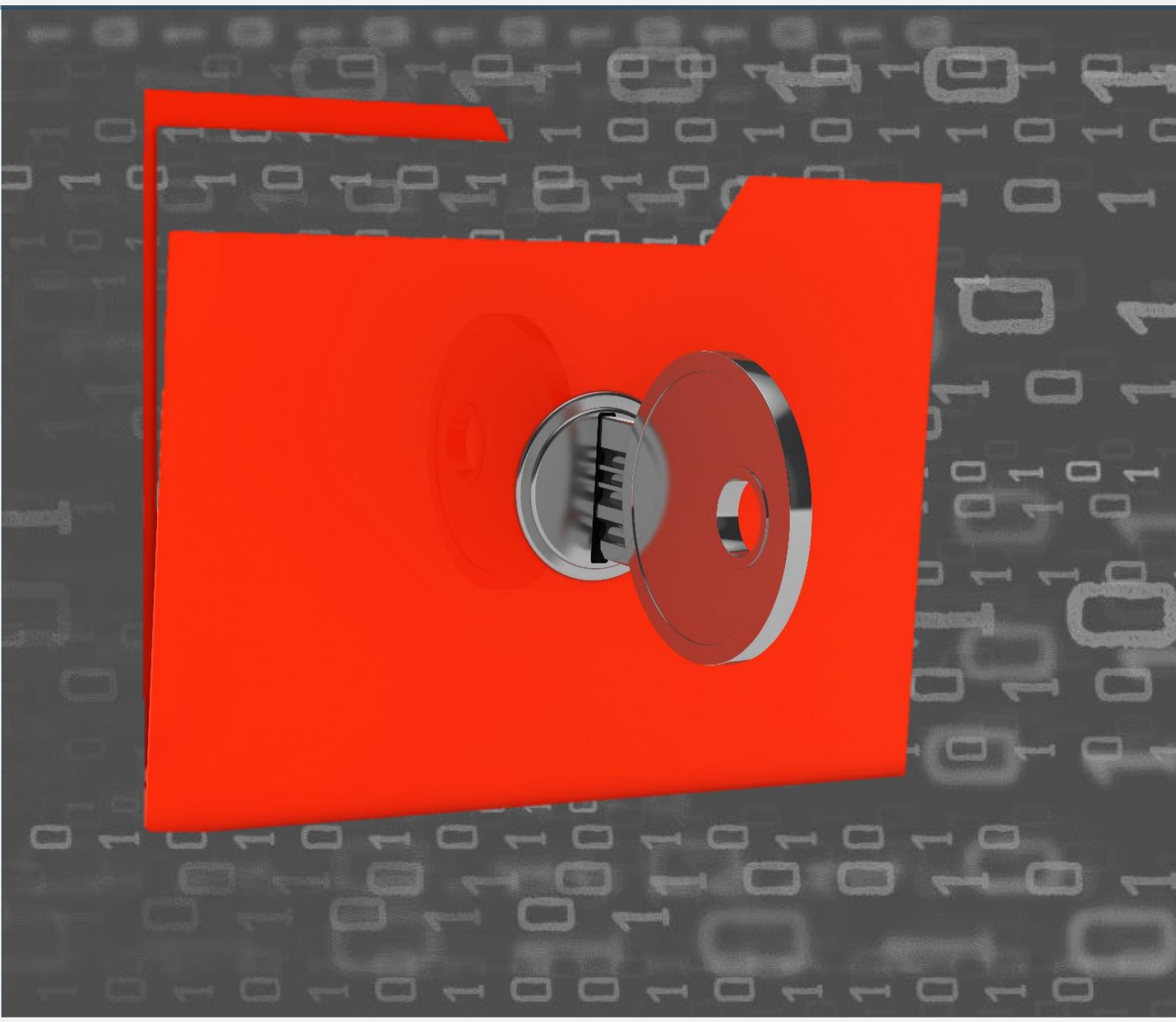
ASOCIACIÓN DE EMPRESARIOS SETE PONTES



REGISTRO INTERNO DE ACTIVIDADES DE TRATAMIENTO

ÍNDICE

Validez de documento:
El documento deberá mantenerse en todo momento actualizado.
Deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
El contenido estará adecuado en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.
Este documento no supone un pronunciamiento explícito o implícito sobre características o situaciones no evidentes y no podrá ser usado para una finalidad distinta de la que es objeto.

1. OBJETO DEL REGISTRO INTERNO DE ACTIVIDADES DE TRATAMIENTO

Ante la decisión por parte de la asociación de adecuar su sistema de información a la legislación vigente en materia de protección de datos de carácter personal tal y como prevé el **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) (UE) 2016/679, y la LEY ORGÁNICA 3/2018 DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES (LOPDGDD), de 5 de diciembre de 2018**, se desarrolla el presente documento que recopila las normas y los procedimientos necesarios para la aplicación de las medidas de seguridad de obligado cumplimiento para todo el personal con acceso a los datos de carácter personal y a los sistemas e instalaciones que los soportan, y que deben servir para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados dichas normativas.

La nueva Ley de Protección de Datos Personales y Garantía de los Derechos Digitales LOPDGDD 3/2018, entró en vigor el pasado 07 de diciembre de 2018, y adapta el derecho español al RGPD (UE) 216/679 que entró en vigor en mayo de 2016, siendo aplicable desde mayo de 2018. Por ello, los responsables deben ante todo asumir las precisiones y desarrollos de la LOPDGDD 3/2018.

El RGPD (UE) 216/679 y la LOPDGDD 3/2018, modifican algunos aspectos del régimen actual y contiene nuevas obligaciones que deben ser analizadas y aplicadas por cada organización teniendo en cuenta sus propias circunstancias.

