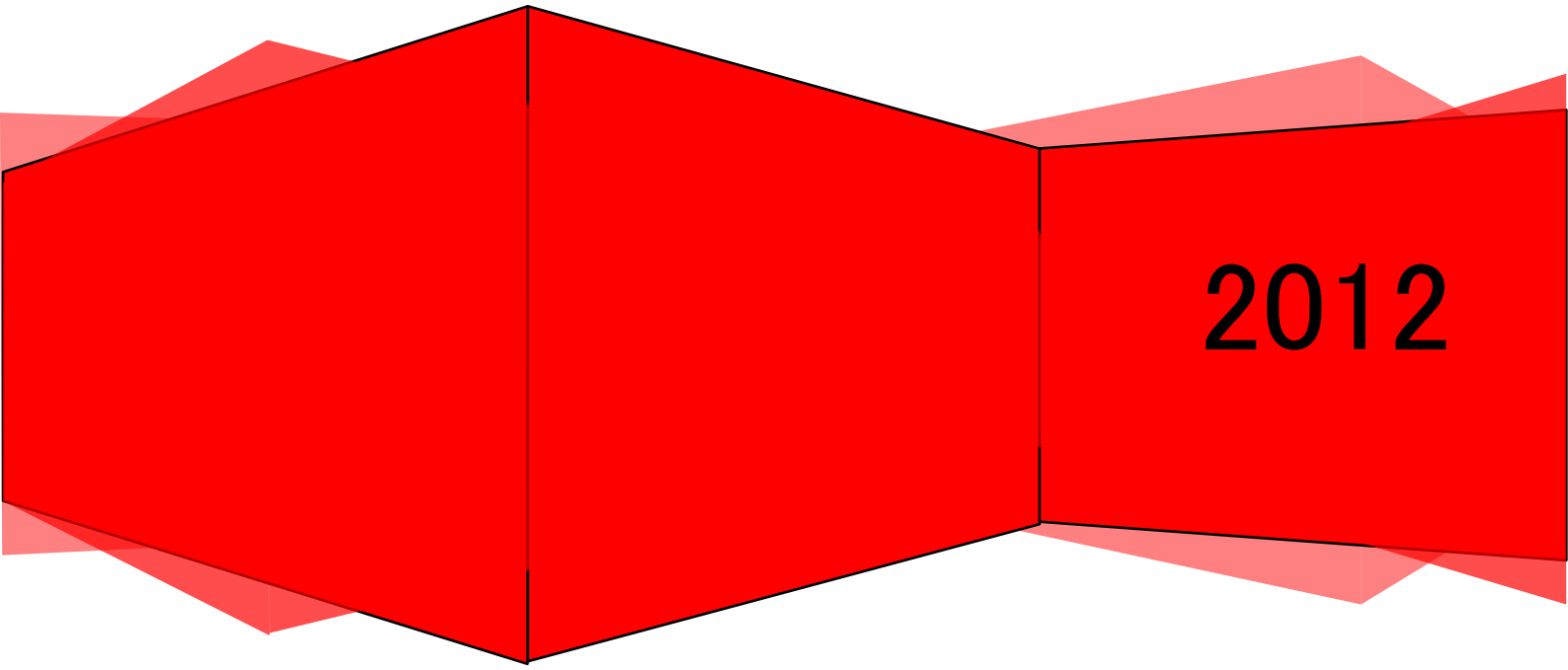
SAF Asesores

POLÍTICA DE SEGURIDAD SOBRE PROTECCIÓN DE DATOS PERSONALES



A. POLÍTICA DE SEGURIDAD SOBRE FICHEROS AUTOMATIZADOS

La Ley Orgánica de Protección de Datos (LOPD) trata de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

Para garantizar que el uso, tenencia y tratamiento de datos personales contenidos o recogidos en los ficheros de las empresas de **ANA RODRÍGUEZ MADRERA (SALÓN LA XANA)**, se ajusta a las exigencias de la LOPD, se han implantado las siguientes normas que usted debe de conocer y, en la medida en la que le afecte, cumplir.

A.1 Acerca del control de acceso a la información automatizada

1) Los equipos informáticos mediante los cuales se acceda a los ficheros de datos personales, deberán tener su acceso restringido mediante un código de usuario y una contraseña.

2) Todos los usuarios con acceso a los ficheros de datos personales deberán de quedar reflejados en el Anexo I del Documento de Seguridad de cada empresa (Relación de Personal Autorizado). Sólo las personas relacionadas en dicho anexo podrán tener acceso a los datos de los ficheros.

3) Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo I del documento de seguridad.

4) Todos los usuarios autorizados para acceder al Fichero, relacionados en la Relación de Personal autorizado, deberán tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

5) En función de las posibilidades técnicas, se limitará el acceso de cada usuario al mínimo conjunto de recursos que necesite para desempeñar su trabajo, configurando de manera adecuada la aplicación y/o el sistema operativo. Deben de existir perfiles de usuario de modo que los usuarios dispongan de acceso exclusivamente a la información que precisan para el desarrollo de sus funciones.

