o que proporcionan información sobre organizaciones o personas externas a la organización.

Como vemos, a medida que incluimos más factores, la valoración del impacto se complica, pero en base a los tres factores anteriores es posible desarrollar una aproximación que ayude a determinar las posibles consecuencias de un incidente. A continuación podemos ver un diagrama que resume los tres factores comentados.



Además de lo anterior, obtener una escala de valores en relación con las consecuencias, requiere contar con una valoración objetiva en el ámbito de la organización de los distintos factores comentados y de otros, en relación con sus consecuencias, siguiendo un procedimiento similar a las encuestas utilizadas en la evaluación de riesgos, puesto que para cada organización, las posible consecuencias y el impacto dependerán también de la valoración que realicen las personas de dicha organización, que conocen su entorno y actividad.

Por otro lado, a partir del árbol de factores que se ha mostrado, calcular el nivel de impacto, requiere considerar los factores de manera que sean dependientes unos de otros, es decir, no es lo mismo una empresa privada que pierde datos de carácter personal pertenecientes a sus propios empleados, que una empresa privada que pierde otro tipo de datos pertenecientes a organizaciones externas. Como vemos, el cálculo es el resultado de varios factores interdependientes.

En relación con lo anterior, no es objeto de este documento desarrollar un método de cálculo del impacto, sino mostrar algunos de los factores que pueden influir de forma decisiva en el valor final que pueda tener ese impacto sobre la organización.

Como vamos a ver en el apartado siguiente, los factores indicados, además de otras consideraciones, servirán para diseñar una hoja de ruta de gestión del incidente de fuga de información.

4. GESTIÓN DE LA FUGA DE INFORMACIÓN

Dada la naturaleza de los incidentes de fuga de información y las consecuencias que pueden derivarse, la gestión de un incidente cobra especial importancia con el objetivo de minimizar las consecuencias y el impacto sobre la organización.

A priori, la gestión del incidente puede parecer una tarea sencilla, pero hay que tener en cuenta muchos aspectos y situaciones, que de no ser gestionadas adecuadamente, pueden suponer un efecto contrario al deseado, es decir, **se puede magnificar el efecto negativo del incidente**, dando lugar a consecuencias no esperadas o efectos colaterales, que den como resultado un empeoramiento del impacto global sobre la organización.

A lo largo del siguiente apartado desarrollaremos una propuesta de hoja de ruta para la gestión de los incidentes de fuga de información, recogiendo los principales puntos y aspectos a tener en cuenta. **La hoja de ruta propuesta es únicamente una guía, que deberá de ser adaptada al escenario específico.**

4.1. HOJA DE RUTA

4.1.1. Los primeros momentos

Los momentos inmediatamente posteriores a un incidente de fuga de información son especialmente críticos y la adecuada gestión de esos primeros momentos puede suponer una reducción considerable del impacto. El problema es que **en muchas ocasiones el incidente no es detectado hasta que este llega a los medios de comunicación o se produce su difusión en Internet**, es decir, la organización afectada conoce la existencia del incidente a través de fuentes externas.

En relación con lo anterior, uno de los mayores retos a los que se enfrentan las organizaciones es conseguir la **detección temprana del incidente**, si es posible, a través de medios internos, de forma que la organización tome el control de la situación en el menor tiempo, iniciando el protocolo de actuación correspondiente.

Precisamente, debido a la posibilidad de que el incidente no sea detectado internamente y sea conocido a través de fuentes externas, es importante que la organización se mantenga informada, de manera que sea posible detectar la publicación de cualquier información o contenido que afecte a la organización y que esté relacionada con el incidente, lo antes posible.

4.1.2. Gabinete de crisis e inicio de la gestión del incidente

Una vez que se conoce la existencia del incidente, ya sea a través de fuentes externas o internas, **el primer paso es iniciar el protocolo interno de gestión del incidente,** convocando a los responsables que forman parte del equipo de gestión que deben tomar las decisiones: **el gabinete de crisis**. Mantener la calma y actuar con organización es

fundamental para evitar decisiones incorrectas o que pueden provocar consecuencias negativas adicionales, ya sea a nivel interno o externo.