Dos elementos de carácter general constituyen la mayor innovación para los responsables y se proyectan sobre todas las obligaciones de las organizaciones:

EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

Se describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.
En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.
En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

EL ENFOQUE DE RIESGO

Se señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas.
De acuerdo con este enfoque, algunas de las medidas que establece el RGPD, se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten.
La aplicación de las medidas previstas por el RGPD (UE) 216/679 y la LOPDGDD 3/2018 deben adaptarse, por tanto, a las características de las organizaciones.

BASES DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS

El RGPD (UE) 216/679 mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPDGDD 3/2018, aunque en nuestro caso las bases jurídicas aplicables son:

- Consentimiento.
- Relación contractual.
- Obligación legal para el responsable.
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

En ese sentido, el RGPD (UE) 216/679 y la LOPDGDD 3/2018, no implica cambios para los responsables del tratamiento de datos.

- Hay que documentar e identificar claramente la base legal sobre la que se desarrolla el tratamiento al proporcionar la información en el momento de recoger los datos de los interesados.
- Hay que especificar y documentar los intereses legítimos en que se fundamentan las operaciones de tratamiento en casos como las Evaluaciones de Impacto sobre la Protección de Datos o en determinadas transferencias internacionales.

La identificación de la base legal es indispensable para estar en condiciones de demostrar que se cumple con las previsiones del el RGPD (UE) 216/679 y la LOPDGDD 3/2018, y dicha identificación y documentación debe adaptarse al tipo de tratamiento y a las características de las organizaciones.

El consentimiento debe ser "inequívoco" y es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.

A diferencia del Reglamento de Desarrollo de la LOPD 15/1999, no se admiten formas de consentimiento tácito o por omisión, ya que se basan en la inacción.

Se contemplan situaciones en las que el consentimiento, además de inequívoco, ha de ser explícito:

- Tratamiento de datos sensibles.
- Adopción de decisiones automatizadas.
- Transferencias internacionales.

El consentimiento puede ser inequívoco y otorgarse de forma implícita cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación).

Los tratamientos iniciados con anterioridad al inicio de la aplicación del el RGPD (UE) 216/679 y la LOPDGDD 3/2018, sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé el propio el RGPD (UE) 216/679 y la LOPDGDD 3/2018, es decir, mediante una manifestación o acción afirmativa.

La adaptación puede llevarse a cabo:

- Obteniendo un consentimiento de los interesados acorde con las disposiciones del el RGPD (UE) 216/679 y la LOPDGDD 3/2018.
- Valorando si los tratamientos afectados pueden apoyarse en otra base legal. Como puede ser, entre otras, el interés legítimo del responsable o del cesionario de los datos que prevalezca sobre los derechos del interesado (los interesados deben ser informados y podrán ejercitar los derechos que, como el de oposición, sean específicamente aplicables a la nueva base legal elegida).

2. DATOS DE IDENTIFICACIÓN DEL RESPONSABLE DE TRATAMIENTO

Razón social: **ASOCIACIÓN DE EMPRESARIOS SETE PONTES**
CIF: **G27162973**
Domicilio social: **Rúa do Castiñeiro, E-1 – 27800 Vilalba (Lugo)**
Teléfono: **982 523 069**
Correo electrónico: **contacto@poligonosetepontes.com**

3. ÁMBITO DE APLICACIÓN

El presente documento será de aplicación a los sistemas de tratamiento de datos de carácter personal que se hallan bajo la responsabilidad de la ASOCIACIÓN DE EMPRESARIOS SETE PONTES, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Este documento ha sido elaborado bajo la responsabilidad de la entidad descrita anteriormente que, como responsable del tratamiento, se compromete a implantar y actualizar esta Normativa de Seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten el acceso a los mismos.

En concreto, los sistemas de tratamiento de datos sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

Socios/asociados y proveedores	Nivel de Seguridad Básico
Socios/asociados potenciales	Nivel de Seguridad Básico
RRHH, Nóminas y Personal	Nivel de Seguridad Medio
Candidatos	Nivel de Seguridad Medio
Contabilidad	Nivel de Seguridad Medio
Transmisiones telemáticas	Nivel de Seguridad Medio
Usuarios Web	Nivel de Seguridad Medio

En el Apartado 6 del presente documento se describen detalladamente cada uno de los sistemas de tratamiento junto con los aspectos que les afecten de manera particular.

4. OBLIGACIONES DEL RESPONSABLE DE TRATAMIENTO

- El responsable de tratamiento se encargará de coordinar y controlar las medidas definidas en este documento, colaborará con el encargado del tratamiento en su difusión y cooperará con él controlando el cumplimiento de las mismas.

- El responsable de tratamiento habilitará un libro de incidencias, a disposición de todos los usuarios y administradores de los sistemas de tratamiento de datos, con el fin de que se registre en él cualquier incidencia que pueda suponer un peligro para la seguridad de los mismos y analizará dichas incidencias registradas, tomando las medidas oportunas en colaboración con el encargado del tratamiento.

- El responsable de tratamiento comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Registro Interno de Actividades de Tratamiento se corresponde con la lista de usuarios que realmente están autorizados en la aplicación de acceso a los datos, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del tratamiento.

  Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de tratamiento sin que se deba permitir, en ningún caso la desactivación de los mismos.

  El responsable de tratamiento se encargará de revisar periódicamente la información de control registrada, los resultados de todos estos controles periódicos, así como de las auditorías, que serán adjuntadas a este documento.

  Además de estas comprobaciones periódicas, el administrador comunicará al responsable de tratamiento, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado a los sistemas de tratamiento.

- Comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de los datos según lo estipulado en este documento.
- A su vez, y también con periodicidad al menos trimestral, los administradores de los sistemas de tratamiento de datos comunicarán al responsable de tratamiento cualquier cambio en el software o hardware, base de datos o aplicaciones de acceso a los datos, procediendo igualmente a la actualización de dichos anexos.
- El responsable de tratamiento, verificará, con periodicidad al menos trimestral, el cumplimiento y la adecuación de las medidas del presente documento a las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias.
- Los informes de auditoría serán analizados por el responsable de tratamiento, quien propondrá al encargado de tratamiento las medidas correctoras correspondientes.

