



MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD Y DEL MEDIO AMBIENTE

P421. Requisitos de la Documentación. Documento de Seguridad (LOPD).

Nº revisión: 13

Fecha: diciembre 2011

APROBADO: Dirección

Índice

1. Objeto.

2. Alcance.

4. Responsabilidades.

5. Método operativo.

5.1. Mantenimiento.

5.1.1. Datos.

5.2. Protección Medioambiental

5.2.1. Normas generales.

5.2.2. Normas generales de orden y limpieza.

5.3. Control de los Documentos y de los Registros del SIG.

5.3.1. Responsabilidades.

5.3.2. Asignación y descripción de las funciones y responsabilidades.

5.3.3. Identificación de los documentos del SIG.

5.3.4. Aprobación de los documentos.

5.3.5. Revisión y actualización de los documentos.

5.3.6. Identificación del estado de revisión actual y de los cambios de los documentos.

5.3.7. Distribución de la documentación.

5.3.8. Otra documentación y datos externos.

5.3.9. Copias controladas.

5.3.10. Control, protección y acceso a los documentos y a los registros.

Documentación aplicable

P800 Gestión de la Mejora: Reclamaciones, Incidencias, Sugerencias. Auditorías Internas

P740 Gestión de Compras y Subcontrataciones

R06 Incidencias en servicios

R10 Informe Diario de Trabajo (Sistemas)

R19 Parte Diario de Servicio

R20 Solicitud de Pedido a Central

R33 Ficha de Control de Vehículos

R48 Recibí Entrega de Vestuario

R49 Inventario Almacén Uniformidad

R50 Salida de Almacén

R56 Inventario Almacén Sistemas

I04 Comunicación Externa

I07 Control de Consumos. Gestión de Residuos.

Revisión	Fecha	Objeto de la revisión
01	FEB 2005	Redacción Inicial



02	FEB 2006	Modificación y creación de diferentes formatos
03	MAR 2006	Creación de diferentes formatos
04	DIC 2007	Nueva redacción
05	JUN 2007	Unificación de varios procedimientos
06	JUN 2008	Integración Protección de Datos. Adecuación al RD 1720/2007
07	FEB 2009	Inclusión Control de Documentos
08	JUN 2009	Adecuación a norma ISO 14001
09	ENE 2010	Eliminación del R70 Documento de Seguridad e integración del mismo en este procedimiento.
10	FEB 2010	Inclusión de fichero LOPD "PRL - Coordinación de Actividades Empresariales"
11	MAY 2010	Modificación de aplicaciones gestión ficheros con datos personales.
12	ABR 2011	División del procedimiento en P421 y P631.
13	DIC 2011	Cambio en la denominación de los procedimientos.



1. Objeto.

- El objetivo del presente procedimiento es definir el método seguido para garantizar la disponibilidad, conservación, custodia y mantenimiento de la información, medios y documentos que afectan a los datos (incluidos los de carácter personal) custodiados por COVIAR.
- Asimismo, regular y proteger la actividad diaria de la empresa afectada por la normativa sobre Protección de Datos de Carácter Personal, especialmente el acceso a los datos de los Ficheros relacionados directamente con la gestión de la propia empresa y para uso de la misma.
 - El incumplimiento de las normas establecidas en este documento es constitutivo de infracción laboral cuya gravedad se gradúa en función de la importancia del incumplimiento.
 - Las infracciones tipificadas en este documento se sancionarán con arreglo a las sanciones reguladas en el vigente Convenio Colectivo aplicable a la empresa.
- Establecer criterios de buenas prácticas ambientales, con el fin de conseguir un lugar de trabajo limpio y seguro en todas las instalaciones de la empresa.
- Establecer y mantener los registros para proporcionar la evidencia de la conformidad con los requisitos, así como de la operación eficaz.

2. Alcance.

El presente procedimiento se aplica a toda la información (incluidos los datos de carácter personal) gestionados por COVIAR que afecten a los servicios prestados.

3. Definiciones.

A continuación se indican algunas definiciones básicas cuyo conocimiento es imprescindible para la correcta aplicación de las obligaciones contenidas en el presente documento:

- **Datos de carácter personal:** cualquier información concerniente a personas físicas identificadas o identificables. La definición anterior incluye todo tipo de información, ya sea numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión.
- **Fichero:** todo conjunto organizado de datos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso (ya sea en soporte papel o en soporte electrónico). En todo caso, para que un fichero pueda calificarse como de datos personales, deberá contener algún dato de carácter identificativo de la persona.
- **Tratamiento de datos:** operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos a personas ajenas a la organización o a otras empresas, incluso que formen parte del mismo grupo empresarial, las cuales resulten de comunicaciones, consultas, interconexiones y transferencias.
- **Responsable del Fichero o tratamiento:** persona física o jurídica que decida sobre la finalidad, contenido y uso del tratamiento. Respecto de los ficheros de datos de carácter



personal utilizados en la empresa, es ésta (COVIAR) quien asume tal condición.

- **Responsable de Seguridad:** es la persona designada por el Responsable del fichero encargada de coordinar y controlar las medidas definidas en este Documento de Seguridad.
- **Responsable de Departamento o Delegación:** es la persona responsable del Departamento o Delegación en que está incardinado el usuario, la cual, de acuerdo con su jerarquía en la organización, asume ciertas obligaciones en la gestión de los procedimientos en materia de datos personales.
- **Usuario:** es la persona que accede habitualmente, o puede acceder, a los datos personales contenidos en los ficheros. Asumen especiales obligaciones en materia de seguridad, según se indica en este Documento y en el Sistema Integrado de Gestión (Calidad y Medio Ambiente) de la empresa.
- **Documento de Seguridad:** es este mismo documento, donde se plasman las medidas de seguridad, de índole técnica y organizativa, que deben aplicarse a los ficheros de datos de carácter personal.

4. Responsabilidades.

Descripción	Custodia, Tratamiento	Inventario, Mantenimiento
Registro de datos	• Personal designado • Responsable Fichero	Responsable Fichero (COVIAR)
Tratamiento de datos		
Seguridad de datos		
Equipamiento informático	Todo el personal afectado	Responsable de Seguridad
Cumplimiento de los requisitos definidos en este procedimiento	Todo el personal afectado	Todo el personal afectado



5. Método operativo

5.1. MANTENIMIENTO.

5.1.1. Datos

Según LOPD, la responsabilidad sobre la información y los datos manejados por la empresa, así como sobre los Ficheros de Carácter Personal y su tratamiento es en todo momento de COVIAR., que con carácter general se encarga de coordinar y controlar las medidas definidas en este documento.

Almacenamiento de soportes. Copia de información en soporte electrónico.

Todos los datos se almacenan según el nivel de seguridad que requiere cada fichero, según este documento, de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

Los soportes se almacenan en lugares a los que sólo tienen acceso las personas autorizadas para el uso de los datos que contengan. Como medida general, se evitarán los cajones sin llave de cierre, superficie de mesas de trabajo y, en general, lugares accesibles o manipulables por terceros. Por otra parte, no se permite la existencia de soportes fuera de los lugares previstos para su custodia cuando no sean utilizados.

Se permite la copia de información en soporte electrónico en los siguientes casos:

- Por necesidades justificadas de trabajo.
- Necesidad de proporcionar los datos a una empresa prestadora de servicios. En este caso, será requisito previo la existencia de un contrato que habilite dicha salida de datos.
- Realizar una captura de información para un determinado proyecto, debidamente aprobado por una persona autorizada.
- Por imperativo legal o resolución judicial.

Copias de seguridad (copias de respaldo)

Copia de respaldo o de seguridad es una copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Se realiza copia de seguridad diaria en red local (LAN), red de área extensa (WAN) o TCP/IP sobre VLAN (NETLAN) de Telefónica, sistema operativo Microsoft Windows, con copia sobre cinta y en RAID 0 (también llamado conjunto dividido o volumen dividido), que distribuye los datos equitativamente entre dos o más discos sin información de paridad o redundancia –es decir, no ofrece tolerancia al fallo (si ocurriese alguno, la información de los discos se perdería y debería restaurarse desde la copia de seguridad).

Copias de seguridad: El resto de datos correspondientes al SIG o custodiados y mantenidos por COVIAR se almacenan en un servidor (dirección IP: 192.168.0.150), situado en las oficinas



centrales, sobre el cual el Responsable de Seguridad realiza copia de seguridad diaria en 5 cintas (lunes a viernes) DLT-V4 160/320 GB mediante software Computer Associates BrightStor ARCserve Backup. Las cintas quedan identificadas y custodiadas en caja fuerte.

Se realizará verificación del respaldo en cada auditoría interna realizada a lo largo del año, en las delegaciones que esto ocurra.

