Cómo gestionar una **fuga de información**

Una guía de aproximación para el empresario

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

2006-2016

TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

INCIBE_PTE_AproxEmpresario_003_FugaInformacion-2016-v1

Índice de figuras y tablas

1 Introducción

La globalización, el aumento de capacidad y velocidad de las transacciones y la movilidad, provocados por la rápida evolución de la tecnología han dejado obsoleta la forma de entender los negocios. Dentro de la empresa existen bienes intangibles como la cartera de clientes, las tarifas, el conocimiento comercial, la propiedad intelectual o la reputación. Elementos que forman parte de la información de nuestra empresa y que constituyen uno de los activos más importantes de la organización.

En este entorno, la seguridad cobra un sentido especial. Todas las propiedades del mercado digital (velocidad, capacidad, movilidad,...) son aprovechadas y explotadas por aquellos que «no juegan limpio». La información se ha convertido en uno de los activos más importantes que posee una organización. Esta información es utilizada 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. Todo ello está convirtiendo a la **fuga de información** en una de las mayores **amenazas** e instrumento de fuerza y presión.

Por este motivo, **la ciberseguridad** es un **elemento clave para el desarrollo económico**. La protección frente a las ciberamenazas (introducción de código dañino en sistemas, ataques a páginas web para robar información, fraude y robo de identidad on-line, destrucción de información,...) y el fomento de la ciberseguridad constituyen factores esenciales para el desarrollo de la economía de Internet. De esta forma evitaremos en la medida de lo posible las filtraciones de información y la pérdida de imagen de nuestra compañía.

Pero hay que tener claro que la ciberseguridad total no existe y en última instancia, la información es manipulada por personas. **«El usuario es el eslabón más importante de la cadena»** en lo que a ciberseguridad se refiere. La fuga de información tiene un componente social y humano muy importante. Detrás de una buena parte de los incidentes de fuga de información se esconden motivaciones personales, económicas, daño a la imagen de la organización o simples errores, entre otras.

La ciberseguridad total no existe y en última instancia, la información es manipulada por personas.
«El usuario es el eslabón más importante de la cadena».

1 Introducción

1.1 ¿Cómo podemos mitigar la fuga de información?

Por un lado debemos desarrollar y actualizar políticas de acceso a la información. Toda organización debe seguir el principio del mínimo privilegio. Este principio se traduce en que un usuario sólo debe tener acceso a aquella información estrictamente necesaria para desempeñar sus funciones diarias, siempre que nos refiramos a información confidencial.

Un usuario sólo debe tener acceso a aquella información estrictamente necesaria para desempeñar sus funciones diarias, siempre que nos refiramos a información confidencial.

Por otro lado la industria de ciberseguridad [1] ofrece multitud de productos y servicios para mitigar esta amenaza. Merece la pena destacar aquellos productos destinados a la gestión del ciclo de vida de la información (*ILM, del inglés Information Lifecycle Management*), productos para el control de dispositivos externos o los que están destinados específicamente a evitar la fuga de información (*DLP, del inglés Data Loss Prevention*).

Además, dado que el factor humano es uno de los componentes de la fuga de la información, es muy importante llevar a cabo campañas de concienciación en materia de ciberseguridad dentro de la organización.

1.2 ¿Qué debemos hacer si se produce una fuga de información en nuestra empresa?

Por desgracia la prevención no es suficiente, puesto que las consecuencias de la fuga de información pueden ser muy negativas y tener un elevado nivel de dispersión, llegando a afectar a otras organizaciones y usuarios. La urgencia por preservar la imagen de la empresa hace que en ocasiones no se tomen las decisiones adecuadas cuando 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.

A lo largo de esta guía se desarrollarán los diferentes aspectos relacionados con la gestión del incidente, es decir, cuando ya se ha producido y hay que gestionar las posibles consecuencias, con el objetivo de minimizar el impacto del incidente de fuga de información sobre la organización y sobre otros actores externos.

2 Fuga de información

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

- La **confidencialidad** implica que la información es accesible únicamente por el personal autorizado.
- La **integridad** de la información hace referencia a que la información sea correcta y esté libre de modificaciones y errores. La información ha podido ser alterada intencionadamente o ser incorrecta y nosotros podemos basar nuestras decisiones sobre ella.
- La **disponibilidad** de la información hace referencia a que la información esté accesible, a las personas o sistemas autorizados, cuando sea necesario.

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

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

El impacto y las consecuencias posteriores a un incidente de fuga de información, son muy negativos. Por un lado, la filtración de información puede dañar la imagen pública de la empresa y por tanto impactar negativamente en el negocio, generando desconfianza e inseguridad en clientes. Asimismo, la publicación de información puede generar consecuencias a terceros: grupos externos de usuarios y otras organizaciones cuyos datos se hayan hecho públicos.