5. DATOS DE LOS EQUIPOS

- Los recursos que, por servir de medio directo o indirecto para acceder a los datos deberán ser controlados por esta normativa son:

  - Los centros de tratamiento y locales donde se encuentran ubicados los datos o se almacenen los soportes que los contengan.

- Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso a los datos.
- Los servidores y el entorno de sistema operativo y de comunicaciones en el que se encuentran ubicados los datos.
- Los sistemas informáticos, o aplicaciones establecidas para acceder a los datos descritos.

La protección de los datos frente a accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

- Los recursos existentes en el ámbito de aplicación de este documento se detallan a continuación:

  - Sistema operativo cuyas características del software se especifican en el documento "ANEXOS" que complementa el presente documento.
  - Ordenadores propios en cada departamento cuyas especificaciones se encuentran en el documento "ANEXOS" que complementa el presente documento.
  - Licencias antivirus de diferentes modelos y especificaciones detalladas documento "ANEXOS" que complementa el presente documento.

- En cuanto al local que contiene los datos de carácter personal, que cumple con las medidas de protección adecuadas al nivel de los datos tratados, se encuentra ubicado en: Rúa do Castiñeiro, E-1 - 27800 Vilalba (Lugo)

6. REGISTROS DE TRATAMIENTOS DE DATOS

El documento "ANEXOS" que complementa el presente documento, contiene los contratos sobre cesión de datos firmados con los empleados con acceso a los mismos, proveedores de productos y servicios, así como las cláusulas informativas incluidas en los formularios de solicitud de información a candidatos y socios y/o asociados potenciales.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Tratamiento: Socios/asociados y proveedores

- Finalidad del tratamiento: Gestión de la relación con los socios/asociados y proveedores.

- Descripción de las categorías de socios/asociados y de las categorías de datos personales:
    - Socios/asociados y proveedores: Personas con las que se mantiene una relación como socio/asociado o proveedor de bienes o servicios.

    - Categorías de datos personales: Los necesarios para el mantenimiento de la relación (facturación, envío de comunicaciones por correo postal, correo electrónico, Whatsapp, redes sociales y fidelización):
        - De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail
        - Datos bancarios: para la domiciliación de pagos

- Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:
    - Administración tributaria
    - Seguridad Social
    - Bancos y entidades financieras
    - Cuerpos y fuerzas de seguridad del estado
    - Gestoría
    - Servicio de transporte y/o mensajería

- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos serán los previstos por la legislación fiscal respecto a la prescripción de responsabilidades.

Tratamiento: Potenciales socios/asociados

- Finalidad del tratamiento: Gestión de la relación con los potenciales socios y/o asociados.

- Descripción de las categorías de potenciales socios y/o asociados, y de las categorías de datos personales:
    - Potenciales socios/asociados: Personas con las que se busca/espera mantener una relación como socios/asociados.

    - Categorías de datos personales: Los necesarios para la prestación de los servicios de la asociación.
        - De identificación: nombre, apellidos y dirección postal, teléfonos, e-mail

- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales: No se contempla.

- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos: Un año desde el primer contacto.

Tratamiento: RRHH, Nóminas y personal

- Finalidad del tratamiento: Gestión de la relación laboral con los empleados.

- Descripción de las categorías de empleados y de las categorías de datos personales:
  - Empleados: Personas que trabajan para el responsable del tratamiento.
  - Categorías de datos personales: Los necesarios para el mantenimiento de la relación laboral (gestión de nóminas, formación, etc.):
    - De identificación: nombre, apellidos, número de Seguridad Social, dirección postal, teléfonos, e-mail
    - Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y porcentaje de minusvalía
    - Datos académicos
    - Datos profesionales
    - Datos bancarios, para la domiciliación del pago de las nóminas

- Las categorías de destinatarios a quienes se comunican o comunicarán los datos personales:
  - Gestoría laboral, fiscal y contable
  - Bancos y entidades financieras
  - Seguridad Social y Mutuas
  - Servicios de Prevención ajenos
  - AEAT

- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades.

Tratamiento: Candidatos

- Finalidad del tratamiento: Gestión de la relación con los candidatos a un empleo en la asociación.

- Descripción de las categorías de candidatos y de las categorías de datos personales:
  - Candidatos: Personas que desean trabajar para el responsable del tratamiento.

  - Categorías de datos personales: Los necesarios para gestionar los *currículums* de posibles futuros empleados.
    - De identificación: nombre, apellidos, dirección postal, teléfonos, e-mail.

- Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y otros excluyendo datos de raza, salud o afiliación sindical.
- Datos académicos
- Datos profesionales.

- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales: No se contempla.

- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos: Un año desde la presentación de la candidatura.

Tratamiento: Contabilidad

- Finalidad del tratamiento: Cumplimiento de la Normativa Mercantil de la Gestión contable de la asociación.

- Descripción de las categorías: Elaboración de Balances, Cuenta de Pérdidas y Ganancias Libro Mayor, Memoria Anual, Estimaciones y Amortizaciones.

- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:
  - Administración tributaria
  - Seguridad Social
  - Gestoría
  - Bancos y entidades financieras

Cuando sea posible, los plazos para la supresión de las diferentes categorías de datos: Los previstos por la legislación fiscal/contable respecto a la prescripción de responsabilidades.

Tratamiento: Transmisiones Telemáticas

- Finalidad del tratamiento: Gestión online de cobros y pagos de socios y/o asociados y proveedores.

- Descripción de las categorías de proveedores y de las categorías de datos personales:

  - Transmisiones Telemáticas: Transmisión online de modelos oficiales a través de sistema propio de las Administraciones para cumplir con las obligaciones mercantiles, fiscales, sociales y personales. Los sistemas de tratamiento telemáticos se transmiten a través de programas de las mismas Administraciones bajo las conexiones seguras de éstas.

