# MANUAL DE USUARIO DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

| | |
|---|---|
| Versión Nº | 1 |
| Fecha | 28/05/2018 |

# ÍNDICE

# CARTA DE LA DIRECCIÓN

El Presente Manual de Usuario de Protección de Datos y Seguridad de la Información (en adelante, el Manual) pretende dar a conocer por la ZONA FRANCA SANTANDER (ZFS), al usuario que éste es responsable de la información que utiliza para su gestión. Dicha información en numerosas ocasiones supone el tratamiento de datos de carácter personal, tanto de su responsabilidad como de responsabilidad de terceros con los que mantiene relaciones comerciales. El presente Manual establece unas normas para garantizar la confidencialidad, seguridad e integridad de la información con datos de carácter personal.

Los datos se recogen y se tratan por los usuarios en los diferentes soportes que ZFS pone a disposición de sus usuarios con la finalidad del cumplimiento de las funciones que, según sus respectivos rangos, tienen asignadas.

El cumplimiento de las medidas de seguridad en materia de Protección de Datos y Seguridad de la Información es responsabilidad de cada uno de los usuarios. Por ello, ZFS ha aprobado el presente Manual que recoge estas medidas que deberán ser conocidas, aceptadas y respetadas por todo el personal.

No todas las secciones del manual son aplicables al trabajo de cada usuario. Si por las características de su trabajo alguna sección de este manual no le es aplicable, no deberá tenerla en cuenta a la hora de realizarlo.

La información, tanto la propia como la suministrada por terceros, es un activo esencial de cualquier organización y, en concreto, para el funcionamiento de ZFS.

En definitiva, debemos adoptar unas medidas de naturaleza técnica y organizativa con el fin de controlar el flujo de esa información y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Las políticas, normas y procedimientos de seguridad de la información han sido desarrollados de acuerdo con la legislación vigente para asegurar que está protegida

de acuerdo con los niveles de criticidad, sensibilidad y las necesidades propias de ZFS y de su actividad.

Si se le presenta un problema que no puede resolver con el presente Manual, o si sabe o sospecha que se puedan estar vulnerando las políticas de ZFS descritas en el mismo, comuníquelo inmediatamente a su Jefe de Departamento, el cual reportará la incidencia al Departamento u órgano Responsable de coordinar la aplicación de la protección de datos de carácter personal en la Organización. La reputación de ZFS depende del compromiso de cada uno de los usuarios de mostrar una conducta ética adecuada en materia de Protección de Datos y Seguridad de la Información.

Se RECOMIENDA una lectura detallada del Manual, el cual se le entrega en este momento y también pone a su disposición para su consulta siempre que lo necesite en el Portal del Empleado en la Web de ZFS

GLOSARIO DE TÉRMINOS

**Datos Personales**: toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

**Tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

**Fichero:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

**Afectado o interesado:** persona física titular de los datos que sean objeto del tratamiento.

**Responsable del tratamiento**: la persona física o jurídica, autoridad, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del

tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

**Encargado del tratamiento**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

**Destinatario**: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

**Tercero:** persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

**Consentimiento del Interesado**: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

**Cesión o comunicación de datos:** tratamiento de datos que supone su revelación a una persona distinta del interesado.

**Violación de la seguridad de los datos personales**: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

**Categorías especiales de datos:** datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual u orientación sexual de una persona física.

**Autenticación:** procedimiento de comprobación de la identidad de un usuario.

**Contraseña:** información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

**Control de acceso:** mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

**Copia de respaldo:** copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

**Documento:** todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

**Ficheros temporales:** ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

**Identificación:** procedimiento de reconocimiento de la identidad de un usuario.

**Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

**Recurso:** cualquier parte componente de un sistema de información.

**Sistema de información:** conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

**Sistema de tratamiento:** modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

**Soporte:** objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

**Transmisión de documentos:** cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

**Telecomunicación por vía electrónica**: transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas.

**Usuarios que intervienen en el tratamiento de datos personales:** todos los usuarios -empleados o colaboradores- que, en el desarrollo de sus funciones tengan acceso a la información con datos de carácter personal y tienen que cumplir con las medidas de seguridad en materia de protección de datos.

FUNCIONES Y OBLIGACIONES

El personal afectado por las medidas de seguridad para la protección de datos de carácter personal se clasifica en las siguientes categorías:

a) Responsable de los Tratamientos. (Entidad o empresa)

b) Delegado de Protección de Datos (DPD)

c) Personal informático.

d) Usuarios de soportes con datos.

Todos los usuarios están obligados a informar al Delegado de Protección de Datos de cualquier situación susceptible de alterar el presente Manual, así como de cualquier modificación que afecte a los tratamientos de datos existentes en ZFS.

## Confidencialidad de la Información

- No podrá enviarse ni transmitir información confidencial de ZFS al exterior, ni mediante soportes materiales ni a través de cualquier medio de comunicación, salvo que se encuentre expresamente autorizado**.**
- La información de ZFS es propiedad de éste. Se considera información confidencial, a título enunciativo y sin carácter limitativo cualquier información con datos de carácter personal, así como documentación interna y procedimientos de ZFS.
- Los usuarios deberán guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar, directamente ni a través de terceras personas o empresas, o

incluso en el ámbito de la propia empresa con personal no autorizado, la información a la que tengan acceso durante su relación laboral/profesional con ZFS, registrada en cualquier tipo de soporte. Esta obligación continuará vigente tras la extinción del contrato laboral/mercantil.

## Control de Acceso

- Los usuarios accederán únicamente a aquellos recursos que precisan para el desarrollo de sus funciones.
- Sólo el personal autorizado puede conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el Responsable del Tratamiento.
- Cuando un usuario requiera accesos a sistemas o recursos distintos de los que determinan su perfil deberá acudir a los responsables de autorizar el acceso a dichos recursos según las políticas internas de accesos a los mismos.
- El usuario debe evitar ausentarse de su puesto de trabajo dejando el ordenador encendido sin activar el protector de pantalla que impida la visualización de los datos, para evitar que otra persona acceda en ese ordenador a información a la que no pueda tener acceso por los privilegios que se le han concedido.
- No se deben dejar en la bandeja de salida de las impresoras/fotocopiadoras documentos que contengan datos personales y/o confidenciales. En caso de que la impresora/fotocopiadora se comparta, los responsables de cada puesto se encargarán de retirar los documentos según vayan siendo impresos / fotocopiados

## Identificación y Autenticación

- El identificador de usuario o clave de acceso son individuales y no deben ser comunicados a otras personas. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del responsable del sistema con el fin de que le asigne una nueva clave.
- Los nombres de usuario y claves de acceso asignadas a cada usuario de la red corporativa son personales, siendo el usuario el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o pérdida de estos. Las claves son intransferibles no pudiendo ser comunicadas de un usuario a otro ni a personal externo subcontratado o cualquier otra persona ajena a la entidad. El uso del identificador y la clave asignada a cada usuario implicará la aceptación, como documento probatorio, de la operación efectuada. Salvo prueba en contrario, se presumirá que los actos que se lleven a cabo con el identificador y la clave asignada han sido realizados por el usuario titular de los mismos.

## Gestión de soportes y documentos

- Sólo están autorizados como soportes de almacenamiento de datos los homologados por ZFS: servidores, PCs, portátiles, CDs, cintas, teléfonos móviles, tabletas, USB, memorias externas, y soportes fotográficos/vídeo, los cuales deberán estar debidamente etiquetados de forma que permitan identificar el tipo de información que contienen.

- El usuario debe colaborar en el mantenimiento y actualización del inventario de soportes vigente en ZFS notificando cualquier alteración o baja en los soportes que le son asignados.
- En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
- Cuando se desecha cualquier documento o soporte que contenga datos de carácter personal se procederá a su destrucción o borrado, adoptándose las medidas necesarias para evitar el acceso a la información contenida en el mismo o su recuperación posterior.
- Queda prohibida la utilización de ordenadores u otros dispositivos portátiles personales que no estén expresamente autorizados por el Responsable de la gestión y coordinación de las medidas de seguridad.
- Comunicar cualquier entrada y/o salida de soportes y documentos que contengan datos de carácter personal.
- *Para los tratamientos con categorías especiales de datos:* Comunicar al Departamento de Sistemas la distribución que se realice de soportes que contengan datos de carácter personal, incluidos, los dispositivos portátiles que se encuentren fuera de las instalaciones de ZFS.

## 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 deberán comunicarse al Departamento de Sistemas.

## Telecomunicaciones

- *Para los tratamientos con categorías especiales de datos:* La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se debe realizar cifrando los datos o bien utilizando mecanismos que garanticen que la información no sea inteligible ni manipulada por terceros. El usuario que lo requiera deberá consultar los procedimientos establecidos y utilizar dichos sistemas de cifrado.