Además, existe un conjunto de normativas y leyes que ponen especial énfasis en el uso y tratamiento de datos de carácter personal. Dentro del tratamiento de datos de carácter personal se han de considerar las fugas de información, ya que en muchas ocasiones, estos incidentes terminan con la difusión o publicación de datos de carácter personal. Dichas normativas prevén sanciones de tipo económico para este tipo de delitos.

Por otra parte la ocultación del incidente de fuga de información también puede ser motivo de sanción. La Agencia Española de Protección de Datos (AEPD) es una 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. Entre sus tareas se encuentra detectar fugas de información. Si una empresa oculta un incidente de fuga de fuga de información y la AEPD lo detecta, la sanción podría ser importante.

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 Fuga de información

2.1 Origen y motivos

El origen de las amenazas que provocan la fuga de información puede ser tanto externo como interno.

Por origen interno se entienden las fugas de información ocasionadas por empleados propios de la empresa, ya sea de forma inadvertida (por desconocimiento o por error) o a propósito.

Por origen interno se entienden las fugas de información ocasionadas por empleados propios de la empresa.

En el segundo caso los motivos «intencionados» que pueden estar detrás de este tipo de incidentes son muy variados y podrían ser: por estar descontento con la empresa, la venganza, la venta de secretos industriales o información privilegiada para la obtención de beneficio económico, el daño a la imagen de la empresa o la creación de una nueva con parte de los activos de información.

Los principales orígenes externos de la fuga de información abarcan desde organizaciones criminales hasta activistas. Sus principales motivaciones pueden ser desde la obtención de un beneficio económico con la venta de la información sustraída, la obtención de información específica (planos, proyectos), hasta dañar la imagen de la empresa o llevar a cabo acciones reivindicativas.

2.2 ¿Cuáles son las causas? ¿Cómo prevenirlas?

Las causas principales de los casos de fuga 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.

Además, la mayoría de las causas, tanto organizativas o técnicas, generalmente, implican la ausencia de algún tipo de medida de seguridad, procedimiento, herramienta, etc. Esta ausencia de medidas supone la falta de control sobre la información y esta falta de control aumenta de forma significativa la probabilidad de que se produzca un incidente de fuga de información.

Dentro de las causas organizativas:

- Uno de los primeros errores que se comete en relación con la protección de la información es la **falta de una clasificación** de la misma. Esta clasificación se puede realizar en base a su nivel de confidencialidad, en función de diversos parámetros: 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 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 quién debe conocer la información y qué tipo de acciones puede realizar sobre esta. Esto se conoce como principio del mínimo conocimiento [2].

2 Fuga de información

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

- 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 de los servicios en la nube, los dispositivos móviles, el correo electrónico, la navegación Web, etc. Por otro lado, debe disponer de ciertos conocimientos y formación en relación con su actividad diaria y en materia de ciberseguridad [3], siendo responsabilidad de la organización proporcionar la formación necesaria de manera que el empleado pueda desempeñar su función de forma segura.

- Otra causa organizativa es la **ausencia de procedimientos** y el establecimiento de pautas y 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 para que se produzca una fuga de información.

- Por último otra causa es que **no existan acuerdos de confidencialidad de la información** con los empleados. Es importante solicitar 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.
  Además, se cuenta con legislación que 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 la información.

Por otro lado, dentro de las causas técnicas nos encontramos con:

- El **código malicioso o malware**, es una de las principales amenazas, siendo el robo de información uno de sus objetivos más comunes. El malware esta muchas veces diseñado utilizando técnicas que permiten mantener oculto su 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, o con motivo de sustraer información sobre secretos industriales. 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 aplicación, puesto que aporta mayor seguridad y denota un trabajo de mejora continua que redunda en beneficio de la aplicación y, por extensión, del usuario.

2 Fuga de información

- La generalización del uso de **servicios en la nube para el almacenamiento** de todo tipo de información puede conllevar a la percepción de que en la nube nuestra información está segura, cuando lo cierto es que no es así. El nivel de seguridad que tiene es el del eslabón más débil, que, muy a menudo son los propios usuarios y sus contraseñas. Los incidentes de fuga información causados por el uso inadecuado de servicios en la nube son parecidos a los causados por uso de redes sociales y la forma de tratarlos es muy similar.