- Categorías de datos personales: Los necesarios para la gestión de cobros y pagos online.
    - De identificación: nombre, NIF, dirección postal, teléfonos, e-mail.
    - Datos de facturación y bancarios: para la domiciliación de pagos.

- Cuando sea posible, los plazos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

Tratamiento: Usuarios Web

- Finalidad del tratamiento: Atención y fidelización a socios/asociados y socios/asociados potenciales.

- Descripción de las categorías usuarios web y de las categorías de datos personales:
    - Usuarios Web: Potenciales socios/asociados que contactan con la asociación a través del formulario disponible en nuestra página web.
    - Categorías de datos personales: Los necesarios para la atención y fidelización de socios que contactan a través de la web de la asociación:
        - De identificación y/o contacto: nombre, empresa, correo electrónico, teléfono y asunto.

- Cuando sea posible, los plazos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos serán transcurrido un mes, salvo comunicación a Fuerzas y Cuerpos de Seguridad, o/y Juzgados y Tribunales.

7. PERSONAL – FUNCIONES Y OBLIGACIONES

Todas las personas que tengan acceso a los datos de carácter personal, bien a través del sistema informático habilitado para acceder a los mismos o bien a través de cualquier otro medio de acceso, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos, siendo requisito obligatorio para poder acceder a los mismos el haber firmado la recepción del mismo.

En el apartado ANEXOS, que complementa este documento, se detallan los usuarios o personal que habitualmente utilizan el sistema de tratamiento en el que se tratan los datos, su nivel de acceso y sus funciones. Este documento es de obligado cumplimiento para todos ellos.

- Funciones que desempeñan: Atención a socios y/o asociados, recogida de información, documentación y procesamiento de las misma, tareas contables tanto propias como de socios y/o asociados, realización de sistemas de tratamiento de datos de recursos humanos así como también cualquier tipo de tarea relacionada con la actividad de la asociación.

- Los puestos de trabajo están bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

- Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación de trabajo implicará la desactivación del salvapantallas con la introducción de la contraseña correspondiente.

- En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos tratados, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

- Queda expresamente prohibida la conexión a redes o sistemas externos de los puestos de trabajo, desde los que se realiza el acceso a los datos. La revocación de esta prohibición será autorizada por el responsable del tratamiento, quedando constancia esta modificación en el Libro de incidencias.

- Los puestos de trabajo desde los que se tiene acceso a los datos tendrán una configuración fija en sus aplicaciones y sistemas operativos que sólo podrá ser modificada bajo la autorización del responsable de tratamiento o por administradores autorizados que estén detallados en el Registro Interno de Actividades de Tratamiento.

Salvaguarda y protección de las contraseñas personales

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

Correo Electrónico

La entidad se reserva el derecho de revisar, sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la entidad como responsable civil subsidiaria.

Cualquier dato introducido en la red corporativa o en el terminal del usuario a través de mensajes de correo electrónico que provenga de redes externas debe cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y a control de virus.

Acceso a Internet

El uso del sistema informático de la asociación para acceder a redes públicas como Internet, se limita a los temas directamente relacionados con la actividad de la asociación y los cometidos del puesto de trabajo del usuario.

El acceso a aplicaciones de mensajería, páginas web, grupos de noticias (Newsgroups) y otras fuentes de información como FTP, etc… se limita a aquellos que contengan información relacionada con la actividad de la entidad o con los cometidos del puesto de trabajo del usuario.

La asociación se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa.

Cualquier dato de carácter personal introducido en la red corporativa o en el terminal del usuario desde Internet, debe cumplir los requisitos establecidos en estas normas y, en especial las referidas a la propiedad intelectual e industrial y al control de virus.

Están expresamente prohibidas las siguientes actividades:

- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la asociación.

- Destruir, alterar, inutilizar o de cualquier forma dañar los datos, programas o documentos electrónicos de la entidad o de terceros. Esto puede constituir un delito de daños, previsto en el artículo 264.2 del Código Penal.

- Enviar mensajes por correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario.

- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. Esta actividad puede constituir un delito de intercepción de las telecomunicaciones, previsto en el artículo 197 del Código Penal.

- Introducir voluntariamente programas, virus, macros, controles Active o cualquier otro dispositivo lógico o secuencial de caracteres que cause o sea susceptible de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros. El usuario tiene la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.

- Utilizar los recursos telemáticos de la entidad, incluida la red de Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.

- Introducir copias ilegales de cualquier programa, incluidos los estandarizados.

- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la entidad, en la red corporativa de la entidad.

- Compartir o facilitar los identificadores de usuario y las claves de acceso facilitados por la Empresa con otra persona física o jurídica, incluido el personal de la propia entidad. En caso de incumplimiento de esta prohibición, el usuario es el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada el identificador del usuario.

- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la asociación o de terceros.

- Intentar aumentar el nivel de privilegios de un usuario en el sistema.

La estructura informática de la asociación mediante doble conexión a la red garantiza el servicio ante posibles averías / ataques en uno de los accesos, con dispositivos firewall y antivirus para protección de acceso a la Red Local corporativa.

Todos los equipos están provistos de un control de acceso con contraseñas alfanuméricas de usuario y antivirus actualizados.

8. NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS Y/O VIOLACIONES DE SEGURIDAD

Las brechas de seguridad pueden tener importantes consecuencias, tanto en términos reputacionales como económicos. Por lo tanto, nos hemos asegurado de poner en marcha todos los procedimientos que permitan detectar, informar e investigar una brecha de seguridad. El RGPD (UE) 216/679 y la LOPDGDD 3/2018, exigen a los responsables del tratamiento que hayan sufrido una infracción en la que el individuo sufra algún tipo de daño, como por robo de identidad o violación de la seguridad de los datos personales, lo notifiquen a su Autoridad de Protección de Datos en un plazo máximo de 72 horas (en caso contrario deberá ir acompañada de indicación de los motivos de la dilación). Los encargados están obligados a notificar al responsable sin demora indebida cualquier incumplimiento en el que hayan incurrido. Es conveniente identificar aquellas categorías de datos cuya afectación puede activar el requisito de notificación.