Evidentemente no todas las organizaciones cuentan con un gabinete de crisis o tienen los recursos necesarios para abordar la gestión del incidente tal y como lo haría una gran organización o una gran empresa. Cada organización deberá de ajustarse a sus recursos, pero en cualquier caso, será necesario contar como mínimo con un responsable que se encargara de la gestión y coordinación de la situación, ya sea personal propio de la organización o externo.

En cualquier caso, todas las decisiones y las actuaciones relativas al incidente deberán de ser tomadas y coordinadas por el gabinete de crisis. Es fundamental evitar actuaciones por libre o que no hayan sido definidas y acordadas por el gabinete.

4.1.3. Auditoría interna y externa

Una vez se inicia el protocolo de actuación, se pone en marcha el gabinete de crisis y se informa a todos sus miembros, debería de dar comienzo la fase de obtención de información sobre el incidente. Para ello, será necesario iniciar por un lado, una auditoría interna, con el objetivo de **determinar con exactitud y en el mínimo tiempo posible** lo siguiente:

- **Determinar la cantidad (tamaño en disco, número de registros, etc) de información ha podido ser sustraída**. Hay que indicar que la información sustraída puede ser mayor que la información que finalmente ha resultado filtrada y hecha pública, en el caso que se haya difundido, por ejemplo, a través de Internet.
- **Establecer el tipo de datos que contiene la información que ha podido ser sustraída**, en especial si incluye datos de carácter personal y cual es su nivel.
- **Determinar si la información es relativa a la propia organización o es externa,** es decir, si por el contrario se trata de información que hace referencia a organizaciones o personas externas a la organización.
- **Establecer la causa principal de la filtración,** si tiene un origen técnico, o humano. Si el origen es técnico, determinar los sistemas que están afectados o en los cuales se ha producido la brecha. Si es humano, iniciar el proceso para identificar como se ha producido la fuga y quien es el responsable.

Además de la auditoría interna, también realizar una auditoría externa, en el sentido de conocer el tamaño, gravedad y nivel de difusión de la filtración en el exterior de la organización. En este punto, hay que distinguir entre información que ha sido sustraída e información que se ha hecho pública, ya que no son necesariamente lo mismo. En relación con lo anterior, será necesario conocer, al menos los siguientes puntos:

- **Determinar donde se ha hecho pública la información sustraída**. Este primer punto es fundamental. Como veremos, en el siguiente paso de la hoja de ruta, es crítico cerrar la brecha de seguridad y cortar la difusión de la información sustraída, para lo cual es necesario conocer donde se ha publicado o donde está disponible.

- **Establecer qué información se ha hecho pública** y determinar la cantidad (tamaño en disco, número de registros, etc) de la información filtrada.
- **Recoger las noticias y otros contenidos** que hayan aparecido en los medios de comunicación, así como en otros medios en Internet.
- **Conocer las reacciones** que se están produciendo en relación con el incidente.

En esta fase, el tiempo de reacción es crítico y sería recomendable conocer todos los datos anteriores y otros que puedan ser recopilados durante la auditoria o que resulten de interés, en un **plazo no superior a 12 horas**, desde el momento en que se ha conocido el incidente. En este sentido, reducir los tiempos es fundamental, pero también hay que proporcionar el margen suficiente para que el personal encargado de la auditoria pueda trabajar y obtener información fiable y no meras hipótesis o suposiciones.

El tiempo que hemos indicado es orientativo, en cualquier caso, más allá de las 48 horas podría considerarse excesivo, aunque dependerá de la gravedad del incidente y de otros factores.