- El uso de las **tecnologías móviles** para el trabajo diario, almacenando en ellos información muy crítica han ocasionado la generalización de medidas como el cifrado de los dispositivos o el uso de VPN (redes privadas virtuales) en las comunicaciones. Sin embargo, si la información almacenada en los dispositivos es realmente critica, ninguna medida puede llegar a ser suficiente. Un dispositivo sustraído, en las manos equivocadas, contendrá mucha información que puede ser publicada. Además este tipo de incidentes son de difícil mitigación. Las medidas de seguridad deben haberse tomado con anterioridad al incidente, porque una vez este ocurre hay poco margen de maniobra.

La generalización del uso de servicios en la nube para el almacenamiento de todo tipo de información puede conllevar a la percepción de que en la nube nuestra información está segura, cuando lo cierto es que no es así.

3 Las consecuencias

Las consecuencias de un incidente de fuga de información preocupan enormemente a las empresas y las organizaciones. Un incidente de estas características que se hace público puede causar un importante daño de imagen y 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 adecuada gestión de incidentes de este tipo. Así será posible diseñar una estrategia, de forma que en caso de que finalmente se produzca, se tomen las decisiones y medidas adecuadas para minimizar el impacto del incidente.

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 de cara a establecer las consecuencias y el posible nivel de impacto.

3.1 Estimación del impacto

Para estimar el conjunto de las consecuencias que se derivan de un incidente de fuga de información, en primer lugar podemos agruparlos en las siguientes categorías:

Un incidente de estas características que se hace público puede causar un importante daño de imagen.

- **Daño de imagen.** Genera un impacto negativo de la entidad y lleva implícita pérdida de confianza.
- **Consecuencias legales.** Podrían conllevar sanciones económicas o administrativas.
- **Consecuencias económicas.** Estrechamente relacionadas con las anteriores se encuentran dentro de aquellas que suponen un impacto negativo a nivel económico, con una disminución de la inversión, negocio, etc.
- **Otras consecuencias.** Son aquellas que afectan o suponen un impacto negativo en ámbitos muy diversos, como por ejemplo, el ámbito político, diplomático, institucional, o gubernamental, entre otros.

Todas estas categorías están relacionadas entre sí y suelen darse conjuntamente. La diferencia estará en función del escenario, donde cada uno de ellos tendrá un peso.

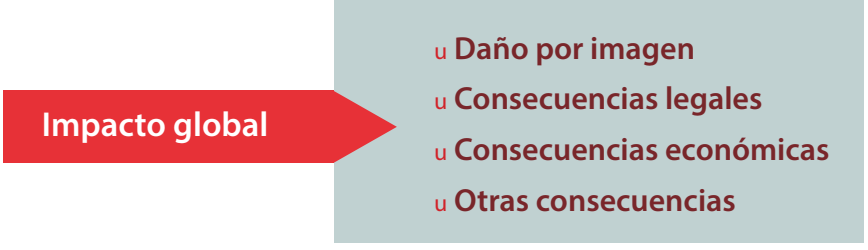

Ilustración 1 *Consecuencias de la fuga de información*

3 Las consecuencias

Uno de los factores que definen el escenario es el **tipo de organización**. El peso de las consecuencias será diferente si el incidente afecta a la administración o si se trata de una entidad privada:

- **Administración.** El posible daño e imagen es un factor que cobra importancia desde un punto de vista político. Sin embargo, las consecuencias económicas, así como las sanciones debidas a incumplimiento de la legislación, son limitadas.

- **Entidades del sector privado.** Las consecuencias que tienen mayor peso son aquellas de carácter económico. Además, a diferencia de las administraciones, el sector privado sí está expuesto a sanciones económicas. Por otra parte, 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 adicionales que definen el escenario es si la información que ha sido accedida es considerada como información confidencial o no. Las consecuencias pueden ser muy distintas. Por tanto, además de la clasificación anterior tenemos también:

- **Información confidencial o restringida**. Aquella información que consideremos crítica para los procesos de nuestra entidad. Por ejemplo, datos de clientes, contabilidad, datos de los propios trabajadores.

- **Información no confidencial**. El hecho de su divulgación impactaría en la imagen de la empresa, pero el peso del impacto económico será menor.

La divulgación o difusión de cualquier dato que identifique o que pueda ser asociado a una persona, puede conllevar sanciones para la organización que ha sufrido el incidente.

3 Las consecuencias

Otro de los factores que definen el escenario es el **tipo de datos**, diferenciando entre:

- **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**. Serán aquellos que no son datos de carácter personal, generalmente relacionados con terceros, información técnica u operativa.

En base a estos tres factores podemos tener una aproximación que ayude a determinar las posibles consecuencias de un incidente.