El RGPD (UE) 216/679 y la LOPDGDD 3/2018, define las violaciones de seguridad de los datos, más comúnmente conocidas como "quiebras de seguridad", de una forma muy amplia, que incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

Obligaciones:

Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.

La notificación ha de incluir un contenido mínimo:

- La naturaleza de la violación.
- Las categorías de datos y de interesados afectados.
- Las medidas adoptadas por el responsable para solventar la quiebra.
- Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Los responsables deben documentar todas las violaciones de seguridad.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos.

El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD (UE) 216/679 y la LOPDGDD 3/2018, requieren que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.

El RGPD (UE) 216/679 y la LOPDGDD 3/2018, añaden a los contenidos de la notificación las recomendaciones sobre las medidas que pueden tomar los interesados para hacer frente a las consecuencias de la quiebra.

A tener en cuenta

La valoración del riesgo de la quiebra es distinta del análisis de riesgos previo a todo tratamiento: Se trata de establecer hasta qué punto el incidente, por sus características, el tipo de datos a los que se refiere o el tipo de consecuencias que puede tener para los afectados puede causar un daño en sus derechos o libertades.

Los daños pueden ser materiales o inmateriales, e ir desde la posible discriminación de los afectados como consecuencia de su uso por quien ha accedido a ellos de forma no autorizada hasta usurpación de identidad, pasando por perjuicios económicos o la exposición pública de datos confidenciales.

Se considera que se tiene constancia de una violación de seguridad cuando hay una certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance.

La mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.

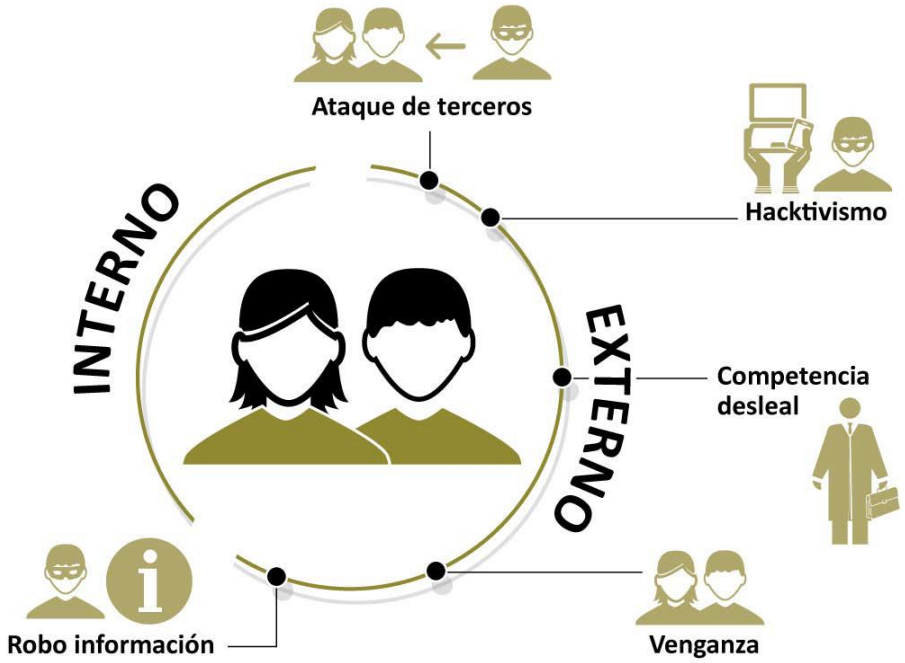
En casos de quiebras que por sus características pudieran tener gran impacto, sí podría ser recomendable contactar con la autoridad de supervisión tan pronto como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

Puede haber casos en que la notificación no pueda realizarse dentro de esas 72 horas, por ejemplo, por la complejidad en determinar completamente su alcance. En esos casos, es posible hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso.

La información puede proporcionarse de forma escalonada cuando no sea posible hacerlo en el mismo momento de la notificación.

El criterio de alto riesgo debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños de entidad a los interesados. Por ejemplo, en casos en que se desvele información confidencial, como contraseñas o participación en determinadas actividades, se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

Posible origen



- Origen interno: dentro de este punto incluimos las fugas de información ocasionadas por el personal de la asociación, 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").

- 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 la asociación o los socios y/o asociados tratados.

  - La venganza de socios y/o asociados descontentos o de antiguos empleados.

  - El robo de información confidencial: el acceso no consentido a información privilegiada de socios y/o asociados 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 a la imagen de la asociación.

  - Otros cuyo objetivo es realizar actividades de competencia desleal.

Prevención

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.

- 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 integrantes de la asociación, quienes, por un lado, deben utilizar los recursos que la organización 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.

Además, hay que tener en cuenta que la legislación laboral permite establecer límites a las actividades de sus trabajadores, ofreciendo canales para ayudar a los empresarios a evitar un uso inadecuado o malintencionado de la información de la que es responsable la asociación.

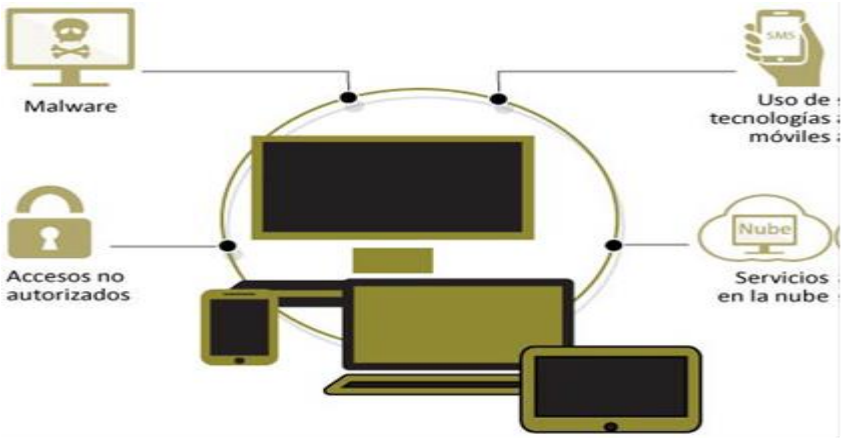
- Dentro de las causas técnicas podemos destacar:

  - 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 asociación -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.