El responsable del fichero delegará las funciones rutinarias en el encargado del tratamiento para efectuar las operaciones oportunas para realizar las copias de respaldo. Estas consistirán en copiar los datos de los ficheros en un soporte que habrá de ser archivado por el encargado del fichero en un lugar donde solo tengan acceso el responsable del fichero y él mismo.

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

1. Las copias de respaldo y recuperación se realizarán en un mismo soporte y serán archivadas por el encargado del fichero.
2. Se realizarán diaria o semanalmente, se conservarán por espacio de lo establecido en el Sistema Integral de Gestión (Calidad y Medio Ambiente) o por la legislación vigente en función de la calidad y el destino de los datos del fichero original.

Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al fichero tratado.

Medidas a adoptar en el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes

Soporte es cualquier objeto físico o lógico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos, tales como cintas, cartuchos, CD-ROM, DVD, disquetes, tarjetas de memoria, etc.

No está permitida la utilización de soportes con fines personales o ajenos a los objetivos propios del puesto de trabajo correspondiente. En general, su uso estará siempre restringido para evitar la posible salida incontrolada de información de las instalaciones de la empresa.

• Salida de soportes

- La salida de soportes con datos personales de las instalaciones únicamente se permite en supuestos justificados por razones de trabajo o bien su comunicación a otras empresas u organismos cuando las circunstancias lo requieran. Esta circunstancia deberá ser comunicada al Responsable de Seguridad, quien deberá autorizar previamente, y por escrito, la salida. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en donde está ubicado el sistema de información, únicamente puede ser autoriza-



da por el responsable del fichero. Los dispositivos móviles que pueden contener datos personales son terminales tipo PDA que contienen nombre, apellidos y teléfono de contacto de personal operativo.

- Sin perjuicio de lo anterior, toda entrada y salida de soportes deberá ser comunicada y autorizada por el Responsable de Seguridad, quien informará al usuario de las medidas que deberá adoptar en relación con el soporte.
- Si los soportes con datos de los mencionados ficheros van a salir fuera de los locales en que se encuentran ubicados, como consecuencia de operaciones de mantenimiento, se adoptarán las medidas oportunas con el fin de impedir cualquier recuperación indebida de la información almacenada en ellos. Cualquier proveedor con posible acceso a datos de carácter personal firmará un documento de sigilo con la siguiente cláusula o equivalente: “El proveedor no facilitará a terceros los datos o información sobre los mismos, debiendo tomar las medidas necesarias para garantizar la privacidad de las operaciones. De igual forma, guardará confidencialidad absoluta en relación a los procedimientos, métodos y manuales operativos de COVIAR, y en general sobre cualquier clase de información y documentación que se le facilite”.
- En el supuesto de que se procediera a dar salida de soportes que incluyeran datos de carácter personal especialmente sensibles (especialmente los referidos a ideología, religión, creencias, origen racial, salud o vida sexual) sería necesario proceder al cifrado de los datos. La salida de este tipo de soportes únicamente se efectuará previa petición al Responsable de Seguridad.
- El incumplimiento de las obligaciones contenidas en este apartado está tipificado como infracción muy grave.
- **Destrucción de soportes.** Los soportes que vayan a ser retirados, destruidos o reutilizados deberán ser borrados o destruidos, de forma que se impida la recuperación posterior de la información en ellos almacenada. Este mismo deber de destrucción será aplicable para la información contenida en papel.
 - La retirada de los residuos y soportes generados en este apartado se realizará según procedimiento **P23 Gestión Medioambiental** e instrucción **I07 Gestión de Residuos**.

Ficheros existentes y regulación

Los ficheros de datos cuyo tratamiento es responsabilidad de COVIAR se encuentran relacionados y regulados a continuación, con indicación del nivel de seguridad correspondiente.

Es responsabilidad de todo el personal en la organización mantener actualizado dicho inventario, por lo que cualquier modificación en los datos en él contenidos, así como cualquier omisión que se aprecie en el mismo (ficheros que contengan datos de carácter personal y no estén incluidos), debe ser comunicada inmediatamente al Responsable de Seguridad.

Adicionalmente, los departamentos, compartimentos, software, aplicaciones, ficheros, bases de datos, elementos informáticos, instalaciones y personal propio o ajeno adscrito a COVIAR.



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
<p>Finalidad y Usos previstos</p> <p><ALARMAS> 1942220783</p> <p>Nivel Básico.</p> <p>Finalidad y usos previstos: Gestión contable, fiscal y administrativa. Contabilidad según código de comercio.</p> <p>Central Receptora de Alarmas.</p>	<p>NIF. NOMBRE Y APELLIDOS. DIRECCIÓN. TELÉFONO</p> <p>Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales: Personal de la empresa. Clientes. Proveedores.</p> <p>Cesiones previstas: Consentimiento previo del afectado.</p> <p>Transferencias Internacionales: N/A</p> <p>Procedencia de los datos: Interesado o su representante legal.</p> <p>Procedimiento de recogida: Declaraciones o formularios. Conversaciones personales.</p> <p>Soporte utilizado para la recogida de datos: Soporte papel, oral.</p>	<p>Dirección IP http://192.168.0.150</p> <p>Intel Pentium 2 CPU 6400 2,13 GHz 1,9 GB RAM Windows 2003 Server</p> <p>Fichero informatizado, no automatizado. Aplicación: JM SYSTEM MANITOU. Accesible a través de 3 ordenadores monopuesto en LAN.</p> <p>Autovía de Logroño, Km. 7,600 50011 Zaragoza</p>	<p>Alta, baja y modificación de registros:</p> <ul style="list-style-type: none"> • José Antonio Baigorri (Responsable C.R.A.) • Operadores C.R.A. • Esteban Bel. • Javier Povedano. <p>Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad:</p> <ol style="list-style-type: none"> 1. Javier Povedano 2. Esteban Bel 3. José Antonio Baigorri 	<p>SAFE IN-FORMÁTICA SL</p>	<p>RAID 1.</p> <p>5 Cintas (lunes a viernes) DLT-V4 160/320 GB custodiadas en caja fuerte servidor. Software Computer Associates BrightStor ARCserve Backup.</p> <p>Conexión remota via VLAN (NETLAN) de Telefónica. La VPN impide la salida de las copias de seguridad de la sede central.</p>



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
<p>Finalidad y Usos previstos</p> <p><CONSULTAS WEB> 2072040678</p> <p>Nivel Básico</p> <p>Proporcionar información y contestar a las personas acerca del motivo de la consulta que realicen a través del sitio web de COVIAR o por correo electrónico a direcciones de mail de los dominios coviar.es, coviar.com y tiempodeformacion.es</p>	<p>NOMBRE Y APELLIDOS. TELEFONO. DIRECCION.</p> <p>Sistema de tratamiento: Mixto</p> <p>Origen: Administraciones Públicas. Entidad Privada. El propio interesado o su representante legal.</p> <p>Colectivos: Clientes y usuarios. Empleados. Estudiantes. Personas de contacto. Padres o tutores. Solicitantes.</p> <p>Cesión o comunicación de datos: N/A</p>	<p>Dirección IP http://195.55.174.233</p> <p>Intel Pentium IV CPU 6400 4,13 GHz 1,9 GB RAM Windows 2003 Server</p> <p>Aplicación de desarrollo: Entorno web Microsoft .ASP. WWW.COVIAR.COM</p> <p>Aplicación cliente: Microsoft Outlook 2003 Microsoft Outlook 2007 Ms. Outlook Express</p>	<p>Alta de registros:</p> <ul style="list-style-type: none"> • Usuario <p>Consulta de registros:</p> <ul style="list-style-type: none"> • Directores Departamento • Directores Delegación • Personal administrativo adscrito a Departamentos o Delegaciones <p>Baja y modificación de registros:</p> <ul style="list-style-type: none"> • Responsable de Seguridad <p>Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad:</p> <ol style="list-style-type: none"> 1. Javier Povedano 2. Jorge Moreno 3. Esteban Bel 	N/A	<p>RAID 1</p> <p>5 Cintas (lunes a viernes) HP DDS-3 24 GB custodias en caja fuerte servidor. Software Computer Associates BrightStor ARCServe Backup.</p> <p>Conexión remota via VLAN (NETLAN) de Telefónica. La VPN impide la salida de las copias de seguridad de la sede central.</p>
<p><CURRICULUM – SELECCIÓN DE PERSONAL> 2100151988</p> <p>SELECCION DE PERSONAL A TRAVES DE CURRICULUM VITAE, SOLICITUDES DE EMPLEO, ANUNCIOS Y AUTOCANDIDATURAS</p>	<p>NIF. NOMBRE Y APELLIDOS. DIRECCIÓN. TELÉFONO. DATOS DE ESTADO CIVIL. DATOS DE FAMILIA. FECHA/LUGAR DE NACIMIENTO. NACIONALIDAD. FORMACIÓN, TITULACIONES. PROFESIÓN. PUESTOS DE TRABAJO. DATOS NO ECONÓMICOS NÓMINA. HISTORIAL DEL TRABAJADOR. GRADO DE MINUSVALIA.</p> <p>Sistema de tratamiento: Mixto</p> <p>Origen: El propio interesado o su representante legal.</p> <p>Colectivos: Solicitantes.</p> <p>Cesión o comunicación de datos: N/A</p>	<p>Fichero papel en cada delegación</p>	<p>Alta de registros:</p> <ul style="list-style-type: none"> • Usuario <p>Consulta de registros:</p> <ul style="list-style-type: none"> • Directores Departamento / Delegación • Personal administrativo adscrito a RRHH. <p>Baja y modificación de registros:</p> <ul style="list-style-type: none"> • Directores Departamento / Delegación <p>Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad:</p> <ol style="list-style-type: none"> 1. Javier Povedano 2. Jorge Moreno 3. Jorge Torres 	N/A	<p>Original en delegación o departamento en caso de contratación.</p> <p>Copia en RRHH en caso de contratación.</p>