Para obtener una escala de valor de las consecuencias, es necesario contar con una valoración objetiva tanto de los factores comentados como de otros factores, siguiendo un procedimiento de análisis de riesgos. Tendremos en cuenta el activo a proteger de la fuga de información, la amenaza, la probabilidad de que ocurra y el impacto para poder obtener el dato real de riesgo.

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. Estos factores servirán para diseñar un plan de gestión del incidente de fuga de información.

Para obtener una escala de valor de las consecuencias, es necesario contar con una valoración objetiva tanto de los factores comentados como de otros factores, siguiendo un procedimiento de análisis de riesgos.

4 Gestión de la fuga de información

Al ser muchos los aspectos y situaciones dentro de este tipo de incidentes, una mala gestión podría tener el efecto contrario al deseado, es decir, se puede magnificar el efecto negativo del incidente.

El plan para la gestión de los incidentes de fuga de información que se propone recoge los principales puntos y aspectos a tener en cuenta. La gravedad del incidente y el contexto en el que se produzca hace que los diferentes pasos se adapten al escenario específico.

1	**Fase inicial**	n detección del incidente n alerta del incidente a nivel interno n inicio del protocolo de gestión
2	**Fase de lanzamiento**	n reunión del gabinete de crisis n informe inicial de situación n coordinación y primeras acciones
3	**Fase de auditoría**	n auditoría interna y externa n elaboración de informe preliminar
4	**Fase de evaluación**	n reunión del gabinete de crisis n presentación del informe de auditoría n determinación de principales acciones n tareas y planificación
5	**Fase de mitigación**	n ejecución de todas las acciones del plan
6	**Fase de seguimiento**	n valoración de los resultados del plan n gestión de otras consecuencias n auditoría completa n aplicación de medidas y mejoras

Tabla 1 *Resumen de acciones*

4 Gestión de la fuga de información

4.1 Fase inicial

Los momentos inmediatamente posteriores a la detección de un incidente de fuga de información son especialmente críticos. Una adecuada gestión en las primeras fases puede suponer una reducción del impacto. Excepto en el caso de pérdida de dispositivos móviles, el principal problema es que en la mayoría de las ocasiones no es detectado hasta que su filtración se hace pública bien a través de los medios de comunicación o Internet, bien a través de algún tipo de notificación por parte del ciberdelincuente responsable del hecho.

Por este motivo, 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, además realizar una constante monitorización de cualquier publicación sobre nuestra entidad, para tomar el control de la situación lo antes posible.

Uno de los mayores retos a los que se enfrentan las organizaciones es conseguir la detección temprana del incidente

Una vez que hemos tenido conocimiento del incidente, en primer lugar debemos de informar internamente de la situación, junto con el lanzamiento del protocolo de actuación. Dentro de la información que debemos transmitir internamente es importante incidir en la prudencia y redirigir a un interlocutor previamente designado cualquier duda o pregunta tanto de los propios empleados como si la misma procede de terceros el exterior. Además, se deberá de informar de la puesta en marcha del proceso de gestión de la incidencia.

4.2 Fase de lanzamiento

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.

No todas las organizaciones cuentan con un gabinete de crisis o tienen los recursos necesarios. Cada organización deberá ajustarse a sus recursos. En cualquier caso, será necesario contar como mínimo con un responsable con capacidad de decisión, ya sea personal propio de la organización 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, la gestión será más efectiva.

Mantener la calma y actuar con organización es fundamental para evitar decisiones incorrectas o que pueden provocar consecuencias negativas adicionales

En cualquier caso, todas las decisiones y las actuaciones relativas al incidente deberán 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.

4.3 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:

- Determinar la cantidad (tamaño en disco, número de registros, etc.) de información ha podido ser sustraída.
- Establecer el tipo de datos que contiene la información que ha podido ser sustraída. Debe considerarse especialmente si se han filtrado datos de carácter personal y de qué nivel según el reglamento de la LOPD [4].
- 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 y acotar 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 responsables de esa información.

Además de la 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

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 información que ha sido sustraída e información que se ha hecho pública, ya que no son necesariamente lo mismo. Al menos es necesario:

- Determinar el alcance de la publicación de la información sustraída (dónde se ha publicado, cuantos potenciales accesos habrá tenido, etc.). Este punto es crítico para cerrar la brecha de seguridad y mitigar la difusión de la información sustraída.
- 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.
- Recoger las noticias y otros contenidos que hayan aparecido en los medios de comunicación, así como en otros medios en Internet sobre el incidente.
- 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, un periodo superior a las 48 horas podría considerarse excesivo, aunque dependerá de la gravedad del incidente y de otros factores. En este sentido, 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 obtenida se inicia el proceso de valoración del incidente, posibles consecuencias e impacto. Se establecen las tareas principales con 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 con agilidad.