¿Cómo mitigamos la fuga de información? El principio del mínimo privilegio

Visto que el factor humano es uno de los principales motivos de fugas de información, realizaremos campañas de concienciación en materia de ciberseguridad dentro de la asociación, 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 desarrollamos actualizadas políticas claras y completas de acceso a la información, 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 de la asociación 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 la asociación. 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 asociación?

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.

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 lo 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 la asociación 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.

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.

No todas las organizaciones cuentan con un gabinete de crisis o tienen los recursos necesarios. Pero eso no obsta a que cada organización deba adaptarse a la gestión del incidente con los recursos con los que pueda disponer. 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 asociación, 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.

Fase de auditoría

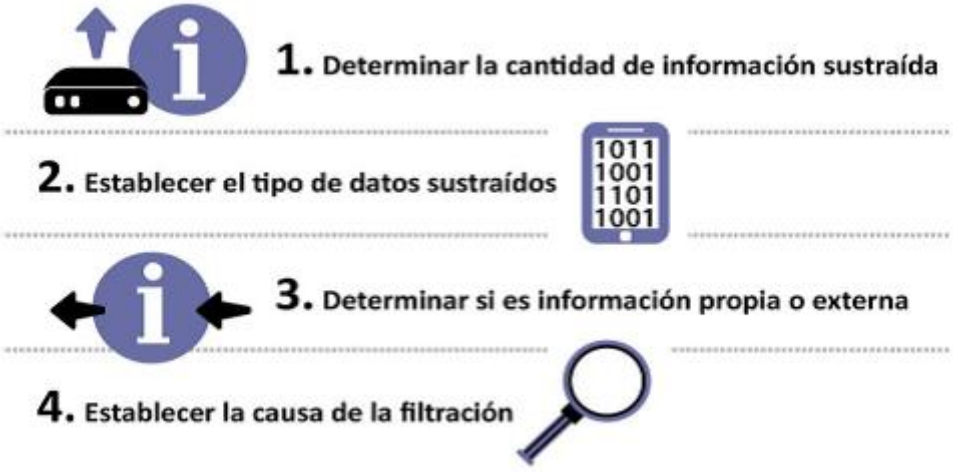
Una vez se han iniciado los pasos anteriores, daría comienzo la fase de obtención de información sobre el incidente. Para ello, será necesario iniciar una auditoría interna, con el objetivo de determinar con exactitud y en el menor tiempo posible lo siguiente:

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

- 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.

- Determinar si la información pertenece a la propia organización 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 organización, con especial consideración a los datos de nuestros socios y/o asociados.

- 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:

- 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.

- 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, 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.

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 con agilidad.

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

- 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.

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 normativa vigente en Protección de Datos.

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.

En caso de existir personas afectadas por la fuga de información, por ejemplo, si se han filtrado datos personales de terceros, como de socios de la asociación, 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. Todo ello sin perjuicio de las eventuales obligaciones de informar al correspondiente Colegio de Abogados si se considerase necesario en virtud de la gravedad del incidente o de la cantidad o calidad de los datos afectados.

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.

9. MEDIDAS Y NORMAS DE SEGURIDAD DE LAS QUE SE DISPONE

Este documento ha sido diseñado para el tratamiento de datos personales no incluidos entre los denominados de alto riesgo (relativos al origen étnico o racial, ideología política religiosa o filosófica, filiación sindical, datos genéticos y biométricos, datos de salud, y datos de orientación sexual de las personas así como cualquier otro tratamiento de datos que entrañe alto riesgo para los derechos y libertades de las personas).

El artículo 5.1.f del RGPD (UE) 216/679 determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad (artículo 5.2) de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

A tenor de las características del tratamiento de los datos manejados por la asociación, las medidas mínimas de seguridad que a tener en cuenta son las siguientes:

MEDIDAS ORGANIZATIVAS

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de los mismos y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

- DEBER DE CONFIDENCIALIDAD Y SECRETO

  - Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público o en soportes con datos personales, etc.).
    Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.

  - Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) las 24 horas del día.

  - No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.

  - No se comunicarán datos personales o cualquier información personal a terceros y se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.

  - El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la asociación.

- DERECHOS DE LOS TITULARES DE LOS DATOS

  - Se informará a todos los trabajadores y voluntarios si los hubiera, acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) teniendo en cuenta lo siguiente:
    - Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión y portabilidad de sus datos, y los de limitación u oposición a su tratamiento. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.

- Para el derecho de acceso se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar sus derechos.
- Para el derecho de rectificación se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.
- Para el derecho de supresión se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.
- Para el derecho de portabilidad los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.

El responsable del tratamiento ha informado a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

- VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL

Cuando se produzcan violaciones de seguridad de datos de carácter personal, como por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en el plazo de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales.

La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

MEDIDAS TÉCNICAS

- IDENTIFICACIÓN

  - Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se dispondrá de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.

- Cuando a los datos personales accedan distintas personas, para cada una de ellas se dispondrá de un usuario y contraseña específicos (identificación inequívoca).

- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

➢ DEBER DE SALVAGUARDA

- ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la medida de lo posible.

- MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida de lo posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.

- CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

- CIFRADO DE DATOS: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

- COPIA DE SEGURIDAD: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los datos originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, y esta revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual.

- Medidas y normas de comunicación al personal involucrado:

Los empleados actuales de la entidad han sido informados personalmente de las medidas y normas aplicables en materia de seguridad. Para quedar constancia de la comunicación y aceptación, han firmado el anexo en conformidad (documento "ANEXOS" que complementa el presente documento) a su entendimiento de las normas de seguridad que aplican individualmente según las funciones asignadas y descritas en este documento.