4.1.4. Evaluación inicial y toma de decisiones

Con la información obtenida se inicia el proceso de valoración del incidente, posibles consecuencias e impacto. Se establecen las principales acciones y se detalla la planificación para cada una de ellas. Hay que indicar que al tratarse de una evaluación inicial, las acciones serán diseñadas y planificadas en función de la información disponible, que puede ser incompleta. Por otro lado, también hay que tener en cuenta la ventana de tiempo disponible, puesto que hay que actuar con la mayor celeridad posible.

En relación con las principales acciones (entre otras) que será necesario llevar a cabo, se indican las siguientes:

- **Determinación de las acciones destinadas a cerrar la filtración** y evitar nuevas fugas de información.
- **Determinación del nivel de difusión de la información** y de las acciones destinadas a minimizar su difusión, en especial si esta contiene datos de carácter personal o se trata de información sensible.
- **Determinación de los afectados por la fuga de información**, ya sean internos o externos.
- **Determinación de las consecuencias legales**, posibles incumplimientos de normativa en materia de protección de datos de carácter personal, o de otra normativa, así como posibles denuncias por los afectados, otras organizaciones, etc.
- **Determinación de las consecuencias económicas**, que puedan afectar a la organización.
- **Determinación de los activos de la organización afectados,** y 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.

Estas acciones y otras que puedan considerarse necesarias, en función del escenario, compondrán el plan de emergencia diseñado para el incidente en cuestión. Su ejecución deberá de estar completamente coordinada y supervisada en todo momento por el gabinete de crisis.

Las acciones indicadas anteriormente, podrán realizarse de forma simultánea o secuencialmente, todo dependerá del escenario, los recursos con que cuente la organización y de otras consideraciones. En cualquier caso, el orden y la coordinación de las acciones será responsabilidad del gabinete de crisis.

Una vez realizada la evaluación inicial y determinadas las acciones y establecidas las prioridades, se inicia el proceso de gestión de contención y control del incidente.

4.1.5. Ejecución del plan de contención y control

Dentro del plan, el primer paso es **terminar con la brecha de seguridad y evitar que se produzcan nuevas fugas de información**. Es posible que sea necesario cerrar la brecha de seguridad a costa por ejemplo, de desconectar un determinado servicio o sistema de Internet, pero **cerrar la fuga es el objetivo número uno**. Más adelante, se llevará a cabo la aplicación de medidas más adecuadas o menos drásticas, pero siempre garantizando la seguridad.

Además de cerrar la brecha de seguridad, es crítico eliminar o minimizar la filtración de la información sustraída, en especial en Internet. Por ejemplo, es habitual que información sustraída o filtrada sea publicada y difundida en diversos sitios web o portales. Se procederá a contactar con los sitios que han publicado información y se solicitará su retirada, en especial si se trata de información sensible.

En caso de ser necesario, se llevará a cabo la comunicación pertinente a los medios, para informar a la opinión pública del incidente, pero tal y como se ha indicado, **únicamente en caso que se considere necesario**. Los medios de comunicación pueden aportar un mecanismo muy eficaz para hacer llegar tranquilidad a los afectados. La coordinación en relación con los medios de comunicación durante la gestión del incidente es un aspecto crítico.

Además, tal y como se ha indicado, en caso de existir afectados por la fuga de información, por ejemplo, si se han filtrado datos de terceros, como clientes o usuarios de un servicio, es fundamental que sean informados, no solo del incidente, sino también de los datos que han sido sustraídos, para que puedan tomar las acciones oportunas para su seguridad, como puede ser el cambio de contraseñas, revocación de números de tarjetas, etc.

Así mismo, es importante no solo informar de lo sucedido, sino proporcionar algún canal o medio de comunicación, de manera 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 caso de ser necesario se comunicará el incidente a las fuerzas y cuerpos de seguridad, ya sean locales, regionales o nacionales, en función del escenario. Por otro lado se llevará a cabo la denuncia del incidente y otras acciones que puedan derivarse de la coordinación o la solicitud de información por parte de las fuerzas y cuerpos de seguridad.