## Uso del Correo Electrónico

- El sistema informático, la red corporativa y los terminales utilizados por cada usuario son propiedad de ZFS. Queda expresamente prohibida la utilización de cuentas de correo electrónico para uso personal.
- ZFS se reserva el derecho a revisar, sin previo aviso, los ficheros LOG de los servidores así como el correo electrónico, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectarle como responsable civil subsidiaria.
- No se deberán abrir correos procedentes de direcciones desconocidas o que no estén relacionadas con motivos de trabajo y ofrezcan las suficientes garantías, con el fin de evitar la entrada de virus.
- Queda estrictamente prohibido el envío de mensajes de correo electrónico de forma masiva o con fines publicitarios o comerciales no solicitados o expresamente autorizados por el destinatario (spam).

- Los mensajes de correo electrónico de la red corporativa que se envíen a múltiples destinatarios con información comercial, noticias, felicitaciones, invitaciones, etc. deben realizarse haciendo uso del campo de copia oculta (CCO) para no desvelar las direcciones de los mismos. Esto no será necesario cuando los correos se envíen a varios destinatarios partícipes en el asunto del correo.
- Su correo electrónico tiene la consideración de herramienta de trabajo. En este sentido, el Responsable de Seguridad o de Departamento podrá revisar el correo electrónico con la finalidad de controlar el uso correcto del mismo, así como el cumplimiento de las funciones y obligaciones propias del puesto de trabajo. De esta forma, el trabajador queda informado de que el resultado de los controles del correo electrónico puede ser utilizado para llevar a cabo, en su caso, actuaciones disciplinarias de acuerdo con la Ley y con el convenio colectivo aplicable.
- Asimismo, en caso de ausencia, baja temporal o definitiva podrá consultar su buzón de correo o redireccionar su cuenta con la finalidad de continuar el normal desarrollo de la actividad del Departamento.

## Acceso a Internet

- Se provee de sistemas de conexión a Internet a los empleados y personal externo para mejorar los sistemas de trabajo y búsqueda de información. Este sistema es propiedad de ZFS y se reserva el derecho de conceder o anular dichos accesos conforme a los criterios que crea convenientes.

- El acceso a Internet se debe limitar a aquellas páginas que contengan información relacionada con la actividad de ZFS o con los cometidos del puesto de trabajo del usuario.
- Queda prohibido el acceso a debates en tiempo real (Chat/IRC) por ser peligrosos al facilitar la instalación de utilidades que permiten accesos no autorizados al sistema.
- ZFS se reserva el derecho de monitorizar, controlar y revisar, de forma aleatoria y sin previo aviso, el uso de Internet y el ordenador con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectarle como responsable civil subsidiaria. El resultado de estas revisiones puede ser utilizado para llevar a cabo, en su caso, actuaciones disciplinarias de acuerdo con la Ley y con el convenio colectivo aplicable.

## Uso de portátiles, smartphones, tabletas digitales.

- No se debe almacenar información corporativa que no sea estrictamente necesaria para el desarrollo del trabajo.
- El usuario es el responsable del equipo portátil o móvil que se le ha facilitado para el desempeño de sus tareas fuera de las instalaciones. Por tanto, es el trabajador el que debe garantizar la seguridad tanto del equipo como de la información que contiene.
- El usuario aplicará las normas recogidas en el presente Manual que sean relativas al uso de un equipo informático (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, etc.).
- Respecto a conexión a redes se deben, en su caso, conectar a redes conocidas y privadas.
- Al conectarse a una red inalámbrica desconocida se debe comprobar que utiliza el protocolo WPA2 y tener en cuenta el uso que se va a hacer de la red para:

- Sólo se deben utilizar redes wifi púbicas no seguras para realizar actividades de bajo riesgo como navegar o leer noticias, pero es necesario asegurarse de que los sitios a los que accedes tienen certificado y utilizan protocolos seguros (https://) si has de iniciar sesión (hacer login) o suscribirte.
- Sólo se deben utilizar redes wifi públicas seguras (al menos con WPA2) si no tienes otro medio más seguro (redes móviles 4G/5G o una VPN) a tu alcance para realizar actividades de alto riesgo (uso de email, trabajar con documentos online, redes sociales, banca online o compras online) comprobando además que se accede a sitos webs legítimos, que utilizan protocolos seguros (https://) y con certificado.