Adicionalmente para cumplir los requisitos que exige el marco legal vigente, todos los empleados han firmado una carta de confidencialidad y responsabilidad que se anexan a este documento, tal como marcan sus funciones (también incluida en el documento "ANEXOS").

Todos los empleados en el proceso de incorporación y promoción son informados de los accesos de que disponen a datos confidenciales y se les proporciona el Registro Interno de Actividades de Tratamiento para su entendimiento y aceptación. Una vez aceptado deben firmar el anexo correspondiente al entendimiento de las normas de seguridad conjuntamente con la carta de confidencialidad que se describe posteriormente.

- Entrada, salida y circulación de datos.

Seguidamente detallamos la política que determina la entrada, salida y circulación de datos de carácter personal.

Cualquier modificación sobre los procedimientos detallados a continuación requerirá la autorización expresa y por escrito de los encargados del tratamiento, tratamiento y seguridad, que incluirá dichas modificaciones y sus efectos en el registro de incidencias.

- Sistema de entrada y captación de datos: Mediante tarjetas de visita, documentos comerciales, formularios, entrevista y/o proporcionados directamente por los socios y/o asociados, proveedores o empleados. Asimismo se consideran los siguientes puntos:

- Cuando el objeto de los datos sea efectuar un tratamiento por cuenta de un tercero se formalizará un contrato con los requisitos y responsabilidades que especifica la reglamentación vigente para poder autorizar la incorporación de dichos datos.
- En caso de datos proporcionados por otros colectivos y/o empresas, será necesario que nos confirmen documentalmente el origen de los datos que nos facilitan, que están legalizados y poseen autorización de los afectados a la cesión que están efectuando y el destino y uso al que estamos autorizados a realizar sobre los datos cedidos.

- Notificación: Se comunicará por escrito, en caso de ser necesario legalmente, que los datos que se han recopilado, forman parte de un sistema de tratamiento y se le notificará sus derechos como afectado, la dirección de acceso y las funciones y usos del sistema.

- Acceso informático: El personal con acceso al sistema de tratamiento informático dispondrá de una contraseña de acceso, que se regirá por la política de contraseñas descrita en el presente documento.

- Salida y/o envío de soportes informáticos y físicos con datos de carácter personal:

  La salida y/o envío de dichos soportes, como son copias de seguridad, copias parciales de archivos con datos de carácter personal y listados será autorizada por escrito por el encargado del tratamiento y el encargado de seguridad cuando sea necesaria dicha salida. En el caso de que la salida de datos sea para que un tercero efectúe un tratamiento (nómina, mailing, impuestos y similares) se formalizará un contrato con los requisitos y responsabilidades que especifica la reglamentación vigente (incluido en documento "ANEXOS" que complementa el presente documento).

  En caso de querer efectuar cesión a terceros de los datos del sistema de tratamiento, dicha cesión requerirá la autorización de los afectados si no se trata de un sistema público y se formalizará documentalmente dicha cesión indicando que poseemos la autorización de los afectados, la procedencia de los datos que cedemos, los usos y finalidades sobre los que están autorizados a realizar con dichos datos y el deber que tienen de tratar dichos datos conforme a todas las obligaciones que el RGPD especifica.

- Consentimiento: Se solicitará el consentimiento expreso y explícito para la inclusión y conservación de datos de carácter personal en sistemas de tratamiento de la entidad en aquellos casos que el uso de los mismos sea de carácter amplio y en especial en aquellos casos que lo exija la legislación vigente. El encargado del tratamiento es el encargado de desarrollar y recopilar los mecanismos y sistemas necesarios para cumplir el objetivo anterior.

- Contraseñas y login de las aplicaciones: Sólo el encargado del tratamiento tiene acceso a las tablas maestras de contraseñas. Como norma una vez instalada una aplicación se cambiarán las contraseñas asignadas por el fabricante y/o instalador.

  Cada semestre o como mínimo anualmente, cambiará todas las contraseñas del personal con acceso a datos.

  La comunicación de la nueva contraseña se realizará personal e individualmente. Se activará en tres intentos la presentación de limitación de intentos erróneos de acceso a la red y recursos instalados.

  El encargado del tratamiento documentará todos los cambios efectuados en el informe periódico.
  Siempre que el sistema lo permita se cerrará la sesión de trabajo cuando sea preciso ausentarse del lugar del trabajo no dejando ninguna aplicación abierta.

- Acceso al ordenador: Se restringirá dicho acceso mediante contraseñas tanto en la BIOS de los puestos como en el acceso al inicio de sesión como usuario registrado y, en caso de no ser usado el puesto más de 10 minutos, se activará el salva pantallas y para su desactivación será necesario la introducción del usuario y de la contraseña.

- Control de software de acceso a los datos: El control mediante contraseñas permitirá al encargado del tratamiento:
  - Asignar permisos de acceso a cada sistema de tratamiento o programa desde cada puesto de trabajo.
  - Restringir la ejecución de programas o accesos directos.
  - Registrar usuario, fecha y hora de cada acceso autorizado así como los intentos de acceso no autorizados.
  - Restringir accesos de sistema y programas
  - Control de cambio de contraseñas

- Informes:
  - Registros de accesos durante el tiempo que se quiera.
  - Consulta de archivo LOG del sistema, donde residen todas las tareas realizadas para cada usuario.
  - Permite registrar las incidencias que afecten a la seguridad de los datos.

- Registro de acceso a los datos:
  Para el registro de acceso utilizaremos la aplicación con contraseñas la cual permite al Responsable de Tratamiento de los datos:
  - Asignar permisos de acceso a cada sistema de tratamiento o programa desde cada puesto de trabajo.
  - Restringir la ejecución de programas o accesos directos.
  - Registrar usuario, fecha y hora de cada acceso autorizado así como los intentos de acceso no autorizados.
  - Restringir accesos de sistema y programas Windows.
  - Control de cambio de contraseñas.
  - Registro de acceso durante el tiempo que se quiera.
  - Consulta de archivo LOG del sistema, donde residen todas las tareas realizadas por cada usuario.
  - Permite registrar las incidencias que afecten a la seguridad de los datos protegidos.

- Encriptación de archivos:
  - Bloqueo de archivos o carpetas para el envío telemático de información que contenga datos de carácter personal.
  - Puede generar contenedores de archivos comprimidos que incluyen grupos de archivos con estructura de carpetas y subcarpetas, cifrando y preservando su contenido.

- Antivirus:
  Utilizaremos un sistema de antivirus que integra la detección de virus así como el Firewall, para control de acceso desde Internet.
  Con el antivirus tendremos nuestros ordenadores protegidos automáticamente de todo tipo de virus, gusanos y troyanos, así como posee una actualización automática de las firmas de virus que se hará diariamente y automáticamente.
  Sus características técnicas se detallan en el documento "ANEXOS" que complementa el presente documento.
  - Firewall personal: Bloquea la entrada de hackers o intrusos a nuestros equipos, dando mayor seguridad a nuestro sistema. Además con este antivirus tendremos protegido nuestros ordenadores contra estafas on-line, Spyware o espías.

10. DATOS SOBRE COPIAS DE SEGURIDAD

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, con una periodicidad semanal en los soportes detallados en el documento "ANEXOS" que complementa el presente Registro Interno.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizan su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

11. CONTROLES Y PERIODICIDAD DE VERIFICACIÓN

Cada 12 meses se realizará una revisión de los sistemas de seguridad y las incidencias que hubiese en ese período de tiempo.

Cada 24 meses se realizará una auditoría, interna o externa, donde se verificará el correcto funcionamiento de todas las medidas de seguridad y se incluirán los cambios referidos a:

- Notificación de incidencias
- Alta y bajas de personal autorizado
- Altas y bajas de sistemas de tratamiento de datos y su notificación a la A.E.P.D.
- Gestión, destrucción e inventariado de soportes.
- Cambio o modificación de los sistemas de tratamiento.

Obligaciones del Responsable de Tratamiento:

- Ejecutar comprobaciones y obtener la información, soporte y actualizaciones necesarias para garantizar la eficacia de las medidas de seguridad con el conocimiento de las incidencias detectadas y de los cambios que se produzcan en el entorno tecnológico y legal. Incluirá estas acciones en los informes periódicos.

- Al objeto de adaptar medidas críticas de seguridad comprobará la eficacia del registro de incidencias verificando la inclusión de los hechos más relevantes como:
  - Altas / bajas de personal.
  - Cambio de funciones y/o responsabilidades.
  - Errores de hardware y/o software.
  - Incidencias en los equipos/dispositivos de comunicación
  - Modificaciones o cambios de software.
  - Altas/bajas de ubicación.
  - Salidas externas de los datos o soportes del sistema de tratamiento.

En caso de no estar recogidas las incluirá en el registro y adoptará las medidas de seguridad que procedan y/o concluirá sobre los posibles efectos.

- Semestralmente o cuando se produzcan hechos de relevancia significativa elaborará un informe donde documentará las recomendaciones, conclusiones y acciones realizadas según sus funciones detalladas anteriormente, de Medidas de Seguridad. Este informe se pondrá a disposición del encargado del tratamiento.

12. PROCEDIMIENTO PARA LA ELIMINACIÓN DE DATOS

Nunca se utilizarán como mecanismo de eliminación, sin destruir los papeles y soportes de datos, los sistemas de papeleras y residuos, ya que éstos tienen que ser destruidos de forma que queden totalmente ininteligibles.

Solamente el encargado de seguridad puede eliminar y/o autorizar la destrucción de soportes/equipos informáticos.

Cuando se decida que un soporte o equipo informático que contenga información deja de ser útil, operativo y por tanto pueda proceder a su sustitución y/o eliminación, se efectuarán los siguientes pasos:

- El usuario lo comunicará al encargado de seguridad y será incluido al registro de incidencias.

- El encargado de seguridad autorizará su destrucción y se asegurará de eliminar la información y/o destruir el soporte/equipo. Incluirá la acción y las medidas de seguridad adoptadas en el registro de incidencias y en el informe periódico.

13. SISTEMAS OPERATIVOS

Los ordenadores utilizan diferentes sistemas operativos que incluyen nuevas características incluyendo:

- Secuencias más rápidas de inicio y de hibernación.

- Capacidad del sistema operativo de desconectar un dispositivo externo sin necesidad de reiniciar.

- Una nueva interfaz de uso más fácil, incluyendo herramientas para el desarrollo de temas de escritorio.

- Uso de varias cuentas, lo que permite a un usuario que guarde el estado actual y aplicaciones abiertas en su escritorio y permita que otro usuario abra una sesión sin perder esa información.

- Soporte de la mayoría de módems ADSL y conexiones Wireless, así como el establecimiento de una red FireWire.

- Los sistemas operativos están actualizados con la última versión disponible de Service Pack, incluyendo así todas las correcciones encontradas en anteriores Service Pack, además de varias novedades centradas sobre todo en dar mayor seguridad en el sistema operativo, siendo algunas de las novedades ya incluidas:

    - Un centro de seguridad, para comprobar el riesgo al que está sometido sistema operativo. Interfaz del Cortafuegos de sistema operativo, además de ser activado por defecto.

    - Importación a los navegadores de acceso a internet instalados, de un bloqueador de ventas emergentes, la capacidad de bloquear ActiveX, el bloqueo de las descargas automáticas y un administrador de complementos.

    - Las actualizaciones automáticas de los sistemas operativos, están activadas por defecto.

    - El programa de gestión de correo bloquea los archivos adjuntos potencialmente peligrosos (.exe o .vbs).