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
Finalidad y Usos previstos <FICHAJE> 2100180628 Nivel Básico Acceso de los empleados Central y Delegación Zara- goza	NOMBRE Y APELLIDOS. FIRMA O HUELLA. Finalidad y usos previs- tos: Gestión de personal Personas o colectivos sobre los que se pre- tenda obtener o que resulten obligados a suministrar los datos personales: Personal de la empresa Cesiones previstas: N/A Transferencias Interna- cionales: N/A Procedencia de los datos: Interesado. Procedimiento de recogida: Fichaje. Soporte utilizado para la recogida de datos: Informático.	Dirección IP http://192.168.0.202 Intel Pentium 4 CPU 2,00 GHz 1 GB RAM Windows 2003 Server Autovía de Logroño, Km. 7,600 50011 Zaragoza Aplicación: INZACARD INZ-PRES	Alta, baja y modifica- ción de registros: • Javier Povedano • Jorge Torres Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad: 1. Javier Povedano 2. Jorge Torres	N/A	RAID 1 5 Cintas (lunes a viernes) DLT-V4 160/320 GB custo- diadas en caja fuerte servidor. Software Computer Associates BrightStor ARCServe Backup.



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
<p>Finalidad y Usos previstos</p> <p><GESTIÓN ECONÓ- MICA> 1942220782</p> <p>Nivel Básico</p> <p>Gestión contable, fiscal y administra- tiva. Contabilidad según código de comercio.</p>	<p>NIF. NOMBRE Y APE- LLIDOS. DIRECCIÓN. TELÉFONO. ACTIVIDA- DES Y NEGOCIOS. BIENES Y SERVICIOS SUMINISTRADOS. BIENES Y SERVICIOS RECIBIDOS. TRANSAC- CIONES FINANCIERAS.</p> <p>Personas o colectivos sobre los que se pre- tenda obtener o que resulten obligados a suministrar los datos personales: Personal de la empresa. Clientes. Proveedores.</p> <p>Cesiones previstas: Consentimiento previo del afectado.</p> <p>Transferencias Interna- cionales: N/A</p> <p>Procedencia de los datos: Interesado o su representante legal.</p> <p>Procedimiento de recogida: Declaraciones o formularios. Conver- saciones personales.</p> <p>SopORTE utilizado para la recogida de datos: SopORTE papel, oral, informático.</p>	<p>Dirección IP http://192.168.7.1</p> <p>Intel Pentium IV CPU 6400 4,13 GHz 1,9 GB RAM Windows 2003 Server</p> <p>Aplicación: VISUAL CONTA. Accesible a través de ordenador monopuesto en LAN.</p> <p>c/ Biarritz, 12 50012 Zaragoza</p>	<p>Alta, baja y modifica- ción de registros:</p> <ul style="list-style-type: none">• María Isabel Royo• Javier Díez• Pascual Canales• Susana Roncal• Beatriz Belloc• Silvia Membrado <p>Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad:</p> <ol style="list-style-type: none">1. Javier Povedano2. Javier Díez	<p>SAFE IN- FORMÁTICA SL</p>	<p>RAID 1</p> <p>5 Cintas (lunes a viernes) HP DDS-3 24 GB custodia- das en despacho Servicios Generales. Software Computer Associates BrightStor ARCserve Backup.</p> <p>Conexión remota via VLAN (NETLAN) de Telefó- nica. La VPN impide la salida de las copias de seguri- dad de la sede central.</p>



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
Finalidad y Usos previstos <GESTIÓN PERSONAL> 1942220784 Nivel Básico Organización del trabajo de los empleados	NIF. NOMBRE Y APELLIDOS. DIRECCIÓN. TELÉFONO. DATOS DE ESTADO CIVIL. DATOS DE FAMILIA. FECHA/LUGAR DE NACIMIENTO. NACIONALIDAD. FORMACIÓN, TITULACIONES. PROFESIÓN. PUESTOS DE TRABAJO. DATOS NO ECONÓMICOS NÓMINA. HISTORIAL DEL TRABAJADOR. GRADO DE MINUSVALIA. Finalidad y usos previstos: Gestión de personal Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales: Personal de la empresa Cesiones previstas: N/A Transferencias Internacionales: N/A Procedencia de los datos: Interesado o su representante legal. Procedimiento de recogida: Declaraciones o formularios. Soporte utilizado para la recogida de datos: Soporte papel, oral.	Dirección IP http://192.168.0.150 Intel Pentium 4 CPU 2,00 GHz 1 GB RAM Windows 2003 Server Autovía de Logroño, Km. 7,600 50011 Zaragoza Aplicación: LOTUS NOTES SERVER VISUALPLAN	Alta, baja y modificación de registros: <ul style="list-style-type: none">Javier PovedanoJorge TorresNieves DomenechPilar AlluevaBernabé Comín (en ausencia de los anteriores)Susana Díaz (en ausencia de los anteriores) Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad: <ol style="list-style-type: none">Javier PovedanoBernabé Comín	SAFE INFORMÁTICA SL NIX UNIVERSAL SL	RAID 1 5 Cintas (lunes a viernes) DLT-V4 160/320 GB custodiadas en caja fuerte servidor. Software Computer Associates BrightStor ARCserve Backup. Conexión remota via VLAN (NETLAN) de Telefónica. La VPN impide la salida de las copias de seguridad de la sede central.



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
<p>Finalidad y Usos previstos</p> <p><NÓMINAS> 1942220786</p> <p>Nivel Alto.</p> <p>Confección de nóminas, seguros sociales, contratos de trabajo, finiquitos</p>	<p>NIF. Nº S.S./MUTUALIDAD. NOMBRE Y APELLIDOS. DIRECCIÓN. TELÉFONO. DATOS DE ESTADO CIVIL. DATOS DE FAMILIA. FECHA/LUGAR DE NACIMIENTO. NACIONALIDAD. FORMACIÓN, TITULACIONES. PROFESIÓN. PUESTOS DE TRABAJO. DATOS NO ECONÓMICOS NÓMINA. HISTORIAL DEL TRABAJADOR. DATOS ECONÓMICOS NÓMINA. GRADO DE MINUSVALÍA.</p> <p>Finalidad y usos previstos: Gestión de personal</p> <p>Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales: Personal de la empresa</p> <p>Cesiones previstas: No se requiere el consentimiento previo del afectado (Art. 10.2 RD 1720/2007).</p> <p>Transferencias Internacionales: N/A</p> <p>Procedencia de los datos: Interesado o su representante legal.</p> <p>Procedimiento de recogida: Declaraciones o formularios, conversaciones personales.</p> <p>SopORTE utilizado para la recogida de datos: SopORTE papel, oral.</p>	<p>Dirección IP http://192.168.0.150</p> <p>Intel Pentium 4 CPU 2,00 GHz 1 GB RAM Windows 2003 Server</p> <p>Aplicación: A3NOM</p> <p>Autovía de Logroño, Km. 7,600 50011 Zaragoza</p>	<p>Alta, baja y modificación de registros:</p> <ul style="list-style-type: none"> Javier Povedano Jorge Torres Nieves Doménech Pilar Allueva Susana Díaz (en ausencia de los anteriores) Bernabé Comín (en ausencia de los anteriores) <p>Entrega de registros a los interesados:</p> <ul style="list-style-type: none"> Delegado. Jefe de Servicios. Inspector. Aux. Administrativo Delegación. <p>Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad:</p> <ol style="list-style-type: none"> Javier Povedano Bernabé Comín 	<p>SAFE IN-FORMÁTICA SL</p>	<p>RAID 1</p> <p>5 Cintas (lunes a viernes) DLT-V4 160/320 GB custodiadas en caja fuerte servidor. Software Computer Associates BrightStor ARCserve Backup.</p> <p>Conexión remota via VLAN (NETLAN) de Telefónica. La VPN impide la salida de las copias de seguridad de la sede central.</p>



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
<p>Finalidad y Usos previstos</p> <p><PROTECCIÓN DE PERSONALIDADES> 2051600136</p> <p>Nivel Alto.</p> <p>Gestión y control de la actividad de protección de personalidades.</p> <p>La transmisión de datos de carácter personal del fichero se realizará de manera codificada, cifrada y encriptada, garantizando que no sean inteligibles ni manipulados por terceros.</p>	<p>D.N.I./N.I.F. TELEFONO. NOMBRE Y APELLIDOS. DIRECCION. DATOS DE CARACTERISTICAS PERSONALES. DATOS ECONOMICOS FINANCIEROS Y DE SEGUROS. DATOS DE CIRCUNSTANCIAS SOCIALES. DATOS DE DETALLES DE EMPLEO. LOCALIZACION GPRS.</p> <p>Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales: Protegidos</p> <p>Cesiones previstas: Consentimiento previo del afectado. MINISTERIO DE INTERIOR</p> <p>Transferencias Internacionales: N/A</p> <p>Procedencia de los datos: Administraciones Públicas. Interesado o su representante legal.</p> <p>Procedimiento de recogida: Conversaciones personales.</p> <p>SopORTE utilizado para la recogida de datos: SopORTE papel.</p>	<p>SopORTE papel.</p> <p>Responsable de PRL.</p> <p>Avda. José Luis Goyoa- ga, 32 - 3ª Planta, Apto 304 - Edificio Noray 48950 Erandio (Vizcaya)</p> <p>Aplicación: GENASYS</p>	<p>Alta, baja y modificación de registros:</p> <ul style="list-style-type: none"> • Susana Díaz • Bernabé Comín • Javier Povedano • Jorge Torres • Delegado Provincial (Escoltas) <p>Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad:</p> <ol style="list-style-type: none"> 1. Javier Povedano 2. Delegado Provincial (Escoltas) 	<p>MINISTERIO INTERIOR. DIRECCION GENERAL DE LA POLICIA Y DE LA GUARDIA CIVIL.</p>	<p>RAID 1</p> <p>5 Cintas (lunes a viernes) DLT-V4 160/320 GB custodiadas en caja fuerte servidor. Software Computer Associates BrightStor ARCserve Backup.</p> <p>Conexión remota via VLAN (NETLAN) de Telefónica. La VPN impide la salida de las copias de seguridad de la sede.</p>



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
Finalidad y Usos previstos <PRL COORDINA- CION DE ACTIVIDA- DES EMPRESARIA- LES> 2100460560	D.N.I./N.I.F. NOMBRE Y APELLIDOS. FORMA- CION PRL PROVEEDO- RES. TCs. Personas que puedan acceder a instalaciones de COVIAR, fruto de contratas o subcontra- tas (legislación de PRL) Cesiones previstas: Consentimiento previo del afectado. Ninguna. Transferencias Interna- cionales: N/A Procedencia de los datos: Empresa presta- taria. Procedimiento de recogida: Correo conve- ncional, correo electró- nico. Soporte utilizado para la recogida de datos: Soporte papel.	Soporte papel. Responsable de PRL (Recursos Humanos) Autovía de Logroño, Km. 7,600 – Pol. Ind. Europa II, nave II (50011 Zara- goza)	<ul style="list-style-type: none">• Delegados Provin- ciales• Jorge Torres (Res- ponsable PRL) Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad: <ol style="list-style-type: none">3. Javier Povedano4. Jorge Moreno	N/A.	N/A.



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
<p>Finalidad y Usos previstos</p> <p><REGISTRO FORMACIÓN> 2070820546</p> <p>Nivel Básico</p> <p>Registro de alumnos y acciones de formación no reglada, ocupacional y continua</p>	<p>D.N.I./N.I.F.. NOMBRE Y APELLIDOS. NUM.S.S./MUTUALIDAD. DIRECCIÓN. TELEFONO. DATOS ACADÉMICOS Y PROFESIONALES.</p> <p>Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales: Empleados; clientes y usuarios; estudiantes; representante legal; solicitantes.</p> <p>Cesiones previstas: Consentimiento previo del afectado. Otros órganos de la Administración Pública.</p> <p>Transferencias Internacionales: N/A</p> <p>Procedencia de los datos: Interesado o su representante legal.</p> <p>Procedimiento de recogida: Declaraciones o formularios, conversaciones personales.</p> <p>Soporte utilizado para la recogida de datos: Soporte papel, oral.</p>	<p>Dirección IP http://192.168.9.2</p> <p>Intel Pentium III 1,8 GHz 256 MB RAM Windows XP Professional</p> <p>c/ Biarritz, 6 50012 Zaragoza</p> <p>Dirección IP http://192.168.11.2</p> <p>Intel Pentium III CPU 2,00 GHz 512 MB RAM Windows 2000 Server</p> <p>Aplicación Teleformación: MOODLE www.tiempodeformacion.es</p> <p>Aplicación: MICROSOFT EXCEL 2003</p>	<p>Alta, baja y modificación de registros:</p> <ul style="list-style-type: none">• Jorge Moreno• Javier Povedano• Personal administrativo <p>Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad:</p> <ol style="list-style-type: none">1. Javier Povedano2. Jorge Moreno3. Bernabé Comín	<p>SAFE INFORMÁTICA SL</p>	<p>RAID 0.</p> <p>1 Disco Duro externo USB FREECOM 250 GB. Software Copia Seguridad Windows XP Profesional.</p>



FICHERO. Nº REGISTRO. NIVEL DE SEGURIDAD.	INFORMACIÓN SOBRE EL FICHERO	SOPORTE FÍSICO O LÓGICO. SOPORTE. APLICACIÓN INFORMÁ- TICA. UBICACIÓN.	ENCARGADOS TRATAMIENTO	TERCEROS CON ACCESO A DATOS	COPIA RESPAL- DO
Finalidad y Usos previstos <VIDEOVIGILANCIA> 2072040406 Nivel Básico TRATAMIENTO DE DATOS PERSONALES CON FINES DE VIGILANCIA A TRAVES DE SISTEMAS DE CAMARAS Y VIDEOCAMARAS	IMAGEN/VOZ. Finalidad y usos previstos: Videovigilancia. Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales: Empleados; Clientes y Usuarios; Proveedores; Representante Legal. Cesiones previstas: FUERZAS Y CUERPOS DE SEGURIDAD Transferencias Internacionales: N/A Procedencia de los datos: Videocámara de vigilancia. Procedimiento de recogida: Información cartel Instrucción 1/2006. Soporte utilizado para la recogida de datos: video digital	Dirección IP http://192.168.0.150 Intel Pentium III 1,8 GHz 256 MB RAM Windows XP Professional Autovía de Logroño, Km. 7,600 50011 Zaragoza Aplicación: SAMSUNG NET-I LIGHVIEWER	Alta, baja y modificación de registros: <ul style="list-style-type: none">• José Antonio Baigorri• Esteban Bel• Delegados Provinciales Sistemas• Operadores CRA Orden de delegación de funciones de seguridad del fichero en ausencia del Responsable de Seguridad: <ol style="list-style-type: none">1. Javier Povedano2. Esteban Bel3. José Antonio Baigorri	SAFE IN-FORMÁTICA SL	RAID 1. Disco duro video digital. Conexión remota via VLAN (NETLAN) de Telefónica. La VPN impide la salida de las copias de seguridad de la sede central.



Solicitud de datos de carácter personal de los ficheros titularidad de COVIAR.

- **Queda totalmente prohibido realizar cesiones de datos a terceros sin la previa autorización escrita del Responsable del Fichero (COVIAR), consentimiento escrito del particular afectado, normativa de obligado cumplimiento o resolución judicial.**
- Esta prohibición no afecta al intercambio de datos entre los distintos departamentos y delegaciones cuando se trate de datos relacionados con la propia gestión de la producción (selección de personal, inserción laboral, confección de nóminas y mantenimiento de la relación laboral, formación, prestación del servicio, compras, etc.).

Consideraciones sobre el correo electrónico

- Todos los mensajes de correo electrónico se realizarán conforme a la instrucción **I04 Comunicación Externa.**

Derechos de acceso, rectificación y cancelación. Cesión de datos.

Los interesados tendrán derecho al acceso, rectificación y cancelación de sus datos de carácter personal sometidos a tratamiento automatizado, en la forma prevista en la Ley Orgánica 15/1999 mencionada, y demás normativa de aplicación en la forma establecida en este procedimiento.

Con la finalidad de que pueda analizarse la procedencia o no de una cesión o comunicación de datos, así como, en su caso, de una rectificación o cancelación de los datos de carácter personal existentes en un determinado fichero, todas las solicitudes deberán dirigirse por escrito dirigido al Responsable de Seguridad (LOPD), según el modelo dispuesto en la dirección web: <http://www.coviar.com/docs/lex/lopd/EjercicioderechosLOPD.pdf>.

Informado el Responsable del Fichero (COVIAR), éste resolverá lo que proceda a través del Responsable de Seguridad conforme a lo establecido en la legislación vigente en la materia.

Medio Ambiente (Control operacional). Control de Consumos. Gestión de residuos.

Se identifica(n) el/los aspecto(s): **Material informático, ordenadores y asimilados (RAEE). Papel.**

Gestión: **Según I07 Control de consumos. Gestión de Residuos.**



5.2. PROTECCIÓN MEDIOAMBIENTAL

5.2.1. Normas generales

- Procurar manejar documentación digitalizada o escaneada, cuando no sea imprescindible el original en papel.
- Evitar el consumo innecesario. Cada artículo consumido representa un coste energético para ser producido y genera un residuo. Con su envase sucede lo mismo.
- Hacer buen uso del papel. Utilizar papel reciclado, reutilizarlo siempre que se pueda, ser selectivo a la hora de imprimir documentos que están en soporte digital, fotocopiar a dos caras.
- Seguir las normas de protección medioambiental establecidas en los procedimientos.
- Tener presente la posibilidad de reducir, reutilizar o reciclar los materiales no aprovechados.
- Segregar los residuos por el destino al que van dirigidos.
- Comunicar cualquier riesgo medioambiental que se detecte al Responsable de Calidad.

COVIAR tiene establecidos códigos de buenas prácticas ambientales que deben ser llevados a la práctica por todos sus empleados. El Responsable de Calidad tiene la responsabilidad de proponer a la Dirección la realización de las modificaciones que considere oportunas respecto a los mismos. Para ello, ha de tener en cuenta las sugerencias del personal, los códigos de buenas prácticas a los que se pueda adherir la empresa y cualquier otra información que considere oportuna.

5.2.2. Normas generales de orden y limpieza

Criterios básicos:

- Las operaciones de orden y limpieza necesitan una atención constante diaria. Una buena limpieza está relacionada con la prevención de riesgos sobre la producción y riesgos laborales: junto con el orden, proporciona una buena imagen de la empresa, estando directamente relacionada con la protección al medio ambiente.
- Conseguir el auto-orden y auto-limpieza de la empresa no es posible sin la implicación de todo el personal: las tareas de orden y limpieza de cada puesto de trabajo son peculiares de cada uno. Por lo tanto, cada persona conoce cómo mantener su puesto de trabajo limpio y ordenado y cuáles son las posibles mejoras.
- Cada persona es responsable de corregir las situaciones de desorden y suciedad de su puesto de trabajo. Cada responsable de área o departamento debe hacer un seguimiento de las conductas descritas.
- No hay que esperar a las auditorías para cumplir con estas conductas; cuando cualquier persona vea algo que no esté en orden o limpio, lo comunicará a su superior o al Responsable de Calidad.

Se pretende:



- Conseguir un lugar de trabajo seguro y limpio, eliminando las cosas innecesarias y ordenando las necesarias; colocando las cosas en los lugares oportunos y manteniendo un sistema de trabajo en el que se puedan tomar medidas correctivas.
- Conseguir un lugar de trabajo claro, donde cualquier persona pueda detectar cualquier anomalía de un vistazo, determinando el qué, el cómo y el dónde fácilmente.

Cómo se consigue:

1. Tener el puesto de trabajo lo más limpio posible, y en especial las ropas de trabajo y los vehículos. Cuando se trate de limpieza que ha de realizar el personal especializado, dejando el puesto en orden para que dicha tarea se pueda realizar eficientemente.
2. Utilizar los contenedores, papeleras, etc. en el puesto de trabajo y durante toda la jornada.
3. Evitar la necesidad de limpieza, disminuyendo la causa de la suciedad cuando sea posible.



5.3. CONTROL DE LOS DOCUMENTOS Y DE LOS REGISTROS DEL SIG

Este apartado establece la metodología con que se elaboran, revisan, aprueban, distribuyen y controlan los documentos emitidos, así como para introducir nueva información, asegurando que toda la que se desprende del SIG implantado, esté disponible cuando se requiera evitando la circulación de información duplicada y obsoleta.

Así mismo:

- Establece y mantiene los registros para proporcionar la evidencia de la conformidad con los requisitos, así como de la operación eficaz del SIG.
- Define los controles necesarios para la identificación, el almacenamiento, la protección, la recuperación, el tiempo de retención y la disposición de los registros.

5.3.1. Responsabilidades

Las responsabilidades de la elaboración, revisión, aprobación, distribución, modificación y archivo de cada documento, así como la responsabilidad de cumplimentar y archivar los diferentes registros del SIG se indican en la lista del control de documentos identificada con el acrónimo **L01 Lista Control de los Documentos y de los Registros del SIG**.

Todo el personal que acceda a datos (de carácter personal o no) está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla. Constituye una obligación del personal notificar al Responsable de Seguridad las incidencias de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos que conozcan en el desarrollo de su trabajo.

5.3.2. Asignación y descripción de las funciones y responsabilidad de los asignados

Responsable del fichero	COVIAR	Representante Legal
Encargado del tratamiento de los ficheros	En función del Departamento	En función del Departamento
Responsable de Seguridad 1	Javier Povedano Urés	Director de Recursos Humanos
Responsable de Seguridad 2	Jorge Moreno López	Responsable de Calidad

El responsable del fichero

El responsable del fichero es la organización COMPAÑÍA DE VIGILANCIA ARAGONESA, S.L. (COVIAR), que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad, de acuerdo con el Reglamento. A estos efectos, delega en el Representante Legal de la empresa.

Funciones propias:



- Legitimación para el tratamiento de los datos. Consiste en cumplir todos los requisitos legales y reglamentarios para obtener el consentimiento del afectado para que los datos puedan ser ingresados, tratados, guardados, transmitidos, manipulados, cedidos y/o cancelados por el responsable del fichero o aquel a quien se haya destinado para cada forma de tratamiento.
- Notificación, inscripción, modificación y cancelación de ficheros en la Agencia Española de Protección de Datos
- Decide sobre la finalidad, contenido, usos y aplicaciones del fichero y responde de su legalidad y legitimación, de acuerdo con lo dispuesto en la Ley Orgánica de Protección de Datos de Carácter Personal, en la Directiva CE 46/95, los Reglamentos y las instrucciones y recomendaciones de la Agencia de Protección de Datos. Es el responsable de cumplir los requisitos exigidos en la legislación vigente para garantizar los derechos de los afectados (acceso, rectificación y cancelación). Responde frente al afectado, frente a terceros y frente a la Administración de todos los daños y perjuicios que se deriven del mal uso de los datos y de los ficheros.
- Es el encargado del ejercicio y tutela de los derechos de acceso, modificación, rectificación o cancelación de los afectados.
- Es el responsable de la legalización y legitimación de los ficheros en los términos previstos en el en la L.O.P.D. y en el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999

Encargado del tratamiento de los ficheros

Dependiendo del departamento, tiene como misión realizar las tareas ordinarias para el desarrollo efectivo de las funciones y aplicaciones para las que ha sido creado el fichero. El encargado, siempre por delegación del Responsable del fichero, ha de realizar las operaciones reglamentarias para proceder conforme a la legislación en el tratamiento de los datos. Se ocupa de realizar las verificaciones necesarias y obligatorias para conservar, tratar y asegurar los datos. Responde en todo caso de la calidad de los datos por acciones ajenas al responsable y al encargado del fichero. Carece de autonomía y siempre actúa por cuenta y riesgo del encargado del fichero.

Funciones propias:

- Acceder a los datos que resulten necesarios para la prestación del desempeño laboral habitual asignado.
- Tratamiento: los datos han de ser tratados de forma leal (de acuerdo con las prescripciones dictadas por el responsable del fichero y cumpliendo rigurosamente las condiciones y las limitaciones impuestas por el Documento de Seguridad) y lícita (cumpliendo escrupulosamente la legislación, en especial lo referido en la Ley Orgánica de Protección de Datos de Carácter Personal).
- Recogida de los datos: los datos han de ser recogidos con fines determinados, explícitos y legítimos, y no pueden ser tratados posteriormente de manera incompatible con los dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas a los afectados.
- Ubicuidad, adecuación y longitud. Los datos recogidos han de ser forzosamente adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y



para los que se traten posteriormente.

- Calidad. Los datos recogidos y que pertenecen a los ficheros han de ser exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o tratados posteriormente sean suprimidos o rectificadas.
- Conservación: los datos han de ser conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. En todo caso, se establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

El Responsable de Seguridad

Es el responsable de coordinar todas las tareas descritas en este documento relacionadas con los datos personales. Además tiene la obligación de elaborar informes periódicos acerca del cumplimiento de todas las obligaciones adquiridas por el responsable del fichero y ha de responsabilizarse para el caso de que existan incidencias y de mantener las normas de actuación y tratamiento de acuerdo a la legislación vigente.

El responsable de seguridad desempeña las funciones encomendadas por nombramiento de COVIAR, la cual podrá nombrar en cualquier momento a otro responsable de seguridad diferente.

Funciones propias:

- Auditoría interna: Es obligación del Responsable de Seguridad rendir cuentas y realizar controles periódicos sobre la seguridad de los datos. Las auditorías, en general, se realizan para la consecución de uno o varios de los objetivos siguientes:
 - Determinar la conformidad o no conformidad de los elementos del Documento de Seguridad con los requisitos especificados.
 - Determinar la eficacia del Documento de Seguridad implantado para alcanzar los objetivos previstos.
 - Proporcionar información para la mejora del Documento de Seguridad implantado.
 - Cumplir los requisitos reglamentarios que apliquen.
- Planificación de las auditorías.
 - Los Responsables de los Departamentos afectados por las auditorías deberán tener conocimiento de las fechas de auditoría.

A tales fines se estará a lo dispuesto en el procedimiento **P800 Gestión de la Mejora: Reclamaciones, Incidencias, Sugerencias. Auditorías Internas** del SIG de COVIAR, delegando la planificación y realización de las auditorías en el Responsable de Calidad.

Esporádicamente, se podrán realizar auditorías específicas o sistemáticas, de forma autónoma al programa general de auditorías, cuando:

- Se observen deficiencias sistemáticas en el tratamiento de los datos.
- Se introduzca un cambio importante en el SIG.
- Se sospeche que la calidad de los datos se está deteriorando.



- Para verificar acciones correctivas y para cumplir con el plan anual de auditorías.

Personal autorizado a acceder a los lugares donde se almacenan los soportes informáticos que contienen datos de carácter personal.

Solamente podrá acceder a los mismos el personal autorizado, durante el transcurso de la jornada laboral. El acceso a los mismos concluida la jornada laboral se controla mediante acceso con llave al recinto y la activación/desactivación de alarma conectada a la C.R.A.

Adicionalmente, todos los accesos a las ubicaciones físicas de los ficheros se encuentran controlados por cámaras de videovigilancia conectadas a la C.R.A.

En casos en que personal no autorizado tenga que tener acceso a los locales por razones de urgencia o fuerza mayor, implicará la desactivación de la alarma previa identificación ante la C.R.A.

Consecuencias del incumplimiento de las obligaciones y medidas establecidas en este apartado

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará dependiendo de la gravedad de la infracción (sanción laboral, administrativa o penal).

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, se facilita a todo el personal (mediante recibí) el **Documento de Sigilo y Protección de Datos Personales**, por el que declaran conocer, como profesionales de seguridad, lo prevenido en el ordenamiento legal vigente sobre la obligación de sigilo y reserva sobre su actividad laboral. También se informa de que (solamente en el caso de ser usuario encargado del tratamiento de datos de carácter personal de COVIAR), tiene acceso a este documento, en el cual se facilitan las normas que se deben cumplir y las consecuencias de no hacerlo.

Una copia de los documentos firmados por los trabajadores se guarda en el expediente personal.

5.3.3. Identificación de los documentos del SIG.

- El Manual.
 - Se identifica y estructura según lo establecido en el Capítulo 4 del propio Manual del SIG.
- Procedimientos.
 - La portada de cada procedimiento contendrá: una cabecera que lo identifique, un índice de su contenido, una lista o tabla de revisiones con los motivos que las originaron y cuando proceda un pie de página destinado para la identificación de las personas que han efectuado la elaboración, revisión y/o aprobación del documento.



- La exposición se relatará sin indeterminaciones. Los apartados descritos a continuación se utilizarán siempre que sean necesarios para una mejor interpretación de los procedimientos:
 - **OBJETO:** Motivo o razón de ser del procedimiento. Debe indicar claramente cuál es la actividad o proceso que pretende regular.
 - **ALCANCE:** Delimitación de las áreas funcionales, procesos, subprocesos o personas a las que afecta el procedimiento.
 - **REFERENCIAS:** Se citan documentos o normas relacionados en forma explícita con el procedimiento.
 - **RESPONSABILIDADES:** Relación de las responsabilidades genéricas aplicables a todo el proceso, las específicas se detallan en cada fase del mismo con indicación precisa del responsable de cada una de las funciones descritas.
 - **MÉTODO OPERATIVO:** Aquí se desarrollan las distintas actividades del proceso. Si se considera necesario se incluirá un diagrama sinóptico, desarrollando cada una de sus fases. Exposición de la forma de actuar relatada sin indeterminaciones. Se dispone de los procedimientos requeridos como imprescindibles por la norma y los identificados como necesarios para la gestión y control de los procesos definidos en el manual de calidad.
- La identificación de los procedimientos se realiza a través de un acrónimo y del modo siguiente: **Pn** (siendo n asociado al capítulo correspondiente de la norma UNE-EN-ISO 9001:2008 y del SIG)
- Instrucciones.
 - Las identificadas como necesarias para la realización y control de los procesos definidos en los procedimientos, no siguen el contenido establecido para los procedimientos. Definen con amplio detalle los pasos a seguir en cada una de las actividades relacionadas con el trabajo individual, normalmente dirigidas a auxiliares, operarios, etc.
 - La identificación de las instrucciones se realiza a través de un acrónimo y del modo siguiente: **In** (n: Número secuencial que progresivamente ha de sustituirse por un número asociado al procedimiento que corresponda).
- Registros y formatos.
 - Los requeridos por la norma y los identificados como necesarios para la gestión, control y seguimiento de sus procesos. Son los documentos que se generan durante el funcionamiento normal del sistema. Los registros demuestran a posteriori que todos los requisitos y acciones exigidos por el sistema se han cumplido.
 - La identificación de los registros se realiza a través de un acrónimo y del modo siguiente: **Rn** (n: Número secuencial). Aquellos registros que estén en formato papel se irán codificando del modo siguiente: **Fn** (n: Número que se asociará al procedimiento que corresponda).

5.3.4. Aprobación de los documentos



Se entiende que un documento está aprobado cuando está puesto a disposición del usuario o pueda visualizarse a través de la red informática. No es necesaria la firma en el Manual de Calidad, Procedimientos, Instrucciones o Registros.

En cuanto al resto de documentos generados por el SIG (política de calidad, objetivos, informes, actas, auditoría, mantenimiento, comunicados internos, autorizaciones personalizadas, etc.) es requisito imprescindible la firma de Dirección o de los responsables del departamento que corresponda en cada caso.

Creación o supresión de ficheros de datos de carácter personal

Los usuarios que prevean o planeen crear o suprimir un fichero que contenga datos de carácter personal, ya sea mediante la obtención de datos nuevos o mediante la utilización de datos contenidos en ficheros preexistentes, deberán comunicarlo al Responsable de Seguridad.

Los usuarios no podrán proceder a la creación o supresión de un fichero que contenga datos de carácter personal sin la obtención previa, por parte del Responsable del Departamento o Delegación, de la correspondiente autorización.

En relación con los nuevos ficheros deberá tenerse en cuenta lo siguiente:

- Sólo se podrán incluir datos necesarios y pertinentes con la finalidad perseguida en la creación del fichero. El incumplimiento de esta obligación está tipificado como infracción grave.
- La información manejada por los usuarios, susceptible de ser considerada como datos de carácter personal, será controlada por el Responsable de Seguridad, limitando los accesos y proporcionando las medidas de seguridad adecuadas, atendiendo al carácter de la información en cuestión. El incumplimiento de esta obligación está tipificado como infracción leve.
- Solamente cumpliendo con la obligación prevista en los párrafos anteriores se posibilita que la información forme parte de los procesos de copias de respaldo efectuadas en la organización, evitando posibles pérdidas de información.
- Las extracciones puntuales de datos realizadas sobre ficheros preexistentes para atender o dar cumplimiento a determinadas necesidades no se considerarán supuestos de creación de un fichero, sino que tendrán la consideración de ficheros temporales.

Se procederá a la supresión de un fichero que contenga datos de carácter personal, siguiendo el procedimiento establecido, en los siguientes supuestos:

- Cuando haya desaparecido la finalidad que motivó la creación del Fichero.
- Cuando los datos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

Y siempre que no haya una norma jurídica que obligue a conservar el fichero durante un cierto período de tiempo (por razones fiscales, mercantiles, etc.).

Es de vital importancia que los usuarios colaboren y cumplan con el procedimiento previsto, puesto que, en caso contrario, podría incurrirse en una infracción tipificada en la normativa de



protección de datos, ya que está prohibida la tenencia de datos personales sin justificación ni finalidad alguna.

Ficheros temporales

Se entiende por fichero temporal aquel generado mediante la extracción de datos de un fichero general preexistente en la empresa, con objeto de atender a una finalidad concreta y limitada en el tiempo, y facilitar su tratamiento de forma más sencilla y directa (por ejemplo, la extracción de nombres de los empleados del fichero de personal, para llevar un control de las vacaciones disfrutadas).

Los ficheros temporales que se generen en el desarrollo de la actividad se guardarán y almacenarán por los usuarios en sus terminales de trabajo y/o en carpetas de red, si bien se ubicarán preferentemente como registros del SIG en la intranet (Lotus Notes). El Responsable del Departamento/Delegación que cree un fichero temporal en una carpeta de red es responsable de solicitar al Responsable de Seguridad la limitación de los accesos a estas carpetas tan sólo a personas autorizadas y, a su vez, solicitar a aquél la implantación de medidas de seguridad que correspondan, atendiendo al nivel del fichero tratado.

Los ficheros temporales cumplirán el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento, y serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

5.3.5. Revisión y actualización de los documentos

El SIG deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes. En todo caso, cuando:

- El resultado de una auditoría cuando ésta así lo aconseje.
- Se observen deficiencias sistemáticas en la aplicación del SIG.
- Existan cambios organizativos importantes o legislativos que resulten de aplicación.
- Se implanten nuevos procesos o modificaciones importantes.
- Se realicen modificaciones de los ficheros inscritos ante la Agencia de Protección de Datos.

Cualquier persona puede solicitar una modificación de los documentos. Para ello puede cumplimentar el **R46 Informe de Mejora** o enviar un correo electrónico a calidad@coviar.com.

El Comité de Calidad, el Responsable de Calidad y los responsables de los procesos, serán los responsables del estudio de los cambios propuestos.

Al igual que el documento original, se someterán nuevamente a aprobación por parte del responsable correspondiente.

Si se aprueba la modificación, se cambiará el estado de revisión incrementando el número de revisión actual, según lo establecido en el apartado siguiente. Al mismo tiempo, y bajo la res-



ponsabilidad del Responsable de Calidad, el documento modificado y aprobado deberá quedar a disposición de todos los usuarios afectados, retirando la versión anterior del documento.

Modificación de ficheros de datos de carácter personal.

Los usuarios que prevean o planeen modificar un fichero que contenga datos de carácter personal, deberán comunicarlo al Responsable de Seguridad.

Los usuarios no podrán proceder a la modificación de un fichero que contenga datos de carácter personal sin la obtención previa, por parte del Responsable del Departamento o Delegación, de la correspondiente autorización.

No se considerará como un supuesto de modificación el mero hecho de incluir nuevos registros en un fichero, sino una modificación de su finalidad, del tipo de datos que se recogen, del tipo de tratamientos que se llevan a cabo sobre el mismo, etc.

Es necesario que los usuarios respeten el procedimiento establecido, pues solo de esta forma se podrán controlar los cambios en ficheros ya existentes y verificar así las actualizaciones producidas en los mismos, por parte del Responsable de Seguridad.

5.3.6. Identificación del estado de revisión actual y de los cambios de los documentos

Inicialmente los documentos se identifican con un número secuencial de revisión. El estado de revisión aparecerá siempre en el documento. Al mismo tiempo es posible conocer el estado de revisión a través de la **L01 Lista Control de los Documentos y de los Registros del SIG**.

Para los principales niveles documentales del SIG, es decir, Manual de Calidad, Procedimientos e Instrucciones, se insertará en la portada o primera página de cada documento una relación de motivos de las revisiones realizadas.

5.3.7. Distribución de la documentación

El SIG asegura que todos los documentos están localizables y accesibles en los puestos de trabajo que se requieren, son eficazmente revisados y aprobados y retirados inmediatamente cuando pierden su vigencia.

Cuando el documento (sea de nueva edición o por reedición) deba distribuirse en soporte papel, el Responsable de Calidad o del proceso hará llegar a los responsables funcionales que corresponda dicha documentación.

Las responsabilidades de distribución aparecen reflejadas en la **L01 Lista Control de los Documentos y de los Registros del SIG**.

En cuanto a la documentación de acceso en soporte informático, no existe distribución. En su lugar, el Responsable de Calidad sustituye la versión anterior por la nueva y comunica a los responsables de proceso, a través de correo interno, el cambio efectuado.



Los documentos entrarán en vigor en el momento de su puesta a disposición.

5.3.8. Otra documentación y datos externos

Toda la normativa aplicable se encuentra actualizada permanentemente en la dirección web pública de la empresa www.coviar.com/legislacion.asp. Además, el Responsable de Calidad mantiene la **L03 Lista de Legislación Aplicable**.

Cuando se produce una modificación en materia de Seguridad Privada, la Dirección General de la empresa y el Responsable de Calidad se encargan de distribuirla a todos los Delegados, siendo éstos los responsables de archivarla junto a la demás legislación.

La documentación y datos externos son recibidos por el personal administrativo de la Delegación, el cual los distribuye a los destinatarios correspondientes en función del tipo de documento de que se trate:

Descripción del documento	Custodia
Legislación de Seguridad Privada	Delegado
Revistas técnicas	Director General
Revistas de información empresarial	Director General
Documentación de Calidad y Medio Ambiente	Responsable de Calidad
Información relativa a Formación	Director de Formación
Ofertas comerciales	Delegado
Publicidad, mobiliario, enseres, oficina...	Director de Administración
Facturas y documentación bancaria	Director de Administración
Publicidad general y mensajería	Según contenido

5.3.9. Copias controladas

Las copias controladas corresponden a las entregadas al personal que no dispone de equipo informático, sobre las cuales se mantiene la obligación de facilitar las revisiones que vaya sufriendo la documentación.

El registro de las copias distribuidas se realiza por doble vía: a través del **R67 Recibí documentos del SIG** cumplimentado, a) en formato informático; o b) en formato papel con la firma del trabajador.

5.3.10. Control, protección y acceso a los documentos y a los registros

La empresa ha adoptado las medidas técnicas y organizativas exigidas por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal para garantizar la seguridad de los ficheros de datos personales, en función de su nivel de protección (básico, medio y alto).



Toda la documentación se controla de tres formas distintas:

1. A través de la **L01 Lista Control de los Documentos y de los Registros del SIG**;
2. Mediante documentos identificados cuando se trata de soporte papel, y
3. A través del sistema informático. En este último caso el alcance del control incluye todos los datos generados por las distintas actividades realizadas.

La protección y control de acceso a la documentación y a los datos se realiza según lo establecido en este mismo procedimiento.

Los registros son legibles y se guardan y conservan en condiciones que impiden su deterioro. En la **L01 Lista Control de los Documentos y de los Registros del SIG**, se indica quién es la persona responsable de cumplimentarlos correctamente, el soporte en el que se encuentra (papel o informático) y el tiempo de conservación mínimo estipulado.

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones.

Exclusivamente el Responsable del Fichero está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos.

- Identificación: Procedimiento de reconocimiento de la identidad del usuario, asignado por el responsable del fichero.
- Autenticación: Procedimiento para la comprobación de la identidad del usuario (contraseña), establecida por el usuario.
 - Las mejores contraseñas constan de una combinación de letras, caracteres y números. Las contraseñas más largas son mejores que las cortas. Las contraseñas distinguen entre mayúsculas y minúsculas.
- Control de Acceso: Mecanismo que en función de la identificación ya autenticada (combinación de identificación y autenticación), permite acceder a datos o recursos.

Puestos de trabajo

El personal de la organización debe tratar, utilizar y manipular de forma correcta y adecuada el material de trabajo que COVIAR pone a su disposición, según lo establecido en este procedimiento y en el **P631 Control de equipos e infraestructura**.

Los puestos de trabajo desde los que se accede a los ficheros tienen una configuración fija en sus aplicaciones o sistemas operativos relacionados con el acceso a los ficheros, que solo puede ser cambiada con autorización del Responsable de Seguridad.

Se incluye la relación de usuarios actualizada con acceso autorizado a cada fichero / sistema de información. Esta lista se actualizará cuando se produzcan variaciones (altas, bajas, etc.) en el personal asignado a cada recurso.

Recursos y material de la organización.



El uso de los recursos y material puesto a disposición por la organización deberá orientarse al cumplimiento de las finalidades previstas para la ejecución de las funciones encomendadas a los empleados. Por tanto, no está permitida la utilización de los recursos de la organización por los empleados con fines personales o ajenos a los objetivos propios del puesto de trabajo correspondiente.

En el caso de la existencia de grabadores de CD's, DVD's, memorias stick o USB, u otro tipo de soportes de grabación de datos en la organización, los usuarios deberán tener en cuenta que no se posibilita el uso de los mismos con fines personales o ajenos a los objetivos propios del puesto de trabajo correspondiente. En general, su uso estará siempre restringido para evitar la posible salida incontrolada de información de las instalaciones de la organización. No obstante, en supuestos en que por motivos justificados de trabajo se requiera la salida de este tipo de soportes de las instalaciones de la organización, se deberá comunicar esta circunstancia al Responsable de Seguridad, para su autorización. El incumplimiento de esta obligación está tipificado como infracción muy grave.

Salvaguarda y protección de las contraseñas personales.

- Contraseñas de los usuarios.
 - Todos los usuarios de los sistemas de información utilizados en la organización dispondrán de contraseñas asociadas a sus identificadores de usuario para permitirles el acceso a los sistemas informáticos (nombre de usuario y contraseña), los cuales tendrán la consideración de personal e intransferible. Cada usuario solo tendrá acceso a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones dentro de la Organización.
- Primer acceso al sistema.
 - Es recomendable por parte del usuario, en su primer acceso al sistema o a una aplicación, el cambio de la contraseña asignada al ser dado de alta o en el proceso de asignación por olvido de la contraseña, en cuyo caso deberá ponerse en contacto con el Responsable de Seguridad, quien le advertirá de esta circunstancia.
- Vigencia de las contraseñas.
 - La vigencia de las contraseñas para la identificación en el acceso a los sistemas será anual, debiendo el usuario modificar tales contraseñas en dicho término, salvo que por especiales razones de seguridad crea conveniente hacerlo antes del transcurso de dicho plazo o porque sospeche que su contraseña ha sido conocida por un tercero no autorizado.
 - Por excepción, en el caso de usuarios con acceso a Ficheros de carácter personal de nivel alto, la vigencia de las contraseñas será de 90 días.
- Configuración de contraseñas
 - El usuario podrá elegir la contraseña que desee, que contendrá como mínimo tres caracteres alfanuméricos, aunque se recomienda utilizar un número de caracteres superior. No podrán repetirse las últimas cinco contraseñas utilizadas. La contraseña no será fácilmente deducible.
 - Se recomienda no seleccionar como contraseña palabras en cualquier idioma o códigos de valores asociables al usuario (nombres de personas, matrículas, teléfonos, fechas, etc.), permutaciones sencillas o secuencias de teclado, o secuencias lógicas fácilmente deducibles.
- Conservación de las contraseñas.



- Si el usuario conserva escritas las contraseñas, deberá mantenerse en lugares no accesibles a terceros, evitando su colocación en lugares visibles y cercanos al puesto de trabajo.
- **Confidencialidad de las contraseñas.**
 - Para posibilitar la confidencialidad de las contraseñas es necesaria la colaboración de los usuarios. En este sentido, no está autorizada la divulgación o comunicación por los usuarios de su clave de acceso a otras personas, ya sean integrantes de la plantilla o ajenas a la organización. Por tanto, cada usuario es responsable de la confidencialidad de su contraseña y de todas las actividades realizadas sobre el sistema con su identificativo de usuario a los sistemas de la organización.
 - En caso de que el identificador de usuario o clave de acceso fueran conocidos fortuita, accidental o fraudulentamente por personas no autorizadas, deberá comunicar esta incidencia inmediatamente, poniéndolo en conocimiento del Responsable de Seguridad para proceder a su cambio.

Recomendaciones generales para el uso de contraseñas

Se debe poner especial atención en la selección de contraseñas fuertes para la autenticación en todos los recursos y servicios de COVIAR.

Una contraseña fuerte tiene, entre otras, las siguientes características:

- Más de ocho caracteres.
- Mezcla de caracteres alfabéticos y no alfabéticos.
- No ser ni derivarse de una palabra del diccionario, de la jerga o de un dialecto.
- No derivarse del nombre del usuario o de algún pariente cercano.
- No derivarse de información personal (del número de teléfono, número de identificación, DNI, fecha de nacimiento, etc...) del usuario o de algún pariente cercano.
- Las contraseñas deben crearse de forma que puedan recordarse fácilmente, bien de forma directa o a través de reglas nemotécnicas.

Se recomienda proteger la contraseña elegida así:

- Usar contraseñas diferenciadas en función del uso (por ejemplo, no debe usarse la misma para una cuenta de recursos y servicios que la usada para acceso a servicios bancarios).
- Si se dispone de diferentes cuentas de acceso a servicios y recursos en COVIAR, deben usarse distintas claves para cada una de ellas.
- No compartir de ninguna forma cuentas y contraseñas. Son estrictamente personales e intransferibles.
- No revelar ni compartir su contraseña por teléfono, correo electrónico, anotándola o de cualquier otra forma a nadie, incluso aunque le hablen en nombre de COVIAR o de un superior suyo en la organización.
- Nunca escribir la contraseña, ni almacenarla en ficheros sin encriptar, ni comunicarla en el texto de mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónica.
- No se comunicarán en conversaciones telefónicas.
- Cambiar las contraseñas con la frecuencia recomendada para cada tipo de cuenta y



servicio.

Terminales de trabajo

Cada usuario será responsable de su puesto o terminal de trabajo. Por tanto, cuando el responsable de un puesto de trabajo lo abandone, temporalmente, de forma que no pueda controlar quién accede al mismo (como en casos de mantener una reunión, hora de la comida, etc.) éste deberá bloquear el ordenador (CTRL+ALT+SUPR), de forma que se impida la visualización de la información y los datos protegidos con los que se encontraba trabajando.

Cuando el usuario tenga acceso a Ficheros de datos personales calificados de nivel alto, lo anterior se deberá realizar mediante la activación de un protector de pantalla automático que impida la visualización de datos y se encuentre protegido por una contraseña. La reanudación del trabajo implicará la desactivación de la pantalla protectora mediante la introducción de la contraseña por el usuario. La pantalla protectora se activará automáticamente cuando transcurran 15 minutos sin utilizarse el equipo. Los usuarios no podrán modificar esta configuración sin autorización del Responsable de Seguridad.

Al finalizar su turno de trabajo, cada usuario será responsable de apagar su equipo, ya que si el equipo quedara encendido y algún fichero de la red abierto, el proceso de copia de respaldo no comprenderá ese archivo, por lo que no se realizará la correspondiente copia de seguridad del mismo.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por escrito por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Ordenadores portátiles, PDAs y teléfonos móviles

Se deberán mantener siempre controlados, evitando su posible sustracción. Respecto de los mismos, el usuario deberá eliminar toda la información que no vaya a ser utilizada, la cual deberá volcarse en una carpeta de red que reúna las medidas de seguridad correspondientes.

Impresoras

Cuando un usuario utilice las impresoras, tras la impresión de trabajos con información de carácter personal, deberá procurar su recogida de forma inmediata, asegurándose de no dejar documentos impresos en la bandeja de salida. En el supuesto de impresoras compartidas con otros usuarios no autorizados para acceder a los datos o información en cuestión, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Acceso a datos a través de redes de comunicaciones. Conexión a redes externas. Uso de internet y correo electrónico.



Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones (acceso remoto vía TCP/IP) garantizan un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

No está autorizada la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso a los ficheros. La revocación de esta prohibición sólo podrá ser autorizada por el Responsable de Seguridad, quedando constancia de esta modificación en el registro de incidencias.

El envío electrónico de información y la utilización de Internet por el personal de la organización se encuentra exclusivamente permitida en relación con el desempeño de las actividades laborales que corresponden a cada empleado, no encontrándose permitido su uso para finalidades distintas.

Toda salida de datos de ficheros ajenos al desempeño habitual que se efectúen mediante correo electrónico, FTP u otras redes de telecomunicación requerirá previa autorización del Responsable de Seguridad. El Responsable de Seguridad informará al usuario interesado en la salida de datos de las medidas de seguridad a adoptar para garantizar la seguridad de la información.

Aplicaciones

La gestión de soportes es competencia del encargado del fichero; sin embargo, el Responsable del tratamiento está facultado para crear y gestionar soportes siempre y cuando haya conseguido, previamente, la autorización expresa del encargado del fichero.

El incumplimiento de las obligaciones contenidas en los apartados anteriores se tipifica como infracción leve, grave o muy grave en función del nivel de seguridad del Fichero afectado (nivel de seguridad básico representa infracción leve; nivel de seguridad medio representa infracción grave; nivel de seguridad alto representa infracción muy grave).