- Se debe notificar al personal técnico responsable la sospecha de infección por virus u otro software malicioso del equipo.
- Se deberán custodiar los soportes móviles cuando se está fuera de las instalaciones. En caso de robo o pérdida del equipo se deberá notificar al personal técnico responsable.
- Si el usuario pretende utilizar soportes móviles de su propiedad, para trabajar con información corporativa deberá contar con autorización de ZFS y cumplir con las Políticas de seguridad establecidas.
- Se debe cifrar la información que contenga categorías especiales de datos o solicitar a Sistemas su cifrado.

## Propiedad Intelectual

- Queda estrictamente prohibido el uso de programas informáticos que no estén homologados por ZFS quien se reserva el derecho de revisar, sin previo aviso, los programas instalados en todos los ordenadores, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectarle como responsable civil subsidiaria.
- Antes de instalar cualquier programa se ha de contactar con el Jefe de Administración y obtener autorización.

## Régimen de trabajo fuera de los locales del responsable o encargado del tratamiento

- Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable o del encargado del tratamiento, será preciso que exista una autorización previa del responsable, y en todo caso deberá garantizarse la aplicación de medidas de seguridad correspondiente al tipo de tratamientos de datos de que se trate.

## Archivos temporales o copias de trabajo de documentos

- Aquellos archivos temporales o copias de documentos creados exclusivamente para la realización de trabajos temporales o auxiliares deben cumplir el nivel de seguridad que les corresponda. Todo archivo temporal o copia de trabajo así

- creado debe ser borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.
- Si en el desarrollo del trabajo se necesita almacenar datos de carácter personal en ordenadores o en cualquier soporte informático, el usuario se responsabiliza de adoptar las medidas de seguridad oportunas mientras dichos datos se mantengan.

## Acceso a través de redes de comunicaciones

- Las medidas de seguridad exigibles a los accesos a datos personales a través de redes de comunicaciones sean o no públicas, deben garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. En caso de desconocer dichos niveles de seguridad abstenerse de su uso y consultar.

## Incidencias

- Es obligación de todo el personal comunicar cualquier incidencia que afecte o pueda afectar a la seguridad de los datos a través del canal que ZFS pone a su disposición. Dicha comunicación deberá realizarse según el **PROCESO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA DE LAS INCIDENCIAS**, en el momento en que se produzca dicha incidencia o desde el momento en que se tenga conocimiento de esta.
- Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos. Algunos ejemplos de incidencias se detallan a continuación:

- **Incidencias que afecten a la confidencialidad:**
  - Lectura no autorizada de la información contenida en los ficheros o sistemas de información.
  - Copia no autorizada de la información.
  - Error en la distribución: que se entreguen informes, soportes, correspondencia, etc. a personas distintas de sus destinatarios.
  - Manipulación no autorizada de la información.
  - Obtención de información desde soportes desechados.
  - Obtención de información desde equipos o soportes destinados a su reutilización.
  - Descifrado de la información o de las claves.

- **Incidencias que afectan a la integridad:**
  - Modificación no autorizada de la información directamente de los ficheros o sistemas de información.
  - Borrado no autorizado de la información.
  - Destrucción parcial o total de la información por fallos en equipos, incendios, inundaciones, tormentas, etc.
  - Imposibilidad de reconstruir los datos partiendo de sus copias de respaldo.
  - Alteración o borrado de la información durante su explotación ocasionado por fallos en el programa.

- **Incidencias que afectan a la disponibilidad:**
  - Modificaciones no autorizadas de permisos de acceso lógico a los ficheros.
  - Imposibilidad o limitación del uso de las instalaciones por fenómenos meteorológicos, huelgas, manifestaciones, etc.

- Indisponibilidad de los sistemas por fallos informáticos.
- Incidencias que afectan a la autenticación:
- Suplantación del usuario autorizado por el no autorizado:
- Por cesión de la clave.
- Por conocimiento de la clave de acceso.
- Por violación de los controles de acceso.
- Fallos en los programas o dispositivos de control de acceso lógico.
- Fallos en la gestión por bajas de personas no comunicadas o autorizaciones de acceso improcedentes.

## Tratamientos de datos en soportes no automatizados.

- Todos los usuarios deberán adoptar las medidas necesarias para asegurar que todos los datos de carácter personal contenidos en tratamientos no automatizados estén debidamente custodiados y protegidos. Serán de aplicación las medidas de seguridad descritas en los apartados anteriores en lo relativo a:
  - Confidencialidad de la información.
  - Control de Acceso.
  - Gestión de soportes y documentos.
  - Registro de incidencias.
  - Régimen de trabajo fuera de los locales del responsable o encargado del tratamiento.
  - Archivos temporales o copias de trabajo de documentos.
- Las siguientes medidas de seguridad se deberán tener en cuenta por el usuario que gestione documentación en papel:

- **Criterios de archivo:** Archivar los soportes o documentos en papel garantizando su correcta conservación, localización y consulta de la información, de modo que posibilite el ejercicio de los derechos por parte del interesado.
- **Dispositivos de almacenamiento:** Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal dispondrán de mecanismos que obstaculicen su apertura. Procurar que los mismos sean debidamente utilizados.
- ***Para los tratamientos con categorías especiales de datos:*** Los armarios, archivadores u otros elementos en los que se almacene documentación con categorías especiales de datos de carácter personal se encontrarán en áreas en las que el acceso esté protegido. Se deben evitar los accesos de personal no autorizado a estas áreas.
- **Custodia de los soportes:** La persona que se encuentre al cargo de documentación con datos personales cuando la misma no esté archivada, por estar en proceso de revisión o tramitación, es responsable de custodiar dicha información y de impedir en todo momento que pueda ser accedida por persona no autorizada.
- **Entrega de documentación en soporte papel:** Queda estrictamente prohibido la entrega o envío de información en soporte papel relativa a personas físicas en sobres, cajas, o cualquier otro recipiente que no esté herméticamente cerrado, y cuya apertura no suponga la rotura del precinto. La entrega se realizará únicamente al titular de los datos o, en su caso, a la persona que haya autorizado por escrito. Asimismo, queda estrictamente prohibido el envío de información relativa a personas físicas, o confidencial a través de medios que no aseguren el cumplimiento de las normas de seguridad exigidas por ZFS.

- **Destrucción de documentación soporte papel:** Para todos los documentos existentes en soporte papel que contengan datos de carácter personal y/o información confidencial existe un sistema de destrucción física de los mismos. Asimismo, queda prohibido deshacerse de la documentación impresa mediante su depósito en papeleras, contenedores o bolsas de basura.
- **Copia o reproducción:** Deben destruirse las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior, siguiendo las instrucciones marcadas en los procedimientos internos.
- ***Para los tratamientos con categorías especiales de datos:*** No realizar copias o reproducción de documentos con categorías especiales de datos, salvo que se cuente con autorización expresa.
- ***Acceso a la documentación para los tratamientos con categorías especiales de datos:*** Acceder exclusivamente a la documentación que se le haya autorizado. El usuario deberá utilizar los mecanismos establecidos que permiten identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

  **Traslado de la documentación para los tratamientos con categorías especiales de datos:** Siempre que se proceda al traslado físico de la documentación personal y/o confidencial, se deben adoptar las medidas tendentes a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte. En este sentido, los envíos pueden realizarse utilizando alguno de los siguientes medios:

  - Empresas de mensajería.
  - Valija interna.
  - Correo certificado.

## Actividades a evitar

- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de ZFS.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar voluntariamente los datos, programas o documentos electrónicos de ZFS o de terceros.
- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de ZFS, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
- Intentar acceder a áreas restringidas de los sistemas de ZFS o de terceros.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema, sin autorización para ello.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por ZFS, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- Borrar voluntariamente cualquiera de los programas instalados legalmente.

- Utilizar los recursos telemáticos de ZFS, incluida la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de ZFS, en la red corporativa del mismo.
- Utilizar ordenadores personales por parte de los empleados de ZFS que no estén expresamente autorizados por la Dirección.

## Violaciones de seguridad

- Estaremos ante una violación de la seguridad cuando se produzca un evento que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, cualquiera que sea la forma de su tratamiento o la comunicación o acceso no autorizados a dichos datos.
- Todo el personal usuario de los soportes o sistemas automatizados o no, que tenga conocimiento de hechos que hayan podido suponer una violación de seguridad que afecte a datos personales, tiene el deber de comunicarla a los responsables de la seguridad de la gestión de datos de ZFS lo antes posible. Reportará toda la información de la que disponga y colaborará en la averiguación de los hechos que dieron lugar a la violación, a fin de poner fin a la situación restaurando los niveles de seguridad de los datos.