6) En los ficheros de nivel alto (que contienen datos personales de salud, creencias, ideología,…), se guardará en un registro de accesos la identificación del usuario, fecha y hora en la que se realizó el acceso, el fichero accedido, el tipo de acceso y si éste ha sido autorizado o denegado. En caso de haber sido autorizado se guardará información que permita identificar el registro accedido. Los datos de este registro deberán conservarse al menos durante dos años. Los mecanismos de registro de estos datos de acceso no podrán ser desactivados en ningún caso, y estarán siempre bajo control del responsable de seguridad competente.

7) El responsable de seguridad revisará periódicamente la información de control registrada en el registro de accesos, y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

A.2 Acerca de las copias de seguridad y la gestión de soportes magnéticos

1) Los administradores de los ficheros de datos personales (Personal de Informática), serán responsable de obtener periódicamente una copia de seguridad de los ficheros de datos, a efectos de respaldo y posible recuperación en caso de fallo. Estas copias de seguridad deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

2) Los soportes destinados a copias de seguridad seguirán todas las normas definidas para la gestión de soportes (identificación, reutilización y eliminación, etc.), debiendo de quedar reflejados en el Inventario de Soportes que acompaña al Documento de Seguridad. Se evitará desgastar en exceso los soportes donde se realizan las copias de seguridad, rotándolos y renovándolos de forma periódica transcurridos un número determinado de grabaciones o un periodo de tiempo largo.

3) Los usuarios que deseen realizar copias de seguridad adicionales de determinados archivos o documentos (además de las realizadas por los administradores), deberán de solicitar autorización al Responsable de Seguridad o al Personal de Informática, quienes se encargarán de la realización de las copias.

4) En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo.

5) Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación. El formulario para notificar una incidencia se encuentra en la sección 12.5.

6) La salida de soportes informáticos que contengan datos de los ficheros fuera de los locales donde está ubicados los ficheros deberá ser expresamente autorizada por el responsable de los

ficheros. El procedimiento y formulario para la salida de soportes se encuentra indicado en el Documento de Seguridad.

7) El responsable del Fichero mantendrá un Libro de registro de entradas y salidas donde se guardarán los formularios de entradas y de salidas de soportes descritos en el capítulo 12 del Documento de Seguridad, con indicación de tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío, destinatario, o persona responsable de la recepción que deberán estar debidamente autorizadas. El procedimiento y formulario para la entrada de soportes se encuentra en la sección 12.4 del Documento de Seguridad.

A.3 Acerca del correo electrónico y envíos de información

En particular, serán especialmente perseguidas las siguientes prácticas catalogadas como abuso del correo electrónico:

a. La difusión de contenido ilegal; como por ejemplo amenazas, código malicioso, apología del terrorismo, pornografía infantil, software pirata, o de cualquier otra naturaleza delictiva.

b. El uso no autorizado de servidores propiedad de la empresa para el envío de correo personal.

c. El envío de correos publicitarios o de cualquier otro tipo que no guarde relación alguna con las necesidades de negocio de la empresa. Este hecho, además, puede llegar a ser interpretado como "spamming". Para el envío de correo electrónico a grupos de empleados de la empresa se utilizará la opción de Copia Oculta (CCO)

d. El envío indiscriminado de correos con intención de imposibilitar o dificultar el servicio de correo de la empresa o de entidades externas.

Todas las comunicaciones de datos personales a terceros se realizarán siempre atendiendo a los supuestos legales que marca la LOPD. El empleado que deba realizar una cesión de datos de carácter personal solicitará previamente autorización al Responsable de Seguridad de la entidad, para que le informe si está dentro de las cesiones consentidas.

A.4 Acerca de la gestión de incidencias y los soportes documentales

1) Los administradores del Fichero (Personal de Informática), con periodicidad al menos trimestral, comunicarán al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los sistemas, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos datos en el Anexo II del Documento de Seguridad y resto de documentos.

2) También se comprobará, con igual periodicidad, que las configuraciones hardware y software de los puestos documentadas se corresponden con las existentes en la realidad, verificando que no se hayan instalado programas sin autorización. Se hará hincapié en verificar que no hay instalados programas especiales como herramientas de utilidad que permitan el acceso no controlado a los ficheros de datos.

3) Igualmente deberá de comprobarse, con periodicidad al menos trimestral, que efectivamente no se están almacenando documentos con datos personales en los PC de usuario de manera no autorizada, debiendo estos de ser almacenados de forma centralizada en los equipos servidores. De igual manera se comprobará que se eliminan los ficheros temporales, tanto en los PC de usuario como en el servidor.

4) El responsable de seguridad del Fichero comprobará trimestralmente que la lista de usuarios autorizados del Anexo I se corresponde con la lista de los usuarios realmente autorizados en las aplicaciones de acceso a los ficheros, para lo que recabará la lista de usuarios de las aplicaciones y sus identificadores al administrador o administradores del Fichero. De igual manera, comprobará que los niveles de acceso de cada usuario se corresponde con las medidas técnicas habilitadas para limitar este acceso (restricción de funciones de las aplicaciones, configuración de permisos de carpetas, etc.).También comprobará que se realizan de manera adecuada los procedimientos de gestión de usuarios y contraseñas, especialmente la renovación periódica de las contraseñas. Además de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

5) Al menos cada dos años, se realizará una auditoria, externa o interna, que dictamine el correcto cumplimiento de la LOPD, así como la adecuación de las medidas de seguridad indicadas en los

Reglamentos de Desarrollo de la Ley, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoria serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

6) El responsable de seguridad de la entidad habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

7) Si usted, como usuario, detectase el incumplimiento de alguna de las medidas de seguridad expuestas, deberá de comunicar la incidencia al Responsable de Seguridad, a través de los medios puestos a su disposición para ello, de modo que pueda procederse al registro de la incidencia en el Libro correspondiente, para su posterior gestión.

B. POLÍTICA DE SEGURIDAD SOBRE FICHEROS NO AUTOMATIZADOS

1) El uso y tratamiento de datos personales recogidos en soporte físico (papel) deberá estar justificado por el cumplimiento de finalidades lícitas y legítimas. Únicamente el personal autorizado para ello podrá disponer de acceso a la documentación en soporte papel en la que figuran datos de carácter personal siempre que dicho acceso sea necesario para el desarrollo de las funciones asignadas por la empresa. Deberá de existir una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos (Anexo I del Documento de Seguridad).

2) En lo que respecta a la conservación, los documentos en soporte papel generados por el personal de la empresa, únicamente se conservarán cuando resulten necesarios para el desarrollo de las funciones profesionales que les han sido encomendadas, cuando en ellos se almacene información que resulta de interés y no se encuentra digitalizada, o cuando existe obligación legal de custodia.

3) Los documentos que contengan datos personales, deberán de ser archivados de manera que se permita la correcta conservación de los documentos, la localización y consulta de la información, y que permitan la posibilidad del ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. Asimismo, los soportes que contengan los documentos en papel (archivadores, AZ's, carpetas,…) deberán de almacenarse de modo que se permita identificar el tipo de información que contiene, debiendo estos de ser etiquetados e inventariados.

4) Tratándose de documentos en los que figuren datos de carácter personal especialmente protegidos (datos de salud, principalmente) éstos se almacenarán en archivadores cerrados con llave o situados en salas cerradas con llave, impidiendo el acceso a los mismos por parte de personal no autorizado.

5) Siempre que los documentos con datos personales no estén archivados, la persona que esté utilizando el documento, deberá de custodiarla y encargarse de asegurar la confidencialidad y la integridad de los datos que contiene, impidiendo el acceso a dicho documento a usuarios no autorizados.

6) Los datos personales recogidos en soporte papel deben mantenerse exactos y puestos al día de forma que el personal responsable de los mismos, en caso de comprobar la desactualización de

alguno de ellos, deberá proceder a su corrección y actualización, dejando constancia escrita del alcance y la fecha en que ha tenido lugar.

7) En lo que respecta a la destrucción de la documentación en soporte papel, no se mantendrán, bajo ningún concepto, datos personales en soporte papel cuando los mismos ya no sean útiles ni necesarios para el fin que justificó su recogida y conservación. En este supuesto se procederá a su destrucción física, utilizando cualquier sistema que impida la reconstrucción de los datos en ellos contenidos (por ejemplo, máquinas destructoras de papel). No obstante, podrá ser conservada aquella documentación e información que sirva como justificante de una actividad o servicio y/o durante los plazos de prescripción de las acciones civiles, penales, administrativas o de cualquier otro tipo que pudieran derivarse de la actividad o servicio prestado.

8) En lo que respecta a la comunicación, en principio, no se comunicarán, intercambiarán o cederán, en todo o en parte, los datos personales recogidos en soporte físico a terceros, salvo que exista una ley que autorice expresamente la cesión o que ésta sea necesaria para el desarrollo de las funciones encomendadas.

9) Cuando sea necesario proceder a realizar envíos, cesiones, préstamos, intercambios, copias o fotocopias, así como entregas, totales o parciales, de los datos personales recogidos en soporte papel, dichos actos deberán ser expresamente autorizados por el Responsable de Seguridad o la persona o personas en quienes delegue, quienes se encargarán de almacenar un registro de las entradas y salidas de documentos para una correcta gestión de estos intercambios de información.

10) El personal que utilice y trate datos personales recogidos en soporte papel estará obligado a velar por la confidencialidad y privacidad de los mismos, debiendo guardar secreto respecto de los mencionados datos y garantizar el cumplimiento de las medidas de seguridad de las que haya sido informado.