Además, se tendrá en cuenta informar a otros organismos que puedan tener competencias derivadas de la información filtrada, como es el caso de la Agencia Española de Protección de Datos, en el caso de datos de carácter personal.

4.1.6. Seguimiento, estabilización y otras consecuencias

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 el impacto. Por otro lado, durante esta fase, en caso de ser necesario, se deberá de hacer frente a otras consecuencias que hayan podido generarse durante la fase de contención del incidente, como puedan ser consecuencias legales, económicas, etc.

Durante esta fase también se iniciará el proceso de estabilización del incidente, comenzando un proceso de valoración global del mismo, que supondrá una auditoría más completa a partir de la cual se diseñaran e implantaran las medidas definitivas para evitar nuevas fugas y restablecer el normal funcionamiento de los servicios e infraestructuras que pudieran haberse visto afectadas.

4.2. TABLA RESUMEN

A continuación resumimos la hoja de ruta descrita en el apartado anterior en la tabla resumen que aparece a continuación:

FASE	DESCRIPCION
FASE INICIAL	○ Detección del incidente ○ Alerta del incidente a nivel interno ○ Inicio del protocolo de gestión
FASE DE LANZAMIENTO	○ Reunión del gabinete de crisis ○ Informe inicial de situación ○ Coordinación y primeras acciones
FASE DE AUDITORÍA	○ Auditoría interna y externa ○ Elaboración de informe preliminar
FASE DE EVALUACIÓN	○ Reunión del gabinete de crisis ○ Presentación del informe de auditoría ○ Determinación de principales acciones ○ Tareas y planificación
FASE DE CONTENCIÓN	○ Ejecución de todas las acciones del plan
FASE DE SEGUIMIENTO Y ESTABILIZACIÓN	○ Valoración de los resultados del plan ○ Gestión de otras consecuencias ○ Auditoría completa ○ Aplicación de medidas y mejoras ○ Restablecimiento de la actividad

5. PREVENCIÓN

Como hemos visto a lo largo del documento, la fuga de información es uno de los incidentes de seguridad más complejos, por su diversidad y por las posibles consecuencias. Por otro lado, el componente humano y organizativo que subyace a muchos de los incidentes de fuga de información, supone todo un reto en relación con la aplicación de medidas de seguridad eficaces, con el objetivo de prevenir incidentes. Pero a pesar de todo, hoy día, las empresas y las organizaciones cuentan con una gran diversidad de herramientas y medidas que pueden ayudar de manera muy eficaz a prevenir y minimizar significativamente las consecuencias de un incidente de fuga de información.

La prevención de la fuga de información pasa por la aplicación de medidas de seguridad desde tres puntos de vista: **técnico, organizativo y legal**. A continuación exponemos las medidas en forma de tabla para cada uno de ellos.

MEDIDAS ORGANIZATIVAS
Buenas practicas
Política de seguridad
Procedimientos
Clasificación de la información, establecimiento de roles y niveles de acceso
Formación e información interna
Sistema de gestión de seguridad de la información

MEDIDAS TÉCNICAS
Control de acceso e identidad
Soluciones anti-malware y anti-fraude
Seguridad perimetral y protección de las comunicaciones
Control de contenidos y control de tráfico
Copias de seguridad
Control de acceso a los recursos
Actualizaciones de seguridad y parches
Otras medidas de seguridad derivadas del cumplimiento de legislación
Gestión de eventos e inteligencia de seguridad

MEDIDAS LEGALES
Solicitud de aceptación de política de seguridad
Solicitud de aceptación de política de confidencialidad
Otras medidas de carácter disuasorio en base a legislación
Medidas relativas a la adecuación y cumplimiento de la legislación aplicable (LOPD, LSSI, etc)

Finalmente, es importante destacar la necesidad de contar con asesoramiento profesional, no solo durante la gestión de un incidente de fuga de información, sino también, en la fase de diseño de las medidas de prevención. Cada organización es diferente y será necesario buscar un equilibrio entre complejidad, coste y riesgo, en relación con la implantación de las medidas de seguridad.