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

Se debe considerar que al tratarse de una evaluación inicial las tareas se diseñan en función de la información disponible, que puede ser incompleta

- Tareas 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.

4.5 Fase de mitigación

El primer paso es reducir la brecha de seguridad y evitar que se produzcan nuevas fugas de información. Por este motivo, en algunos casos es posible que sea necesario desconectar un determinado servicio o sistema de Internet. Ante esta situación debe primar el objeto del plan que no es otro que 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 es debemos 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 y se solicitará su retirada, en especial si se trata de información sensible o protegida por la LOPD.

Junto con el paso anterior, si se considera necesario, se llevará a cabo 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.

El primer paso es reducir la brecha de seguridad y evitar que se produzcan nuevas fugas de información.
Por este motivo, en algunos casos es posible que sea necesario desconectar un determinado servicio o sistema de Internet.

4.5

En caso de existir personas afectadas por la fuga de información, por ejemplo, si se han filtrado datos de terceros, como clientes o usuarios de un servicio, es fundamental que estos sean informados. Se informará no solo del incidente, sino también de los datos que han sido sustraídos a fin de que puedan tomar las acciones oportunas para su seguridad, como puede ser el cambio de contraseñas, revocación de números de tarjetas, ser especialmente cautelosos con correos de desconocidos, 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.

Posteriormente se pondrá en conocimiento del incidente a las fuerzas y cuerpos de seguridad del estado, 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 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.

4.6 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 de hacer frente a otras consecuencias que hayan podido generarse durante la fase de mitigación del incidente, como puedan ser consecuencias legales, económicas, etc.

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 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.

Durante esta fase también se iniciará el proceso de estabilización de la situación generada por el incidente.

5 Prevención

Las principales medidas de prevención deben orientarse hacia el componente humano y organizativo que se encuentra dentro de las causas de este tipo de incidentes.

La prevención de la fuga de información pasa por la aplicación de medidas de seguridad desde tres puntos de vista: técnico, organizativo y legal.

Medidas organizativas

- Poner en marcha buenas prácticas para la gestión de fuga de la información.
- Definir una política de seguridad y procedimientos para todo el ciclo de vida de los datos.
- Establecer un sistema de clasificación de la información, para ligarlo a roles y niveles de acceso.
- Llevar a cabo acciones de formación e información interna en ciberseguridad.
- Implantar un 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 telecomunicaciones.
- Control de contenidos, control de tráfico y copias de seguridad.
- Control de acceso a los recursos, actualizaciones de seguridad y parches.

Medidas legales

- Solicitud de aceptación de la política de seguridad y de la de conformidad por parte de los empleados.
- Medidas relativas a la adecuación y cumplimiento de la legislación aplicable (LOPD, LSSI, etc).
- Otras medidas de carácter disuasorio en base a la legislación.

Tabla 2
Medidas preventivas

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. Pero el **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 es de vital importancia.

Para evitar fugas de información causadas por el uso inadecuado de servicios en la nube, debemos seguir las mismas medidas que para otros tipos de incidentes: sobre todo un buen control del acceso a dichos servicios y concienciación de los empleados.

Para los incidentes causados por dispositivos móviles, la prevención se basa en implantar políticas de uso y medidas técnicas: soluciones anti-malware, cifrado, uso de sistemas VPN, etc.

6 Referencias

1 INCIBE – Empresas - Herramientas – Catálogo de ciberseguridad
https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad
[consulta: 30/06/2015]

2 Blog Empresas de INCIBE – ¿Acceso a la información? Sólo el mínimo.
https://www.incibe.es/protege-tu-empresa/blog/politica-acceso-informacion-principio-minimo-conocimiento
[consulta: 12/05/2015]

3 INCIBE – Empresas – Kit de concienciación
https://www.incibe.es/protege-tu-empresa/kit-concienciacion
[consulta: 30/06/2015]

4 BOE – Art. 80 y 81 (Niveles de seguridad y aplicación de los niveles de seguridad) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
http://www.boe.es/buscar/doc.php?id=BOE-A-2008-979
[consulta: 12/05/2015]

5 INCIBE - Dossier Protección de la información
https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion
[consulta: 12/05/2015]

6 ENISA - Recommendations for a methodology of the assessment of severity of personal data breaches.
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity/at_download/fullReport
[consulta: 12/05/2015]

7 ENISA - Recommendations for the technical implementation of the Art.4 of the ePrivacy Directive.
https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech
[consulta: 12/05/2015]

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL