Documento de Seguridad

NORD SUD LOGISTICS S.L

DOCUMENTACIÓN L.O.P.D.

*Estos documentos solo existirán en caso de que la empresa recabe datos a través de la página web (8 Informe Web) o existan cámaras de seguridad en las instalaciones de la empresa (10 Videovigilancia).

1. GUÍA DEL USUARIO

1. GUÍA PARA EL DOCUMENTO DE SEGURIDAD
2. GUÍA A TEXTOS Y CONTRATOS
3. CUADRO RESUMEN MEDIDAS DE SEGURIDAD
4. CONTACTO.

1. GUÍA PARA EL DOCUMENTO DE SEGURIDAD

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal, (LOPD) establece en su punto 1 que "el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

Entre estas medidas, se encuentra la elaboración de un documento que debe recoger las medidas de índole técnica y organizativa acorde a la normativa de seguridad vigente que es de obligado cumplimiento para toda entidad jurídica.

Con la finalidad de dar cumplimiento a esta obligación, hemos elaborado para usted el Documento de Seguridad de NORD SUD LOGISTICS S.L que contiene todas las medidas de seguridad vigentes en la empresa. Con el ánimo de facilitarle la labor, al lado de cada una de las medidas que no estaban debidamente desarrolladas, hemos incluido una recomendación para que dicha medida sea subsanada y se adecúe correctamente a lo establecido en la legislación vigente en materia de protección de datos.

¿Qué debe hacer usted, por tanto? A partir de ahora, debe revisar lo expuesto en el documento de seguridad y realizar los cambios oportunos en el seno de la empresa para que las medidas implementadas en la misma sean acordes a lo establecido en la normativa en relación con el nivel de datos que trata en NORD SUD LOGISTICS S.L ..

Con nuestra ayuda, podrá proceder a la implementación de dichas medidas sin mayor pérdida de tiempo. Si tiene cualquier duda, no tiene más que contactar con nuestro departamento jurídico a través de los canales de comunicación de manera que le ayuden a solventar cualquier duda que le pueda surgir.

2. GUÍA PARA TEXTOS Y CONTRATOS

Una parte importante de cualquier adaptación son los textos jurídicos y los contratos que regulan las relaciones de NORD SUD LOGISTICS S.L con terceras personas, ya que las mismas son las que pueden generar mayor problemática en relación con la protección de datos. Es por ello que todas esas relaciones deben estar bien reguladas para evitar posibles complicaciones con la Agencia Española de Protección de Datos.

Para ello, les facilitamos los textos jurídicos que pueden ver a continuación, de forma que los firmen con los terceros interesados.

- Información y consentimiento: Las cláusulas informativas y de consentimiento que GRUPO OCLEM le ha facilitado en el documento "Textos Jurídicos", se deberán comunicar debidamente a los titulares de los datos (clientes, proveedores, etc.).
- Prestación de servicios sin acceso a datos: Se deberá firmar la cláusula de prohibición de acceso a datos facilitada por GRUPO OCLEM en el documento "Textos Jurídicos", con todas las entidades que presten sus servicios en las oficinas de la entidad y para los que no se requiera acceso a los datos (ej. Servicio de limpieza).
- Contrato Tratamiento por cuenta de Terceros: Se deberá firmar el contrato de tratamiento por cuenta de terceros facilitado por GRUPO OCLEM en el documento "Documento para empresas con acceso a datos", con todos los proveedores que presten sus servicios para los que se requiera el acceso a los datos (ej. Gestoría, mantenimiento informático).
- Funciones y Obligaciones del Personal: Los empleados deberán firmar "Cláusula informativa para empleados en régimen laboral al igual que "Compromiso de confidencialidad y secreto" incluidos en el apartado "Documentos para empleados".
- Aviso Legal y LOPD Web: En caso de que disponga de sitio web, deberá incluir el Aviso Legal facilitado por GRUPO OCLEM en el documento "Informe Web" a través de un link que se encuentre visible en todas las páginas del sitio web. Si además el sitio web dispone de formulario de recogida de datos, deberá incluir otro link con la cláusula de protección de datos contenida en el apartado LOPD y LSSI en la web del citado "Informe Web". Se incluye también la política de cookies para el caso de que su página las utilice, obligatoria por Real Decreto-Ley de 31 de marzo de 2014.

3. CUADRO RESUMEN MEDIDAS DE SEGURIDAD

Soporte automatizado / soporte informático

	Nivel básico	Nivel medio	Nivel alto
Funciones y Obligaciones del personal	✓	✓	✓
Registro de incidencias	✓	✓	✓
Control de acceso	✓	✓	✓
Gestión de soportes y documentos	✓	✓	✓
Reconocimiento de la identidad	✓	✓	✓
Copias de seguridad (backup)	✓	✓	✓
Copias de respaldo y de recuperación	✓	✓	✓
Responsable de seguridad		✓	✓
Auditoria		✓	✓
Gestión de contraseñas		✓	✓
Control de acceso físico		✓	✓
Transporte seguro (cifrado)			✓
Copias de seguridad cifradas			✓
Registro de accesos			✓
Telecomunicaciones			✓

Los ficheros contenidos en **soportes automatizados** son aquellos que almacenan la información en soportes informáticos (bases de datos, archivos, carpetas, Excel, tablets, dispositivos móviles, TPV).

Funciones y obligaciones del personal: En el documento de seguridad podrá encontrar cuáles son las funciones y obligaciones del personal que tenga acceso a los datos:

1. El responsable del fichero adoptará las medidas necesarias para que el personal de NORD SUD LOGISTICS S.L conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.
2. Funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información que estarán claramente definidos y documentados en el documento de seguridad que GRUPO OCLEM ha realizado para su empresa.

Registro de incidencias: Todo fichero automatizado deberá tener un Registro de Incidencias en el que aparecerá cualquier anomalía que afecte o puede afectar a la seguridad de los datos de carácter personal. Ante cualquier tipo de incidencia es necesario que se ponga en contacto con el personal del Departamento Jurídico de GRUPO OCLEM .

Ante datos que requieran nivel de seguridad medio o alto, se necesita autorización del Responsable del Fichero para llevar a cabo los procedimientos de recuperación de datos (a través de las copias de seguridad). Se deberá indicar la persona que ejecutó el proceso de recuperación de los datos, los datos recuperados.

Control de acceso: en todos los ficheros se debe implantar el mecanismo que controle el acceso de los usuarios a los datos de carácter personal:

1. Los usuarios únicamente tendrán acceso a los datos necesarios para cumplir con sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada entre usuarios y perfiles de usuarios. El responsable del fichero establecerá mecanismos para impedir que los usuarios sin autorización accedan a información no necesaria para el desempeño de sus funciones.

Gestión de soportes y documentos: la salida de soportes (dispositivos móviles, tablets, ordenadores, USB, memorias externas) y documentos que contengan datos de carácter personal fuera de NORD SUD LOGISTICS S.L deberá ser autorizado por el control de responsable del fichero o tratamiento, y se debidamente anotado en los Anexos del Documento de Seguridad que GRUPO OCLEM les ha facilitado. El traslado de esta documentación se adoptará las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información. Antes de desechar cualquier tipo de documento o soporte (dispositivos móviles, tablets, ordenadores, USB, memorias externas) deberá procederse a su destrucción o borrado. Mediante la adopción de medidas que eviten la lectura o el conocimiento de dichos datos por personas no autorizadas. Con carácter extraordinario deberá realizarse dicha auditoria

cuando se realicen modificaciones en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad.

Registro de entrada y salida: deberá establecerse un sistema de registro de entrada y salida que permita conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos de soportes, el tipo de información, y en caso de ser enviado la forma de envío, la persona responsable de la recepción.

Gestión de contraseñas: En el caso de ficheros de nivel medio o alto, se deberán bloquear los equipos, dispositivos, soportes (dispositivos móviles, tablets, ordenadores, USB, memorias externas, etc.), programas, gestores de datos u sistemas análogos, en caso de intentos de accesos fallidos o con contraseñas incorrectas.

Reconocimiento de la identidad: el responsable del fichero deberá adoptar un mecanismo que garantice la correcta identificación y comprobación de la identidad de las personas que acceden a datos de carácter personal en los siguientes términos: mecanismos que permitan la identificación de forma inequívoca y personalizada de todo aquél usuario que intenta acceder al sistema de información, y la comprobación de que esté autorizado. Lo más común es que el mecanismo utilizado sea mediante "usuario y contraseña". Existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad. **Las contraseñas deberán ser cambiadas con una periodicidad mínima anual., y en caso de ser almacenadas se harán de formas cifradas o ininteligibles.**

Copias de seguridad (back up): en todos los ficheros automatizados el responsable del fichero debe establecer un procedimiento que permita realizar copias de seguridad semanalmente de todos aquellos datos de carácter personal que queden almacenados en algún soporte (dispositivos móviles, tablets, ordenadores, USB, memorias externas, etc.) Dicho procedimiento debe cumplir con los siguientes requisitos:

1. Realizarlo semanalmente, salvo que no haya producido modificación de los datos.
2. El responsable del fichero comprobará cada seis meses el correcto funcionamiento de las copias de seguridad.
3. Se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción al estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Responsable de seguridad: cuando se traten con datos que requieran de un nivel de seguridad medio o alto, en el Anexo del Documento de Seguridad, deberá designarse uno o varios en función del tamaña de la compañía. Las funciones del Responsable de Seguridad serán: coordinar y controlar las medidas definidas en el Documento de Seguridad.

Auditoría: los ficheros que requieran un nivel de seguridad medio o alto se deberá realizar cada dos años una auditoria que compruebe que los sistemas de información e instalaciones donde se tratan,

almacenan los datos de carácter personal cumplen con las medidas de seguridad previstas en el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (LOPD).

Control de accesos físicos: ante ficheros que requieran nivel de seguridad medio o alto, solamente podrán acceder a los lugares donde se hallen instalados los equipos físicos que sirven de soporte para tratar los datos de carácter personal las personas autorizadas en el Documento de Seguridad.

Transporte seguro (cifrado): el traslado de dispositivos móviles, tablets, ordenadores, USB, memorias externas, etc. que contengan datos de carácter personal se deberán realizar utilizando algún mecanismo que dicha información no se accesible o no sea manipulada durante su transporte, como por ejemplo, el cifrado. Deberá evitarse el traslado en caso de no poderse adoptar las medidas citadas.

Copias de seguridad cifradas: ante datos que requieran nivel de seguridad alto la copia de respaldo o seguridad, deberá estar en un lugar diferente de aquél en el que se encuentren los equipos informáticos que lo tratan.

Registro de accesos: ante datos que requieran de un nivel de seguridad alto, será exigible un sistema que registre el acceso a la información:

1. No será necesario el registro de accesos, que a continuación se define, en caso de que, el responsable del fichero garantice que únicamente será él quien acceda y trate datos personales.
2. Cada intento de acceso se guardará la persona que intentó conocer esa información, la fecha, hora, el fichero al que accedió y si se le autorizó o no.
3. En caso de que autorizase, será preciso guardar la información que permita identificar al registro accedido. Los mecanismos que permita el registro de accesos estarán bajo el control del responsable de seguridad sin que sea posible la manipulación o desactivación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. Una vez al mes el Responsable de Seguridad revisará la información del registro, así como los problemas detectados.

Telecomunicaciones: ante datos que requieran un nivel de seguridad nivel alto, la transmisión de comunicaciones electrónicas deberá realizarse de manera que la información no pueda ser leída ni manipulada por terceros.

Ficheros no automatizados / soporte papel

	Nivel básico	Nivel medio	Nivel alto
Funciones y Obligaciones del personal	✓	✓	✓
Registro de incidencias	✓	✓	✓
Gestión de soportes y documentos	✓	✓	✓
Criterios de archivo	✓	✓	✓
Dispositivos de almacenamiento	✓	✓	✓
Custodia de los soportes	✓	✓	✓
Responsable de seguridad		✓	✓
Auditoria		✓	✓
Almacenamiento de la información			✓
Copia o reproducción			✓
Traslado de la documentación			✓
Acceso /Control de acceso			✓

Los ficheros contenidos en soportes **no automatizados** son un conjunto de datos de carácter personal que se contienen en soporte papel de forma clasificada.

Funciones y obligaciones del personal: el Documento de Seguridad define cuáles son las funciones obligaciones del personal que tenga acceso a datos de carácter personal.

Registro de incidencias: deberá existir un registro de incidencias en el que se hará constar el tipo de incidencia, el momento (fecha y hora) que se ha producido o detectado, la empresa que realice la notificación a quien se le comunica, los efectos que se hubiesen derivado de la misma, y las medidas correctoras aplicadas.

Gestión de soportes y documentos: los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y sólo deberán ser accesibles el personal autorizado para ello en los Anexos del Documento de Seguridad.

La salida de documentos que contengan datos personales de NORD SUD LOGISTICS S.L deberán ser autorizados por el Responsable del Fichero o actualizado en el Documento de Seguridad.

El traslado de documentos se deberá evitar el robo, pérdida, lectura indebida de la información.

Cuando se deseche cualquier documento que contengan datos de carácter personal deberá ser destruido de forma que se evite acceder a su contenido.

Criterios de archivo: los documentos que contengan datos personales debe realizarse de forma que se garantice la correcta conservación de los documentos, se facilite la localización de la información y se posibilite el ejercicio de los Derechos ARCO.

Dispositivos de almacenamiento: el Responsable del Fichero deberá adoptar medidas que impidan el acceso de personas no autorizadas a los documentos. Esta labor se realizará mediante mecanismos que obstaculicen su acceso o la apertura de lugares donde estén los documentos.

Custodia de los soportes: las personas que se encuentren al cargo de documentos que contengan datos de carácter personal deberán custodiar e impedir que en todo momento personas no autorizadas puedan acceder a la información contenida en los documentos que esté tratando.

Responsable de seguridad: cuando traten con datos en ficheros no automatizados que requieran de un nivel de seguridad medio o alto, se designará uno o varios responsables de seguridad en función del tamaño de la empresa. Las funciones del Responsable de Seguridad serán: coordinar y controlar las medidas definidas en el Documento de Seguridad.

Auditoría: los ficheros que requieran un nivel de seguridad medio o alto se deberá realizar cada dos años una auditoria que compruebe que los sistemas de información e instalaciones donde se tratan, almacenan los datos de carácter personal cumplen con las medidas de seguridad previstas en el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (LOPD).

Almacenamiento de la información: los ficheros no automatizados que contengan datos personales que requieran de un nivel alto de seguridad serán almacenados con los siguientes requisitos:

1. Armarios, archivadores en los que se almacenen los documentos deberán encontrarse en aéreas en las que el acceso esté protegido con puertas dotadas con sistema de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso acceder a los documentos.
2. Si atendidas las características de los locales de su empresa en el que dispusiera el Responsable del Fichero del Tratamiento no fuera posible cumplir lo estipulado en el apartado anterior, el Responsable adoptará medidas alternativas que motivará e incluirá en el Documento de Seguridad.

Copia o reproducción: cuando se trate de ficheros con un nivel de seguridad nivel alto de seguridad la generación de copias con datos personales únicamente podrá ser realizada en los siguientes términos:

1. Podrá ser realizada bajo el control del personal autorizado en el Documento de Seguridad.
2. Deberá procederse a la destrucción de las copias que no sean necesarias, de forma quemse evite su lectura.

Traslado de la documentación: cuando se traten datos que contengan datos de carácter personal el traslado físico de la documentación deberá realizarse de manera que no pueda ser acceder o manipular.

Acceso / Control de acceso: cuando se traten datos personales que requieran un nivel alto de documentación, deberán realizarse el tratamiento siguiendo los siguientes requisitos:

1. Sólo podrá acceder a la documentación el personal autorizado
2. Se establecerán mecanismos que permitan identificar los accesos realizados y las personas que los llevaron a cabo.
3. En el caso de que accedan personas no autorizadas deberá quedar reflejado en el Documento de Seguridad.

Control de acceso: en todos los ficheros se debe implantar el mecanismo que controle el acceso de los usuarios a los datos de carácter personal:

1. Los usuarios únicamente tendrán acceso a los datos necesarios para cumplir con sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada entre usuarios y perfiles de usuarios. El responsable del fichero establecerá mecanismos para impedir que los usuarios sin autorización accedan a información no necesaria para el desempeño de sus funciones.

2 DOCUMENTO DE SEGURIDAD

1. APROBACIÓN OFICIAL DEL DOCUMENTO DE SEGURIDAD

La DIRECCIÓN de NORD SUD LOGISTICS S.L .(en adelante NORD SUD LOGISTICS S.L) aprueba, con fecha 02 de Noviembre de 2016, el presente Documento de Seguridad y lo asume como propio de NORD SUD LOGISTICS S.L .

La DIRECCIÓN de NORD SUD LOGISTICS S.L ha adoptado las medidas necesarias para que todos los profesionales de su organización estén familiarizados con la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD), que establece las obligaciones y procedimientos tendentes a garantizar y proteger los derechos de los titulares de datos personales.

Todos los profesionales de NORD SUD LOGISTICS S.L con acceso a datos personales deberán cumplir las prescripciones contenidas en el presente Documento de Seguridad, así como las medidas de seguridad en él contempladas.

Así mismo la DIRECCIÓN de NORD SUD LOGISTICS S.L ha establecido las funciones y responsabilidades necesarias para cumplir y hacer cumplir en todo momento la citada Ley, haciendo especial énfasis en los procedimientos y medidas de seguridad a adoptar por aquellos profesionales que tienen acceso a datos de carácter personal.

Este documento se mantendrá actualizado y será revisado siempre que se produzcan cambios relevantes en la información u organización del mismo. El contenido se adecuará en todo momento a las disposiciones legislativas vigentes en materia de seguridad de los datos de carácter personal, protegiendo NORD SUD LOGISTICS S.L adecuadamente la información conforme a la legislación mencionada.

En Madrid a 02 de Noviembre de 2016

LA DIRECCIÓN

2. INTRODUCCION

Las Tecnologías de la Información fomentan la utilización de la informática tanto en las grandes como en las pequeñas y medianas empresas, facilitando y agilizando el tratamiento de datos.

Si bien lo anterior supone grandes avances desde el punto de vista de la gestión y eficiencia desde el punto de vista del negocio, también aumenta el riesgo de vulneración de los DerechosFundamentales de las personas titulares de datos personales.

La confidencialidad de los datos personales y el derecho a la intimidad de las personas físicas pueden verse amenazados dados los avances tecnológicos que permiten la transmisión y fuga de datos personales con un mínimo esfuerzo, si no se realiza un adecuado uso de las tecnologías de la información y se incorporan los controles necesarios.

Ante esta nueva realidad tecnológica, el legislador promulga una serie de normas que tienen por objeto garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, en lo que concierne al tratamiento de los datos personales.

La Constitución española, en su artículo 18.4, establece que:

"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

En desarrollo de este precepto constitucional se ha elaborado una normativa específica sobre Protección de Datos de Carácter Personal, tanto a nivel de Ley, como de Reglamentos:

- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que establece una serie de obligaciones y procedimientos tendentes a garantizar y proteger los derechos de los titulares de datos personales.
- **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 (RLOPD).
- **Ley 34/2002,** de 11 de Julio, de servicios de la sociedad de la información y de comercio electrónico.

A partir de dicha legislación se han establecido distintas medidas las cuales se pueden agrupar de la siguiente manera:

- Jurídicas
- Organizativas
- Técnicas

Las medidas **jurídicas** se recogen en el articulado de la LOPD, la cual se remite al RLOPD para regular las medidas **técnicas** y **organizativas**.

La Protección de los Datos de Carácter Personal es una obligación impuesta a toda entidad que posea ficheros con datos personales. Cualquier empresa que disponga de nombres y apellidos en un fichero de su ordenador o en soporte papel, siempre y cuando estén organizados, debe de adaptarse a la LOPD, debiendo implantar una correcta Política de Protección de Datos dentro de la organización.

3. OBJETO DEL DOCUMENTO DE SEGURIDAD

El presente Documento de Seguridad responde a la obligación establecida en artículo 88 del RLOPD y tiene como objetivo describir las medidas de seguridad de índole organizativa y técnica que garantizan

la confidencialidad, integridad y disponibilidad de la información contenida en los ficheros con datos de carácter personal.

La finalidad del Documento de Seguridad es dar transparencia al sistema de tratamiento de los datos personales, plasmando en el mismo los siguientes aspectos:

- Personas autorizadas para acceder a los datos.
- Herramientas utilizadas y sistemas que procesan y tratan los datos.
- Soportes que contienen y almacenan los datos.
- Cualquier otro aspecto relativo al tratamiento de los datos.

Es responsabilidad de NORD SUD LOGISTICS S.L adoptar las medidas de índole técnico y organizativo que garanticen el nivel de seguridad exigido para el tratamiento automatizado de los datos de carácter personal, evitando su alteración, pérdida, tratamiento o acceso no autorizado, teniendo en cuenta la naturaleza de los mismos y los riesgos a los que están expuestos.

Además la legislación vigente impone el deber de **secreto profesional** tanto al Responsable del Fichero, como a quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, aún después de finalizar sus obligaciones con el Responsable del Fichero.

Por otro lado, en el presente Documento de Seguridad se determinan los procedimientos y normas de seguridad adoptados con la finalidad de preservar la integridad, confidencialidad y disponibilidad de los datos personales, así como el procedimiento de su publicación para que sea conocido por todos los profesionales que intervienen en su tratamiento.

Por todo ello, se elabora este Documento de Seguridad, en el que se recogen las directrices del Reglamento, en lo que respecta a Medidas de Seguridad de **nivel básico, medio y alto.**

Además se nombra a un Responsable de Seguridad de NORD SUD LOGISTICS S.L , como encargado de coordinar y controlar las medidas definidas en este documento y de verificar el cumplimiento de los controles periódicos a realizar para cada fichero.

Cualquier modificación debidamente informada y documentada de las circunstancias organizativas, normativas o técnicas en relación con un fichero de datos de carácter personal, conllevará la revisión y actualización por parte del Responsable de Seguridad del presente documento.

A continuación se detallan todos aquellos ficheros inscritos en el RGPD, y que constituyen la base del Sistema de Información del presente Documento de Seguridad:

- NOMINAS ,PERSONAL Y RRHH **Nivel de Seguridad BÁSICO**
- VIDEOVIGILANCIA **Nivel de Seguridad BÁSICO**

4. AMBITO DE APLICACIÓN

4.1 INTRODUCCIÓN

En base a la legislación anteriormente citada, se desarrolla este Documento de Seguridad en el que se exponen las medidas técnicas y organizativas que garantizan la confidencialidad, integridad y

disponibilidad de los datos de carácter personal, así como la responsabilidad de NORD SUD LOGISTICS S.L de preservar el honor y la intimidad personal y familiar de las personas afectadas. Por tanto, el presente documento es aplicable a los ficheros, automatizados o no, existentes en NORD SUD LOGISTICS S.L .

El Artículo 81 del Reglamento de Desarrollo de la LOPD diferencia tres niveles de seguridad: básico, medio y alto, atendiendo a la naturaleza de los datos y a la necesidad de confidencialidad en la Información.

- Nivel básico, exigibles a ficheros con datos de carácter personal.
- Nivel medio, exigibles a los que contienen datos relativos a la hacienda, información de solvencia patrimonial y crédito, infracciones administrativas y/o penales, o ficheros con datos que definan el perfil psicológico de cualquier persona.
- Nivel alto, exigibles a los que contienen datos sobre ideología política, religión, creencias, origen racial, salud o vida sexual.

En el caso de los ficheros propiedad de NORD SUD LOGISTICS S.L los ficheros y niveles de seguridad son los que se incluyen en el Apartado 6, correspondiente a la descripción de los ficheros.

Dada la naturaleza de los ficheros de NORD SUD LOGISTICS S.L y las notificaciones de inscripción de ficheros a la Agencia Española de Protección de Datos, el presente Documento de Seguridad aplicará las medidas de seguridad correspondientes al nivel de seguridad ALTO, MEDIO y BÁSICO, según el fichero a tratar.

Debido a lo anterior, serán de aplicación todas las Medidas de Seguridad de Nivel Básico, Medio y Alto que se establecen en el Reglamento de desarrollo de la LOPD (RLOPD), sin perjuicio de adoptar para cada uno de los ficheros las medidas que les correspondan en función de los datos que estén contenidos en ellos.

Asimismo, estas medidas afectan a los Sistema Informáticos que almacenan y tratan la información, así como a cualquier otro medio automatizado o no de acceso a los ficheros.

4.2 ÁMBITO DE APLICACIÓN MATERIAL

Las medidas descritas en el presente Documento de Seguridad serán de aplicación en NORD SUD LOGISTICS S.L , Responsable de los Ficheros descritos anteriormente, en relación a los siguientes recursos protegidos:

Los ficheros de datos de carácter personal inscritos en el “Registro General de la Agencia Española de Protección de Datos”, así como a todos los ficheros que se creen en un futuro, que contengan datos de carácter personal. Dichos ficheros con sus correspondientes niveles se encuentran referenciados en el Apartado 6.

- Los centros de tratamiento y locales donde se encuentran ubicados los ficheros o se almacenen los soportes que los contengan.
- Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso a los ficheros.
- Los servidores y el entorno de los sistemas y comunicaciones en el que se encuentran ubicados los ficheros.

- Las aplicaciones informáticas disponibles para acceder a los datos.

4.3 ÁMBITO DE APLICACIÓN PERSONAL

Este documento es aplicable a quien, teniendo acceso a la información, preste servicios para NORD SUD LOGISTICS S.L , incluso en el supuesto de que la naturaleza de su relación no tenga carácter laboral y/o se haya extinguido el mismo.

Todas las personas que tengan acceso a los datos de los ficheros, bien a través de los sistemas informáticos o bien a través de cualquier otro medio automatizado o no de acceso a los mismos, se encuentran obligadas por Ley a cumplir lo establecido en el Documento de Seguridad y están sujetas a las consecuencias que pudieran derivarse en caso de incumplimiento.

Cada profesional autorizado a acceder a datos de carácter personal deberá recibir una copia de la parte correspondiente al Documento de Seguridad que le afecte, siendo requisito obligatorio para poder acceder a esos datos haber firmado su recepción.

4.4 ÁMBITO DE APLICACIÓN FUNCIONAL

Las medidas de seguridad que se adopten en este Documento serán de aplicación tanto en el local de NORD SUD LOGISTICS S.L , como en cualquier otro lugar en el que NORD SUD LOGISTICS S.L autorice el tratamiento de los datos, tanto a trabajadores de la propia empresa como a terceras personas, mediante una relación contractual.

Es decir, los ficheros automatizados cuyo tratamiento o explotación sean realizados por una empresa o terceras personas externas, a través de un contrato de prestación de servicios y fuera de las instalaciones de NORD SUD LOGISTICS S.L , están sometidos a la misma Política de Seguridad que aquéllos cuyo tratamiento se realiza en las instalaciones de NORD SUD LOGISTICS S.L .

Es, por tanto, responsabilidad de estos terceros adecuar las medidas de seguridad necesarias en los equipos informáticos, aplicaciones e instalaciones en las que se encuentren los ficheros.

5. DEFINICIONES LEGALES

- **AEPD:** Agencia Española de Protección de Datos de carácter personal, ente público cuya función principal es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- **LOPD:** Ley Orgánica de Protección de Datos de Carácter Personal 15/1999.
- **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables.
- **Fichero:** Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- **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 que resulten de comunicaciones, consultas, interconexiones y transferencias.
- **Tratamiento Automatizado:** Cualquier operación o procedimiento técnico que permita la recogida, grabación, conservación, elaboración, modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los datos, cotejo o interconexión así como su bloqueo o cancelación.
- **Responsable del Fichero o tratamiento:** Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
- **Afectado o interesado:** Persona física titular de los datos que sean objeto del tratamiento.
- **Usuario:** sujeto o proceso autorizado para acceder a datos o recursos.
- **Responsable de Seguridad:** Persona o personas a las que el Responsable del Fichero ha asignado formalmente la función de coordinar y controlar las Medidas de Seguridad aplicables.
- **Encargado del tratamiento:** La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
- **Consentimiento del interesado:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- **Cesión o comunicación de datos:** Toda revelación de datos realizada a una persona distinta del interesado.
- **Sistema de información:** Conjunto de ficheros automatizados, programas soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
- **Recurso:** Cualquier parte o componente de un sistema de información.
- **Accesos autorizados:** Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.
- **Identificación:** Procedimiento de reconocimiento de la identidad de un usuario.
- **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.
- **Control de acceso:** Mecanismo que en función de la identificación ya autenticada permite acceder a los datos y recursos.
- **Incidencia:** Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
- **Soporte:** Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

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

6. IDENTIFICACIÓN DE LOS RESPONSABLES Y RECURSOS PROTEGIDOS

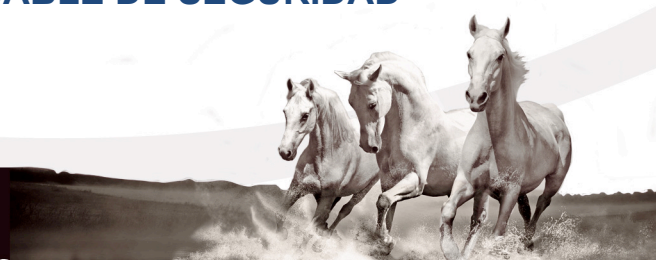
6.1 IDENTIFICACIÓN DEL RESPONSABLE DEL FICHERO

Responsable del Fichero	**NORD SUD LOGISTICS S.L .**
C.I.F.:	**B85512788**
Dirección:	**Calle Bronce 33-34 CP:28890 Loeches**
Representante:	**Angel Ramos**

6.2 PERSONAL CON ACCESO AL CENTRO DE PROCESAMIENTO DE DATOS (CPD)

Nombre y apellidos	N.I.F.	Puesto

6.3 IDENTIFICACIÓN RESPONSABLE DE SEGURIDAD



Responsable de Seguridad	Angel Ramos
N.I.F.	50946037W
Puesto	**Dirección**

6.4 CENTROS DE TRATAMIENTO

El centro de tratamiento de los datos contemplan las medidas de seguridad física y de control de acceso necesarias para garantizar la disponibilidad y confidencialidad de los datos.

El acceso físico al centro de tratamiento de datos de carácter personal está restringido única y exclusivamente a los profesionales referenciados en él.

CENTRO 1	**NORD SUD LOGISTICS S.L .**
Dirección	**Calle Bronce 33-34 CP:28890 Loeches**

6.5 RECURSOS PROTEGIDOS

Los recursos protegidos son todos aquellos datos de carácter personal incluidos en los diferentes ficheros existentes, es por ello, que en cumplimiento del artículo 26 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se han inscrito en el Registro General de la Agencia Española de Protección de Datos los Ficheros existentes en NORD SUD LOGISTICS S.L .

Dichos ficheros así como todas sus características, están descritos en el Apartado 7.

DESCRIPCIÓN DE LOS FICHEROS.

Datos de los Equipos

Los sistemas informáticos de **NORD SUD LOGISTICS S.L** serán detallados en los siguientes registros:

1 ENTORNOS DE LAS COMUNICACIONES.

2 EQUIPAMIENTO Y SISTEMA INFORMATICO

3 PROGRAMAS Y APLICACIONES INFORMATICAS

7. DESCRIPCIÓN DE LOS FICHEROS

7.1 FICHERO: NÓMINAS Y PERSONAL

Sistema	SOPORTE PAPEL Y MICROSOFT OFFICE
Nº Inscripción RGPD	
Nivel de Seguridad	BÁSICO
Procedencia	DEL PROPIO INTERESADO
Procedimiento de Recogida	ENTREVISTAS Y CONTRATOS
Soporte de obtención	SOPORTE PAPEL, TELEMÁTICA Y DIGITAL

7.1.1 DESCRIPCIÓN

Datos relativos a los contratos que NORD SUD LOGISTICS S.L firma con sus trabajadores.

7.1.2 FINALIDAD

Los datos recabados por **NORD SUD LOGISTICS S.L** tienen como finalidad la gestión del personal para cubrir puestos necesarios según las necesidades de NORD SUD LOGISTICS S.L .

7.1.3 ESTRUCTURA

El fichero en cuestión tiene la estructura determinada en la declaración de ficheros inscrito ante la AEPD, que se adjunta a continuación.

DATOS DE CARÁCTER IDENTIFICATIVO
DNI/NIF
NOMBRE Y APELLIDOS
Dirección (postal, electrónica)
TELÉFONO

IMAGEN / VOZ
DATOS DE CARACTERÍSTICAS PERSONALES
DATOS DE ESTADO CIVIL
FECHA DE NACIMIENTO
LUGAR DE NACIMIENTO
EDAD
SEXO
NACIONALIDAD
LENGUA MATERNA
DATOS DE CIRCUNSTANCIAS SOCIALES
FORMACIÓN, TITULACIONES
EXPERIENCIA PROFESIONAL
PERTENENCIA A COLEGIOS Y ASOCIACIONES DE PROFESIONALES
SANCIONES ADMINISTRATIVAS
DATOS DE DETALLES DE EMPLEO
PROFESIÓN
PUESTO DE TRABAJO

7.1.4 CESIONES DE DATOS

A menudo las empresas comunican datos de carácter personal de sus ficheros para el cumplimiento de fines directamente relacionados con la actividad empresarial con el previo consentimiento del interesado, salvo que, la cesión esté autorizada por una ley o cuando ésta responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implica necesariamente la conexión con ficheros de terceros, siempre y cuando se limite a la finalidad que lo justifique.

NORD SUD LOGISTICS S.L , cede datos de sus empleados a las Administraciones públicas correspondientes por imperativo legal y a las cajas y bancos para el pago de las nóminas.

7.1.5 ENCARGADOS DE TRATAMIENTO

Es posible el tratamiento de datos por terceros como parte de los procedimientos administrativos y comerciales convencionales.

Siempre que un tercero tenga que tratar de datos de NORD SUD LOGISTICS S.L han de contemplarse los siguientes aspectos:

El tratamiento debe tener siempre un carácter temporal.

Ha de firmarse un contrato de acceso a datos entre las partes, en el cual debe de contemplarse:

- Responsabilidades.
- Ficheros de datos de carácter personal que se tratan.
- Medidas de seguridad que aplica el tercero en función de los datos que se tratan.

Es necesario que los datos que vayan a ser tratados por terceros, ya sean empresas o personas físicas estén sujetos a una relación contractual que regule los distintos aspectos necesarios para garantizar la confidencialidad, integridad y disponibilidad de dichos datos.

Los encargados del tratamiento se encuentran reflejados en el **DOCUMENTO NÚMERO 7 "EMPRESAS CON ACCESO A DATOS".**

7.1.6 RELACIÓN ACTUALIZADA DE USUARIOS AUTORIZADOS

Nombre	**Departamento**
Angel Ramos	**Dirección**

7.2 FICHERO: VIDEOVIGILANCIA

Sistema	VIDEOVIGILANCIA
Nº Inscripción RGPD	
Nivel de Seguridad	BÁSICO
Procedencia	DEL PROPIO INTERESADO
Procedimiento de Recogida	CAMARAS DE VIDEOVIGILANCIA
Soporte de obtención	CAMARAS DE VIDEOVIGILANCIA

7.2.1 DESCRIPCIÓN

Grabaciones realizadas a través de las cámaras para la vigilancia y control de acceso a las instalaciones de la empresa.

7.2.2 FINALIDAD

Los datos recabados por **NORD SUD LOGISTICS S.L** tienen la finalidad de gestionar la seguridad del establecimiento.

7.2.3 ESTRUCTURA

El fichero en cuestión tiene la estructura determinada en la declaración de ficheros inscrito ante la AEPD, que se adjunta a continuación.

DATOS DE CARÁCTER IDENTIFICATIVO
IMAGEN / VOZ

7.2.4 CESIONES DE DATOS

A menudo las empresas comunican datos de carácter personal de sus ficheros para el cumplimiento de fines directamente relacionados con la actividad empresarial con el previo consentimiento del interesado, salvo que, la cesión esté autorizada por una ley o cuando ésta responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implica necesariamente la conexión con ficheros de terceros, siempre y cuando se limite a la finalidad que lo justifique.

NORD SUD LOGISTICS S.L , podría hacer cesión de sus datos a compañías de seguridad.

7.2.5 ENCARGADOS DE TRATAMIENTO

Es posible el tratamiento de datos por terceros como parte de los procedimientos administrativos y comerciales convencionales.

Siempre que un tercero tenga que tratar de datos de NORD SUD LOGISTICS S.L han de contemplarse los siguientes aspectos:

El tratamiento debe tener siempre un carácter temporal.

Ha de firmarse un contrato de acceso a datos entre las partes, en el cual debe de contemplarse:

- Responsabilidades.
- Ficheros de datos de carácter personal que se tratan.
- Medidas de seguridad que aplica el tercero en función de los datos que se tratan.

Es necesario que los datos que vayan a ser tratados por terceros, ya sean empresas o personas físicas estén sujetos a una relación contractual que regule los distintos aspectos necesarios para garantizar la confidencialidad, integridad y disponibilidad de dichos datos.

Los encargados del tratamiento se encuentran reflejados en el **DOCUMENTO NÚMERO 7 "EMPRESAS CON ACCESO A DATOS".**

7.2.6 RELACIÓN ACTUALIZADA DE USUARIOS AUTORIZADOS

Nombre	Departamento
Angel Ramos	**Dirección**

8. MANUAL DE FUNCIONES Y OBLIGACIONES DEL PERSONAL

8.1 FUNCIONES DEL PERSONAL

Las distintas funciones que deben existir dentro de la organización de NORD SUD LOGISTICS S.L , con responsabilidades en el tratamiento de datos de carácter personal, son las siguientes

8.1.1 RESPONSABLE DEL FICHERO O TRATAMIENTO

El Responsable del Fichero o Tratamiento es la propia empresa**.**

La Dirección de **NORD SUD LOGISTICS S.L** como representante legal de la misma, será quien decida sobre la finalidad, ontenido y uso de los datos contenidos en un fichero y será el encargado de implantar lo establecido en el presente Documento, adoptando las medidas necesarias para que los profesionales con acceso a los datos personales conozca las normas que afecten al desarrollo de sus funciones.

En el caso de **NORD SUD LOGISTICS S.L** , aunque la responsabilidad legal ante la AEPD es de la propia Sociedad, la ejecución de las tareas y las obligaciones asignadas al Responsable del Fichero serán llevadas a cabo por el Responsable de seguridad de la misma.

El Responsable del Fichero designará al Responsable de Seguridad, que en este caso coinciden en la misma persona.

8.1.2 RESPONSABLE DE SEGURIDAD

El Responsable de Seguridad, será designado por el Responsable del Fichero y será el encargado de oordinar y controlar las medidas establecidas en el presente documento, así como de administrar y mantener el entorno operativo de los Ficheros.

8.1.3 USUARIOS

Se entenderá por usuarios, el personal que habitualmente utiliza el sistema informático de acceso a los Ficheros en NORD SUD LOGISTICS S.L , muchos de los cuales pueden tener acceso al tratamiento de datos de carácter personal.

8.2 OBLIGACIONES DEL PERSONAL

8.2.1 OBLIGACIONES DEL RESPONSABLE DEL FICHERO

1. Implantar las medidas establecidas en el presente Documento de Seguridad, así como obligar a su cumplimiento.

2. Designar al Responsable de Seguridad.

3. Designar a la persona competente para decidir el nivel de acceso al sistema de tratamiento de cada usuario que en NORD SUD LOGISTICS S.L coincide con la persona del Responsable del Fichero y del Responsable de Seguridad.

4. En relación con el entorno del sistema operativo y de comunicaciones deberá aprobar o designar al Administrador del Sistema, que en este caso es la Responsable del Departamento Laboral y la empresa de mantenimiento informático.

5. En relación con el sistema informático o aplicaciones de acceso a los Ficheros, se encargará de que exista una relación actualizada de personas que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso (mediante contraseñas).

6. Autorizar, en caso de que sea necesario, el tratamiento de los datos personales en lugar distinto de donde están ubicados los Ficheros.

7. El tratamiento de datos personales fuera de NORD SUD LOGISTICS S.L , deberá ser autorizada por el Responsable del Fichero. (Debe habilitarse un listado en el que se especifique los equipos móviles, PDA´s, portátiles...que salen de NORD SUD LOGISTICS S.L , y la persona a la que se le ha asignado cada uno de ellos).

8. Deberá conservar una copia de respaldo y de los procedimientos de recuperación de datos, en un lugar con acceso restringido al personal autorizado.

8.2.2 OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD

1. Coordinar la puesta en marcha de las medidas de seguridad establecidas en el Documento de seguridad de NORD SUD LOGISTICS S.L .

2. Entregar una copia total o parcial del Documento de Seguridad al personal que tenga acceso a los Ficheros.

3. Adoptar las medidas necesarias para que el personal conozca las normas de seguridad, así como las consecuencias de su incumplimiento.

4. Velar por el cumplimiento de las medidas de seguridad, en colaboración con el Responsable del Fichero, mediante controles periódicos.

5. Mantener el Documento de Seguridad actualizado en relación a cambios relevantes que se puedan producir y adecuarlo a las disposiciones vigentes en materia de protección de datos de carácter personal.

6. Encargarse de la autorización, alteración y anulación de los accesos permitidos, estableciendo los mecanismos necesarios para evitar que un usuario pueda acceder a los datos o recursos con derechos distintos de los autorizados.

7. Mantener actualizado un inventario de soportes informáticos que contengan datos de carácter personal.

8. Habilitar un registro de incidencias cuya existencia sea conocida por los empleados de NORD SUD LOGISTICS S.L .

9. Analizar las incidencias registradas y tomar las medidas oportunas en colaboración con el Responsable del Fichero.

10. Autorizar la salida de soportes informáticos que contengan datos de los ficheros objeto de protección fuera de los locales en los que se encuentren ubicados dichos ficheros.

11. En relación con el procedimiento de respaldo y recuperación deberá encargarse de verificar la definición y correcta aplicación de las copias de respaldo y recuperación de datos. Los procedimientos de back-up deberán garantizar la reconstrucción de los datos en el estado en el que se encontraban al tiempo de producirse la pérdida o destrucción.

En el Fichero de Empleados, si hay recuperación de datos y dado el nivel alto de los mismos se debe indicar la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. También será necesaria la autorización por escrito del Responsable del Fichero para la ejecución de los procedimientos de recuperación de datos.

12. Realizar copias de seguridad semanalmente almacenándolas en un lugar con acceso restringido al personal autorizado.

13. Asignar y custodiar las contraseñas del personal con acceso a los datos y establecer los mecanismos técnicos tendentes a garantizar la confidencialidad de las mismas. Dichas contraseñas deben impedir el acceso no autorizado al sistema informático, aplicaciones y ficheros no autorizados.

14. Gestionar y controlar un registro de entrada y salida de soportes informáticos.

15. Verificar la Auditoría bienal y elevar las conclusiones al Responsable del Fichero.

16. Conservar durante al menos 2 años el registro de acceso a los datos de nivel alto (en este caso los accesos al Fichero Empleados)

17. Conservar un log con la identificación del usuario, fecha y hora en que se realizó el acceso, el fichero accedido, tipo de acceso y si el acceso ha sido autorizado o denegado.

18. Si se distribuyesen soportes que contengan datos de carácter personal especialmente protegidos, el Responsable de Seguridad, se debe encargar de que se cifren esos datos, o bien que se utilice otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.

19. Si se transmiten datos de carácter personal especialmente protegidos de Nivel Alto, a través de redes de telecomunicaciones, se deberá encargar de que se cifren dichos datos, o bien utilizar cualquier otro mecanismo que garantice que la información no es inteligible ni manipulada por terceros.

20. Hacer que se cumplan las siguientes medidas en cuanto a los soportes informáticos que contengan datos relativos a los ficheros protegidos:

- Identificar los soportes mediante etiquetas externas que indiquen de qué fichero se trata, el tipo de datos que contienen, el proceso que los ha originado y la fecha de creación.
- Almacenar los soportes que contengan datos de carácter personal en lugares a los que no tengan acceso personas no autorizadas.

8.2.3 OBLIGACIONES DE LOS USUARIOS

1. Garantizar que la información no pueda ser visible por personas no autorizadas.

2. Las pantallas, impresoras y cualquier tipo de dispositivos conectados al puesto de trabajo, deberán estar ubicados en lugares que garanticen la confidencialidad.

3. Impedir la visualización de los datos a terceros, protegiendo a través de protectores de pantalla y / u otros mecanismos la visualización de datos personales por terceros.

4. El usuario deberá comprobar que no hay documentos que contengan datos protegidos en la bandeja de salida de la impresora. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

5. La conexión a redes o sistemas desde los que se realiza el acceso a datos de carácter personal estará sujeta a las medidas establecidas en el Documento de Seguridad.

6. En el caso de que se produjese cualquier incidencia relacionada con la entrada y salida de datos por red, deberá notificarse al Responsable de Seguridad y cumplimentar el correspondiente registro de incidencias.

7. Responsabilizarse de la confidencialidad de la contraseña de acceso al sistema y, en el supuesto de que dicha contraseña sea conocida fortuita o fraudulentamente por personal no autorizado, proceder al cambio de la misma, así como a notificárselo al Responsable de Seguridad, que lo hará constar en el Registro de incidencias.

8.2.4 OBLIGACIONES GENERALES (PARA TODO EL PERSONAL)

Con carácter general todo el personal empleado de NORD SUD LOGISTICS S.L deberá cumplir con las siguientes obligaciones:

1. Cumplir con todo lo dispuesto por el Responsable de Seguridad.

2. Actuar según las especificaciones, medidas y procedimientos conforme determina el Documento de Seguridad de NORD SUD LOGISTICS S.L .

3. Usar los datos de carácter personal única y exclusivamente para la finalidad para la que fueron recabados y que necesiten para el desarrollo de sus funciones.

4. Guardar secreto sobre los datos que manejen, con un rango de secreto profesional, incluso después de finalizar su relación con NORD SUD LOGISTICS S.L .

5. Informar a los titulares de los datos de la existencia de un tratamiento de datos de carácter personal y de su finalidad, así como de la posibilidad de ejercer los derechos de acceso, rectificación y cancelación, ante petición de información.

6. Facilitar los destinatarios de la información, la identidad y dirección del Responsable del Fichero y, en su caso, su representante legal, cuando así lo soliciten.

7. En caso de que un afectado ejerza sus derechos de acceso, rectificación o cancelación, tramitar el asunto conforme a lo dispuesto en la legislación vigente.

8. Recabar los datos de carácter personal que sean adecuados, pertinentes y no excesivos en relación a la finalidad para la que se recogen, no extralimitándose en las instrucciones de recogida de datos que imponga el Responsable del Fichero. En ningún caso podrán ser tratados con finalidades incompatibles a las que motivaron su recogida.

9. Mantener la exactitud de los datos actualizándolos verazmente a la situación real, rectificando los datos incompletos o inexactos, sustituyéndolos por los correctos, en todas las aplicaciones.

10. Cancelar los datos una vez que dejen de ser pertinentes y necesarios para la finalidad para la que fueron recabados.

11. A garantizar la seguridad de los datos tanto en lo referente a su custodia y tratamiento, como en lo referente a permitir el acceso por el usuario afectado. La obligación se entiende en evitar la pérdida, tratamiento o acceso no autorizado a los datos de carácter personal.

12. A no utilizar los datos con fines fraudulentos, desleales o ilícitos.

NORMAS DE USO DEL MATERIAL INFORMÁTICO Y ACCESO A INTERNET

Todos los usuarios dados de alta en el sistema deberán atender a las siguientes normas de utilización:

Los usuarios serán plenamente responsables del uso adecuado de los terminales, así como sus accesorios desde el momento de su asignación.

Todo el material informático deberá ser utilizado conforme a las instrucciones dadas por el Responsable de Seguridad.

Todo el material asignado deberá se utilizado sólo y exclusivamente para la realización de las tareas empresariales designadas, no pudiendo por tanto utilizarse para cuestiones personales.

Los usuarios sólo podrán acceder a los recursos que el Responsable de Seguridad les haya comunicado, en ningún caso intentarán acceder a recursos sin los privilegios necesarios. El Responsable de Seguridad, en todo momento podrá visualizar el intento de acceso a los mismos.

Queda totalmente prohibida la utilización de dispositivos USB o soportes informáticos, salvo autorización del Responsable de Seguridad.

Se mantendrá bajo estricta confidencialidad las claves de acceso a los recursos, quedando totalmente prohibido escribir las mismas, así como pegarlas en las pantallas de los terminales o comunicársela a terceros. En caso de olvido de contraseñas deberán comunicárselo al Responsable de Seguridad.

El acceso a Internet está sólo autorizado para cuestiones laborales, quedando totalmente prohibida la navegación por ocio, así como la descarga de información, ficheros o programas de Internet.

La utilización de correo electrónico está sólo autorizada para cuestiones laborales.

Facebook, Whatsapp, Twitter así como cualquier otra red social o aplicación de mensajería instantánea está totalmente prohibida, salvo autorización expresa del Responsable de Seguridad, y siempre por

motivos justificados de trabajo, en el caso de tener autorización, no podrán descargarse, en ningún caso, ficheros por este medio.

Los usuarios y empleados de NORD SUD LOGISTICS S.L han sido informados del contenido del presente Manual y como acreditación de la recepción y compromiso de cumplimiento del mismo han firmado el correspondiente recibí por duplicado, estando una de las copias archivada por el Responsable de Seguridad.

Los listados de Usuarios actualizados se adjuntarán como Anexo I de este Documento y se mantendrán constantemente actualizados.

9. NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

Se considera una incidencia cualquier evento o suceso que pueda suponer un peligro para la seguridad de datos, ficheros, sistemas y centros de tratamiento en general o para la confidencialidad, integridad o disponibilidad de los mismos.

El Registro de Incidencias, contemplado por el RLOPD, es una herramienta muy importante para la prevención de riesgos así como para realizar un seguimiento de las mismas.

Los aspectos a tener en cuenta son los siguientes:

- Cualquier profesional, sea o no usuario de los sistemas, que tenga conocimiento de una incidencia deberá informar inmediatamente al Responsable de Seguridad, mediante correo electrónico en primer lugar, y si no es posible mediante llamada telefónica o cualquier otro medio efectivo de comunicación.
- El conocimiento y la no notificación o registro de una incidencia por parte de un profesional puede ser considerado como una falta contra la seguridad de los ficheros.

9.1 CONCEPTO Y TIPOS DE INCIDENCIAS

Algunos sucesos que se pueden catalogar como incidencias son:

- Averías de servidores y otros componentes hardware.
- Indisponibilidad del software del sistema.
- Fallo o indisponibilidad de las líneas de comunicaciones.
- Acceso y uso no autorizado de servicios y sistemas.
- Necesidad de una restauración total del sistema.
- Mal funcionamiento de los procesos de restauración de ficheros y bases de datos.
- Extravío de soportes y copias de seguridad.
- Intrusiones en la red.
- Consecutivas situaciones de bloqueo de identificadores de usuario.

- Intentos reiterados de accesos a recursos no autorizados.
- Modificaciones no autorizadas de los datos.
- Intento de suplantación de usuarios específicos.
- Desprotección de recursos protegidos.
- Intentos reiterados de accesos al sistema por usuarios inexistentes.
- Distintos aspectos relacionados con la seguridad física (alarma de incendios, humedades, accesos no autorizados a zonas restringidas, etc.).

9.2 PROCEDIMIENTO A SEGUIR

Cualquier suceso que un usuario considere relevante será notificado al Responsable de Seguridad el cual tomará la decisión de considerarlo o no como una incidencia. Lo será en lammedida en que pueda afectar a la integridad y calidad de los datos personales y, por tanto, deberámponer en marcha los procedimientos de actuación correspondientes:

1. Identificación de la posible incidencia por cualquier profesional de **NORD SUD LOGISTICS S.L .**

2. Comunicación inmediata al Responsable de Seguridad por e-mail en primer lugar, si esto no es posible por teléfono o mediante cualquier medio de comunicación efectiva.

Tras la comunicación de un empleado de una posible incidencia, el Responsable de Seguridad deberá actuar conforme al siguiente procedimiento:

1. Valoración por parte del Responsable de Seguridad que realizará los análisis correspondientes junto con el resto de profesionales que considere necesario.

2. En el caso de que el Responsable de Seguridad lo valore como una incidencia que pueda afectar a los sistemas de **NORD SUD LOGISTICS S.L** y, por tanto, a los ficheros de datos personales, deberá proceder a completar el **Registro de Incidencias**. En dicho registro, que tiene como finalidad el seguimiento de la incidencia y las medidas adoptadas para su resolución, se detallarán todos los aspectos necesarios.

3. El Responsable de Seguridad, deberá de informar al Responsable del Fichero en el caso de que tener que adoptar medidas o procedimientos que impliquen recuperaciones de datos en los ficheros de nivel medio o alto o que supongan la toma de decisión respecto a posibles nuevas medidas de seguridad a implantar en los sistemas de **NORD SUD LOGISTICS S.L .**

4. **Mensualmente** el Responsable de Seguridad de cada centro de trabajo elaborará un informe con las incidencias ocurridas durante ese periodo y lo elevará al Responsable del Fichero, con el fin de que se tomen las mediditas necesarias para evitar la reiteración de incidencias del mismo tipo.

La gestión de incidencias se encuentran reflejadas en el **DOCUMENTO NÚMERO 4 “ANEXOS”.**

10. MEDIDAS Y NORMAS DE SEGURIDAD DE QUE SE DISPONE

10.1 PROCEDIMIENTOS Y NORMAS TÉCNICAS DE ACCESO

El presente Documento de Seguridad regula el uso y acceso a los sistemas y comunicaciones de forma que se impida el acceso no autorizado a los datos de los Ficheros.

Los sistemas y comunicaciones que tratan los datos tienen varios Administradores de Sistema, que coinciden con el Responsable del Departamento Laboral y la empresa encargada del mantenimiento informático.

Ninguna herramienta o programa de utilidad que permita el acceso al Fichero, deberá ser accesible a ningún usuario o administrador no autorizado.

Si la aplicación o sistema de acceso al Fichero utiliza normalmente ficheros temporales, o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, los Administradores deben verificar que los datos no son accesibles posteriormente por personal no autorizado.

Si el ordenador en el que están ubicados los ficheros está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso a los ficheros, los Administradores deberán asegurarse de que este acceso no se permite a personas no autorizadas.

10.2 CONTROL DE ACCESO LÓGICO

10.2.1 Identificación y Autenticación de Usuarios

El Responsable del Fichero, es el responsable de la relación actualizada de usuarios con acceso a los ficheros protegidos, y de establecer los procedimientos de identificación y autenticación para dicho acceso mediante código de usuario y contraseña. Ambos son las llaves de acceso a los sistemas y constituyen un componente básico de la seguridad de los datos y deben de estar especialmente protegidos:

- La identificación de usuario (UserId) es personal e intransferible y es asignado una sola vez. La nomenclatura del usuario está definida con la primera letra del nombre seguida por el apellido.
- Las contraseñas son estrictamente confidenciales y secretas, y cualquier incidencia que comprometa su confidencialidad debe ser inmediatamente comunicada al Responsable de Seguridad y subsanada en el menor tiempo posible.
- Cada usuario es responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida, fortuita o fraudulentamente por personas no autorizadas, debe registrarse como una incidencia y procederse por parte del Usuario a su cambio inmediato.
- Las contraseñas no son almacenadas, se asigna una única contraseña de acceso al sistema, y es el usuario el encargado de cambiarla en el primer acceso. En caso de ser necesario el administrador del sistema invalida dicha contraseña.
- El procedimiento de asignación, distribución, almacenamiento y gestión de las contraseñas debe seguirse en todos los casos.

10.2.2 Gestión de Contraseñas

Las contraseñas de acceso al sistema son un pilar fundamental de la Protección de Datos pues otorgan y garantizan confidencialidad en la información.

- Longitud de la contraseña: Más de 8 caracteres
- Complejidad de la contraseña: alfanumérica
- Vigencia de la contraseña: 12 meses
- Bloqueo de los sistemas tras intentos fallidos de acceso: 3 intentos

BLOQUEO DE USUARIOS Y CONTRASEÑAS:

Tras un tercer intento fallido de acceso, el sistema bloqueará automáticamente el usuario. El procedimiento para que el usuario afectado pueda ser rehabilitado es el siguiente:

- El usuario afectado deberá dirigirse mediante llamada telefónica o bien personalmente, al Responsable de Seguridad para que, una vez verificada la situación y comprobado que el usuario no está intentando acceder de manera fraudulenta, se lo comunique al administrador del Sistema para que reactive al usuario asignándole una nueva contraseña que obligará a cambiarla al primer acceso.

10.2.3 Asignación, Distribución y Almacenamiento de Usuarios y Contraseñas

PROCEDIMIENTO DE ALTA DE USUARIOS

- La Dirección comunica al Administrador del Sistema correspondiente el alta de un profesional en NORD SUD LOGISTICS S.L , indicando el puesto de trabajo y los privilegios necesarios para el desempeño de sus funciones.
- El Administrador del Sistema procederá a dar de alta en el mismo al nuevo usuario, procediendo el Responsable de Seguridad a actualizar los registros necesarios incluyéndolo en el Documento de Seguridad.
- El Responsable del Fichero comunica al nuevo profesional los siguientes aspectos:

- Nombre de usuario.
- Contraseña asignada.
- Aplicaciones a las que tiene acceso.

- El sistema obliga al nuevo usuario a cambiar la contraseña la primera vez que accede.

PROCEDIMIENTO DE BAJA DE USUARIOS

- La Dirección, tan pronto como tenga noticia de la baja de un profesional en NORD SUD LOGISTICS S.L , lo comunicará de manera inmediata al Administrador del Sistema correspondiente.

- En el plazo de un mes el Administrador del Sistema correspondiente, procederá al bloqueo del usuario y contraseña del profesional que causó baja.

PROCEDIMIENTO DE MODIFICACIÓN DE USUARIOS

- La Dirección comunicará al Administrador del Sistema correspondiente la necesidad de un cambio en el perfil del profesional indicando el nuevo puesto asignado y los nuevos privilegios asignar.
- El Administrador del Sistema correspondiente previa autorización del Responsable del Fichero, procederá a realizar las modificaciones pertinentes, debiendo tener especial atención a dar de baja al profesional en los recursos a los que ya no deba acceder.
- El Administrador del Sistema comunica al nuevo profesional los siguientes aspectos, en el caso de que sea necesario:

- Nombre de usuario.
- Contraseña asignada
- Aplicaciones a las que tiene acceso.

10.2.4 Directivas de Auditoría

- Auditoría de inicio de sesión de cuenta: Se puede auditar cuando un usuario inicia sesión y si en ese inicio ha habido incidencias tales como introducir mal las contraseñas o intento de inicio de sesión con otra cuenta, etc. Todos estos sucesos, se graban en el registro de seguridad del sistema.
- Auditoría del seguimiento de procesos: Controlar la actividad de un usuario en el sistema, verificando los pasos que sigue, los accesos, rutinas y pautas de comportamiento.

10.3 GESTIÓN DE SOPORTES

Los soportes informáticos son todos aquellos objetos físicos susceptibles de ser tratados en un sistema de información, medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona los ficheros.

Los soportes mayormente utilizados son fácilmente transportables, por lo que es evidente la peligrosidad para la seguridad de los datos, y por lo tanto, la importancia de gestionar un control sobre estos medios.

Dado que la mayor parte de los soportes que actualmente se utilizan (discos duros externos, pendrive's, etc) son fácilmente transportables, reproducibles y/o copiables, es necesario adoptar las medidas de seguridad necesarias para evitar los riesgos contra la confidencialidad, integridad o disponibilidad de los datos.

10.3.1 Procedimiento de uso de los soportes

En relación con los soportes deben seguirse las siguientes normas:

- Identificación inequívoca mediante etiqueta externa que permita a NORD SUD LOGISTICS S.L conocer los siguientes aspectos:

- Fecha de creación.
- Información que contienen.

- Deben guardarse en un lugar protegido, con acceso restringido a personas no autorizadas. Dicho almacenamiento se realiza en cajones bajo llave, bajo el control del Responsable del Fichero.
- La salida de estos soportes, fuera de los locales donde están ubicados dichos ficheros protegidos, deberá ser expresamente autorizada por el Responsable de Fichero, y el Responsable de Seguridad lo hará constar en el registro de salida de soportes establecido al efecto.
- Cuando los soportes con información de carácter personal tengan que salir fuera del lugar de ubicación del fichero para operaciones de mantenimiento o reparación, se establecerán una medidas de seguridad tendentes a evitar la recuperación de información por terceros no autorizados, por lo que, en el caso de que sea posible se deberá extraer el disco duro del terminal o bien realizar una copia de la información contenida en el mismo y proceder a su formateo a bajo nivel. Cuando esto no sea posible se establecerá un contrato de acceso a datos durante el período de dicho mantenimiento, haciendo a NORD SUD LOGISTICS S.L responsable del uso malintencionado o indebido de los datos en él contenidos.
- Los soportes reutilizables deberán ser formateados o sobrescritos con anterioridad a su reutilización libres de información anterior y de forma que los datos que contenían, no se puedan recuperar.
- Cuando los soportes con información de datos de nivel alto salgan fuera del centro de tratamiento deben estar protegidos mediante contraseña de forma que sea ilegibles para impedir cualquier tercero tenga acceso a la información almacenada en ellos.
- Para la destrucción de los soportes se seguirán las siguientes pautas:

- Destrucción física de los mismos, para ello, se dará de baja previamente en el inventario y se darán al Responsable de Seguridad correspondiente que procederá a su destrucción física.
- En el caso de ficheros no automatizados en soporte papel es necesario el uso generalizado de destructoras de papel.

10.3.2 Inventario de soportes

La relación de los soportes con datos de carácter personal, existentes en NORD SUD LOGISTICS S.L , se lleva a cabo por los Responsables de Seguridad a través del Registro establecido debidamente, así como la información que contienen.

10.3.3 Control de terminales portátiles

Todos los terminales portátiles estarán controlados por el Responsable de Seguridad, que será quien decida sobre la asignación o no de un terminal a un usuario de forma esporádica, así como la información que deberá contenida en el mismo.

El Responsable del Fichero en su caso, determinará la asignación de terminales portátiles permanentes a los usuarios designados.

Para controlar dichos terminales, el Responsable de Seguridad de cada centro de trabajo, llevará un registro de asignaciones, incluyendo el usuario designado, la identificación del terminal, la información que contiene y la fecha de entrega y devolución.

Durante el tiempo que el usuario tenga designado el terminal será responsable del buen mantenimiento y manejo del mismo, respondiendo de los deterioros que pudiera llegar a sufrir por negligencia del mismo.

En el caso de pérdida o robo de un terminal mientras el usuario lo tenga asignado deberá comunicárselo inmediatamente a su Responsable de Seguridad para que tome las debidas medidas necesarias.

10.3.4 Distribución de soportes

Se considera distribución de soportes, el traslado físico de soportes fuera del lugar de ubicación del fichero independientemente del soporte que contenga la información, debiendo ser cifrados o bien utilizar cualquier otro mecanismo que evite su manipulación durante su traslado.

Cuando dichos traslados afecten a ficheros de Nivel Alto, dicha documentación se entregará en sobre cerrado con cierre “open-trac”, procediendo el usuario a la estampación de dos sellos de NORD SUD LOGISTICS S.L en los bordes del cierre del sobre de forma que el destinatario de la información conozca si el contenido ha sido manipulado o no, cuando se trate de datos en soporte papel, y encriptados mediante contraseña cuando se trate de datos contenidos en soportes informáticos.

10.4 SEGURIDAD FÍSICA

El centro de trabajo donde se ubican los ficheros con datos de carácter personal y donde se encuentran los sistemas de información, corresponde a NORD SUD LOGISTICS S.L .. La entidad dispone de puertas de acceso a las instalaciones, equipadas con sistemas de seguridad y portero físico que limitan el acceso a las mismas únicamente al personal así autorizado para ello. De igual manera, cuentan con archivadores y armarios que quedan cerrados mediante llave, alarma para evitar accesos no autorizados y extintores contra incendios como medidas de seguridad física.

Archivo de papel con datos de los empleados con acceso restringido. La información en papel que es necesario mantener por obligaciones legales, se almacena durante el periodo legal establecido, en armarios cerrados con llave.

10.5 FICHEROS TEMPORALES

Los ficheros temporales, utilizados en general para obtener ficheros finales tras distintos tratamientos de los mismos, contienen datos personales que deben ser objeto de las mismas medidas de seguridad que los datos finales.

NORMAS DE USO DE LOS FICHERO TEMPORALES

- Los usuarios sólo podrán crear ficheros temporales previa autorización del Responsable de Seguridad y siempre por motivos justificados de trabajo, siempre se almacenarán en las carpetas departamentales compartidas.
- El Responsable de Seguridad realizará comprobaciones periódicas de los ficheros temporales creados por los usuarios, procediendo al borrado de todos aquellos ficheros que no estén previamente justificados o que hayan dejado de ser necesarios para la finalidad para el que se creó.
- Dichos ficheros temporales deberán ser dados de alta en un registro establecido al efecto por el Responsable de Seguridad.

10.6 COPIAS DE SEGURIDAD Y RESTAURACIÓN

Las copias de seguridad son realizadas por NORD SUD LOGISTICS S.L en el servidor con frecuencia diaria, por el personal designado al efecto, mediante un procedimiento establecido debidamente, y se realizan anexando volúmenes. Todas las copias de seguridad se almacenan en un lugar seguro, en instalaciones propias.

En caso de ser necesario recuperar datos, el Responsable del Seguridad lo registrará como una incidencia comunicándose al Responsable del Fichero, quien autorizará o no dicha recuperación.

En caso de ser autorizada el Responsable de Seguridad se lo comunicará a la empresa de mantenimiento contratada que realizará la recuperación de datos partiendo de las cintas de seguridad a través de acceso remoto.

10.7 TRANSMISIONES TELEMÁTICAS

Toda transmisión de datos por redes de telecomunicaciones se realizará cifrando dichos datos o estableciendo un mecanismo que evite su manipulación por terceros no autorizados mediante la transmisión y llegada a su destinatario, mediante contraseña, según el siguiente procedimiento.

10.7.1 Protocolo de actuación para el cifrado de Ficheros

10.7.2 Forma de proceder

El usuario cuando envíe un archivo que deba ir cifrado, enviará a su destinatario la contraseña en un archivo diferente, a aquél que se quiere distribuir. Podrá efectuarse dicha comunicación pormcualquier medio, bien, por teléfono, carta ordinaria o a través de correo electrónico, pero siempremla contraseña irá en un mensaje diferente a mail donde se inserte del fichero.

Toda otra comunicación por parte de NORD SUD LOGISTICS S.L por redes de telecomunicaciones a terceros que afecten a datos personales, se realizará cifrando su contenido mediante contraseña.

10.7.3 Procedimiento de Cifrado

Todos los ficheros, con independencia de su formato deben enviarse convenientemente cifrados.

FICHEROS EXCEL:

Cuando se deba cifrar un fichero de tipo .xml será suficiente proteger el fichero poniéndole una contraseña tal como se indica.

1. A la hora de guardar el fichero utilizar la opción: Guardar como
2. Con el botón: Herramientas à Seleccionar Opciones generales
3. Introducir la contraseña de protección y la de escritura
4. Volver a escribir la contraseña (contraseña de apertura) y Aceptar
5. Volver a escribir la contraseña de escritura (2ª contraseña) y Aceptar
6. Guardar el documento y enviar

FICHEROS EN OTROS FORMATOS:

1. Encriptar el fichero con WINZIP y Abrir el fichero
2. Pulsando Encrypt (candado), aparece una pantalla. Pinchar en OK
3. Introducir la contraseña y confirmarla, señalar la opción de 256-Bit AES encryption
4. (stronger). Pinchar en OK
5. Enviar el fichero ZIP que se ha generado.

FICHEROS EN PDF:

Si se utiliza el programa ACROBAT WRITER se puede utilizar las herramientas que el propio programa tiene para el cifrado de los ficheros.

1. Una vez abierto el documento, ir a Archivo y entrar en Propiedades del Documento (Ctrl+D)
2. Marcar Seguridad, y en sistema de seguridad elegir Seguridad mediante contraseña
3. Marcar solicitar contraseña para abrir el documento e introducir la contraseña. En los permisos, marcar usar contraseña para restringir la impresión y la edición del documento y su configuración de seguridad. Escribir la contraseña (ha de ser diferente a la anterior). Se puede limitar la impresión y se puede permitir o no los cambios. Aceptar
4. Aceptar
5. Introducir de nuevo la contraseña de permisos (la segunda contraseña). Aceptar
6. Aceptar
7. Guardar y cerrar el documento y enviar.

11. CONTROLES DE VERIFICACIÓN DE CUMPLIMIENTO

11.1 DOCUMENTO DE SEGURIDAD

La veracidad de los datos contenidos en el Documento de Seguridad y sus Anexos, así como el cumplimiento de las normas que contiene, deben ser comprobados, de forma que puedan detectarse y subsanarse las posibles anomalías.

Es muy importante que se realicen tanto revisiones puntuales como periódicas de forma que se verifique que los procedimientos, controles y medidas implantados están operativos y que el entorno se adapta tanto a la realidad del tratamiento de los datos como a las normas e instrucciones legales vigentes.

El Responsable de Seguridad semestralmente verificará al menos los siguientes aspectos:

- Que los usuarios autorizados se corresponden con la lista de los usuarios realmente autorizados.
- El cumplimiento de lo previsto en relación con las entradas y salidas de datos, sean por red o en soporte magnético.
- La existencia de las copias de respaldo que permitan la recuperación de los ficheros.
- Junto con el Responsable del Fichero analizará las incidencias registradas para, independientemente de las medidas concretas adoptadas en su momento, adoptar las acciones necesarias que las limiten en el futuro.
- Revisará los cambios que se haya realizado en el entorno (hardware, software, aplicaciones, etc.) procediendo a la actualización del Documento de Seguridad y de los Registros correspondientes.
- Otros aspectos que el Responsable de Seguridad pueda considerar.

El Responsable de Seguridad mensualmente, verificará la información de control registrada de Incidencias y elaborará un Informe de Revisión el cual recogerá los incidentes detectados proponiendo, en su caso, las medidas a adoptar.

Adicionalmente, al menos cada dos años se realizará una auditoría, externa o interna, que dictamine el correcto cumplimiento y la adecuación de las medidas del presente Documento de Seguridad y Anexos a las exigencias del Reglamento de Desarrollo de la LOPD, identificando las deficiencias y proponiendo las medidas correctoras necesarias.

11.2 REVISIÓN MENSUAL LOG DE ACCESO A FICHEROS DE NIVEL ALTO

El Responsable de Seguridad deberá revisar una vez al mes los log de acceso a las aplicaciones que tratan datos de nivel alto, y elaborar un Informe en el que se relacionen las incidencias detectadas.

11.3 AUDITORÍA BIENAL

Los sistemas de información y centros de tratamiento de datos se someterán a una auditoría interna o externa, cada dos años que verifique el cumplimiento del RLOPD y de los procedimientos e instrucciones vigentes en materia de protección de datos.

- El Informe de Auditoría resultante deberá cubrir los siguientes aspectos:
- Dictaminar sobre la adecuación de las medidas y controles establecidos.
- Identificar las deficiencias en el entorno y proponer las medidas correctoras o complementarias necesarias.
- Incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

El Responsable de Seguridad analizará el Informe de Auditoría y transmitirá las conclusiones al Responsable del Fichero para que adopte las medidas correctoras adecuadas.

Las debilidades reflejadas en el Informe de Auditoría serán subsanadas de forma inmediata y las recomendaciones que incluya dicho Informe implantadas a la mayor brevedad posible.

El Informe de Auditoría debe estar siempre a disposición de la Agencia Española de Protección de Datos, la cual, en caso de inspección, verificará que el contenido del mismo se ha llevado a efecto.

Los datos de las auditorías bienales realizadas deben ser registrados.

3 ANEXOS

ANEXO 1. REVISIONES DEL DOCUMENTO DE SEGURIDAD

VERSIÓN D.S.	FECHA MODIFICACIÓN	MOTIVO MODIFICACIÓN
1.0	**02 de Noviembre de 2016**	Creación

ANEXO 2. REGISTRO DE ACCESO A LOS FICHEROS

Nombre y apellidos	DNI	Fichero Accedido	Fecha Acceso	Hora Acceso	Autorización	Motivo autorización	Tratamiento (Automatizado/ Papel)

ANEXO 3. GESTIÓN DE INCIDENCIAS

Procedimiento de actuación ante una incidencia:

I. LA ENTIDAD dispone de un Registro que permite controlar y analizar todas las incidencias que hayan tenido lugar en la organización, y que pudieran afectar a la seguridad de los datos de carácter personal.

II. Las incidencias se deberán notificar a través de _____ al Responsable del Departamento, y éste a su vez informará al Administrador del Sistema y/o al Responsable de Seguridad.

III. El usuario que detecte una incidencia procederá a hacerla constar en el Registro de Incidencias o en su caso a comunicarla a la persona designada para tal fin, para que, en cualquier caso, quede constancia de la comunicación aportando los datos necesarios para el correcto registro de dicha incidencia.

IV. En la gestión de incidencias, se hará constar como mínimo, los datos del tipo de incidencia, el momento en que se produjo, la persona que realiza la notificación, a quien se le notifica y los efectos que se hubieran derivado de la misma.

V. En el caso de que la incidencia consistiera en la recuperación de datos de nivel medio y/o alto deberán consignarse, además, los procedimientos realizados para tal recuperación, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, los datos que han sido necesarios grabar manualmente en el proceso de recuperación.

VI. En el caso anteriormente descrito será necesaria, además, la autorización por escrito del Responsable de Seguridad para la ejecución de los procedimientos de recuperación de datos.

VII. Una vez comunicada y registrada la incidencia, el responsable designado para tal fin, procederá al análisis de la incidencia y a sus consecuencias para luego iniciar el proceso de resolución y proponer, por último, la solución a la misma.

Notificación y registro de incidencias

Nº DE INCIDENCIA	
FECHA Y HORA DE LA INCIDENCIA	
DESCRIPCIÓN DE LA INCIDENCIA:	
EFECTOS PRODUCIDOS PO LA INCIDENCIA:	
PERSONA QUE NOTIFICA LA INCIDENCIA	
MEDIDAS CONRRECTORAS ADPTADAS:	
FECHA DE NOTIFICACIÓN Y FIRMA DE LA PERSONA QUE NOTIFICA LA INCIDENCIA	
FIRMA DEL RESPONSABLE DE SEGURIDAD	

Catálogo de posibles incidencias

Si bien no es posible tipificar a priori un catalogo exhaustivo de incidencias que pueden afectar a la seguridad e integridad de los datos personales, se adjunta a modo de ejemplo, un listado orientativo de incidencias conocidas.

1. **Incidencias que pueden afectar a la confidencialidad**

1.1 Lectura no autorizada de la información contenida en los ficheros.

1.1.1 Por parte de personal informático.

1.1.2 Por parte de otras personas de la organización.

1.1.3 Por parte de personas ajenas a la organización.

1.2 Copia no autorizada de la información.

1.2.1 Por parte de personal informático.

1.2.2 Por parte de otras personas de la organización.

1.2.3 Por parte de personas ajenas a la organización.

1.3 Error en la distribución:

1.3.1 de informes

1.3.2 de soportes

1.4 Error en la manipulación:

1.4.1 de informes

1.4.2 de soportes

1.5 Obtención de información desde soportes desechados.

1.6 Descifrado de la información:

1.6.1 Por descubrimiento de claves.

1.6.2 Por conocimiento directo de las claves.

2. **Incidencias que afectan a la integridad:**

2.1 Modificación no autorizada de la información:

2.1.1 Por parte de personal de la organización.

2.1.2 Por parte de personas ajenas a la organización.

2.2 Borrado no autorizado de la información:

2.2.1 Por parte de personal informático de la organización.

2.2.2 Por parte de personas de la organización.

2.2.3 Por parte de personas ajenas a la organización.

2.3 Destrucción parcial o total de la información por:

2.3.1 Fallos en equipos.

2.3.2 Fallos en instalaciones ocasionadas por:

- Incendios

- Inundaciones

- Tormentas

2.4 Imposibilidad de recuperar datos, partiendo de las copias de respaldo.

2.5 Alteración o borrado de la información durante su explotación por:

2.5.1 Fallos ocasionados por aplicaciones.

2.5.2 Fallos ocasionados por sistemas operativos.

3. **Incidencias que afectan a la disponibilidad:**

3.1 Modificaciones no autorizadas de permisos de acceso lógico a los ficheros.

3.2 Imposibilidad o limitación del uso de las instalaciones:

3.2.1 Fenómenos meteorológicos.

3.2.2 Huelgas, manifestaciones.

3.2.3 Otras.

3.3 Indisponibilidad de los sistemas:

3.3.1 Por fallos informáticos.

4. **Incidencias que afectan a la autenticación:**

4.1 Suplantación del usuario autorizado por el no autorizado:

4.1.1 Cesión de la clave.

4.1.2 Por conocimiento de la clave de acceso.

4.1.3 Por violación de los controles de acceso.

4.2 Por fallos en los programas o dispositivos de control de acceso lógico.

4.3 Por fallos en su gestión:

4.3.1 Bajas de personas no comunicadas.

4.3.2 Autorizaciones de acceso improcedentes.

3.1 SALIDA DE SOPORTES.

SALIDA DE SOPORTES
CODIGO DE SALIDA: Fecha y hora de salida de soporte: Forma de envío:
SOPORTE Identificación: Contenido: Fichero de procedencia de los datos Fecha de creación:
FINALIDAD, ORIGEN Y DESTINO Finalidad: Origen: (Persona que responda al envío) Destino: Destinatario:
AUTORIZACIÓN Persona que autoriza: Cargo Observaciones: Firma:

3.2 ENTRADA DE SOPORTES

SALIDA DE SOPORTES
CODIGO DE ENTRADA: Fecha y hora de entrada de soporte: Forma de envío:
SOPORTE Identificación: Contenido: Fichero de procedencia de los datos Fecha de creación: Fecha de creación:
FINALIDAD, ORIGEN Y DESTINO Finalidad: Origen y Remitente: Destinatario: (Persona resposnable de la recepción
AUTORIZACIÓN Persona que autoriza: Cargo Observaciones: Firma:

ANEXO 4. AUTORIZACIÓN PARA TRABAJO FUERA DE LOS LOCALES

AUTORIZACIÓN DE TRABAJO FUERA DE LOS LOCALES
Fecha de emisión:
Período de validez de la autorización:
Nombre y apellidos de las personas autorizadas:
Motivo de la autorización:
Alcance de la autorización:
Nombre y apellidos de la persona que autoriza: Cargo: Firma

4 TEXTOS JURIDICOS

CLÁUSULAS DE INFORMACIÓN Y CONSENTIMIENTO

1. **CLÁUSULA INFORMATIVA PARA CLIENTES**
2. **CLÁUSULA INFORMATIVA PARA PROVEEDORES**
3. **CLÁUSULA INFORMATIVA PARA POTENCIALES CLIENTES**
4. **CLÁUSULA A INCLUIR EN LA FIRMA LOS CORREOS ELECTRÓNICOS**
5. **CLÁUSULA A FIRMAR CON TERCEROS PRESTADORES DE SERVICIOS SIN ACCESO A DATOS (Ejemplo: Servicio de limpieza)**
6. **CLÁUSULA INFORMATIVA PARA EL TRATAMIENTO DE LA IMAGEN**

1. CLÁUSULA INFORMATIVA PARA CLIENTES(1)

De conformidad con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de carácter Personal NORD SUD LOGISTICS S.L , domiciliado en Calle Bronce 33-34 CP:28890 Loeches , le informa que los datos que nos proporcione para la contratación de nuestros productos/servicios, formarán parte de un fichero debidamente inscrito ante la Agencia Española de Protección de Datos con la finalidad de gestionar la prestación del servicio y dar cumplimiento a obligaciones legales y contractuales.

(2)En el caso en que desee que NORD SUD LOGISTICS S.L le remita información comercial por cualquier medio incluidos los electrónicos, sobre nuestras ofertas de productos y servicios. Si autoriza el tratamiento de sus datos con esta última finalidad le rogamos marque esta casilla (…)

En el supuesto de que desee ejercitar los derechos que le asisten de acceso, rectificación, cancelación y oposición dirija una comunicación por escrito a NORD SUD LOGISTICS S.L a la dirección indicadaanteriormente a los referidos efectos, con la referencia “LOPD - Clientes” adjuntando copia de su Documento Nacional de Identidad o documento identificativo equivalente.

Le informamos asimismo que sus datos personales, no serán objeto de ninguna cesión ni transmisión sin su previo consentimiento y que de acuerdo al artículo 4. 2 de la Ley de Protección de Datos, los datos recabados serán utilizados única y exclusivamente para el fin con el que fueron recabados que es la gestión de las actividades de la empresa e información comercial, así como la gestión de cobro de las facturas correspondientes a los trabajos contratados.

Nombre y apellidos:

Fdo.:

(1) En el supuesto de que NORD SUD LOGISTICS S.L pueda acceder de algún modo a datos de ficheros responsabilidad del cliente para poder prestarle el servicio, se deberá además suscribir con el cliente el contrato de tratamiento por cuenta de terceros que se indica más adelante en el presente documento (actuando NORD SUD LOGISTICS S.L en calidad de Encargado del tratamiento).

(2)Únicamente será necesario cuando efectivamente se vayan a llevar a cabo acciones comerciales.

2. CLÁUSULA INFORMATIVA PARA PROVEEDORES(3)

De conformidad con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, NORD SUD LOGISTICS S.L domiciliado en Calle Bronce 33-34 CP:28890 Loeches , le informa que los datos personales que nos ha proporcionado serán incorporados a un fichero de datos de carácter personal responsabilidad de dicha entidad con la finalidad de llevar a cabo la gestión de la relación negocial y / o contractual que mantiene con la misma.

Asimismo le comunicamos, que en el supuesto de que sea un profesional autónomo y realicemos el pago de su factura mediante transferencia bancaria, comunicaremos sus datos identificativos a la entidad bancaria desde la que realicemos la transacción económica. En caso de autorizar dicha cesión, marque la siguiente casilla ( )

Para ejercitar los derechos de acceso, rectificación, oposición y cancelación reconocidos por la legislación vigente, el interesado deberá realizar una comunicación a la dirección Calle Bronce 33-34 CP:28890 Loeches , indicando como referencia “LOPD – Proveedores”, adjuntando copia de su Documento Nacional de Identidad o documento identificativo equivalente.

Nombre y apellidos:

Fdo.:

(3) En el supuesto de que el proveedor pueda acceder de algún modo a datos de ficheros responsabilidad de NORD SUD LOGISTICS S.L para poder prestar el servicio, deberán suscribir además de esta cláusula informativa, el Contrato de tratamiento por cuenta de terceros (actuando NORD SUD LOGISTICS S.L en calidad de Responsable del fichero) indicado más adelante en el presente documento.

3. CLÁUSULA INFORMATIVA PARA POTENCIALES CLIENTES

De conformidad con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de carácter Personal, NORD SUD LOGISTICS S.L domiciliado en Calle Bronce 33-34 CP:28890 Loeches , le informa que los datos que nos ha proporcionado formarán parte de un fichero de datos de carácter personal, responsabilidad de dicha entidad, con la finalidad de remitirle información comercial y publicitaria sobre nuestros productos y servicios a través de cualquier medio, incluidos los electrónicos. Si autoriza el tratamiento de sus datos con esta última finalidad le rogamos marque esta casilla (…).

Para ejercitar sus derechos de acceso, rectificación, oposición y cancelación reconocidos por la legislación vigente, dirija una comunicación a la dirección Calle Bronce 33-34 CP:28890 Loeches, adjuntando copia de su Documento Nacional de Identidad o documento identificativo equivalente.

Nombre y apellidos:

Fdo.:

4. CLÁUSULA A INCLUIR EN LA FIRMA LOS CORREOS ELECTRÓNICOS

En cumplimiento de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal le informamos que su dirección de correo electrónico, sus datos personales y de empresa pasarán a formar parte de nuestro fichero de Gestión, registrado ante la Agencia de Protección de Datos. Los datos personales que existen en nuestro poder están protegidos por nuestra Política de Seguridad, y no serán compartidos con ningún otro organismo o empresa. Le informamos que usted puede ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Para el ejercicio de dichos derechos deberá remitirse escrito al responsable del Fichero a la siguiente dirección: Calle Bronce 33-34 CP:28890 Loeches que en un plazo de 5 días resolverá.

5. CLÁUSULA A FIRMAR CON TERCEROS PRESTADORES DE SERVICIOS SIN ACCESO A DATOS (Ejemplo: Servicio de limpieza)

De acuerdo con lo establecido en el artículo 83 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y dado que la prestación de servicios acordada entre las partes no requiere el acceso por parte de_____ a datos de carácter personal, se prohíbe expresamente que _____ acceda a datos de carácter personal incluidos en ficheros responsabilidad de NORD SUD LOGISTICS S.L o que en cualquier caso, sean objeto de tratamiento por parte de la misma.

Sin perjuicio de lo dispuesto en el párrafo anterior, _____ se obliga al cumplimiento de la obligación de secreto respecto a los datos que el personal de su entidad hubiera podido conocer con motivo de la prestación del servicio, responsabilizándose de las consecuencias que en cualquier ámbito pudieran derivarse como consecuencia de la vulneración de la referida obligación.

Nombre y apellidos:

DNI:

Fdo.:

6. CLÁUSULA INFORMATIVA PARA EL TRATAMIENTO DE LA IMAGEN

De conformidad con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, le informamos que su imagen será expuesta en la web http://www.NORD SUD LOGISTICS S.L ..es/ perteneciente a NORD SUD LOGISTICS S.L domiciliada en Calle Bronce 33-34 CP:28890 Loeches .

La persona abajo firmante autoriza expresamente a que NORD SUD LOGISTICS S.L trate su imagen en la página web http://www.NORD SUD LOGISTICS S.L ..es/ .

En el supuesto de que desee ejercitar los derechos que le asisten de acceso, rectificación, cancelación y posición al tratamiento de sus datos de carácter personal, debe dirigir una comunicación escrita a NORD SUD LOGISTICS S.L a la dirección arriba indicada, a los referidos efectos, con la referencia “LOPD - Imagen”, incluyendo copia de su Documento Nacional de Identidad o documento identificativo equivalente.

Nombre y apellidos:

DNI:

Fdo.:

5 DOCUMENTACIÓN PARA EMPLEADOS

CLÁUSULAS DE INFORMACIÓN Y PARA EMPLEADOS

1. **CLÁUSULA INFORMATIVA PARA EMPLEADOS EN RÉGIMEN LABORAL**

   1.1 FIRMAS PARA EMPLEADOS

2. **OBLIGACIONES DE LOS EMPLEADOS CON ACCESO A DATOS**

3. **OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD**

4. **OBLIGACIONES DEL RESPONSABLE DEL SISTEMA INFORMÁTICO**

5. **RESUMEN DE ALERTA SOBRE TRATAMIENTO DE DATOS**

   5.1 WARNING: DATOS PERSONALES

      5.1.1 INSTRUCCIONES PARA EL TRATAMIENTO DE DATOS PERSONALES

      5.1.2 EL EMPLEADO DEBERÁ

6. **COMPROMISO DE CONFIDENCIALIDAD Y SECRETO**

1. CLÁUSULA INFORMATIVA PARA EMPLEADOS EN RÉGIMEN LABORAL

De conformidad con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, NORD SUD LOGISTICS S.L domiciliada en Calle Bronce 33-34 CP:28890 Loeches , le informa que los datos personales que nos ha proporcionado así como aquellos otros que facilite en un futuro, incluidas posibles grabaciones de videovigilancia, formarán parte de un fichero de datos de carácter personal, responsabilidad de NORD SUD LOGISTICS S.L , con la finalidad de gestionar la relación laboral que mantiene con la misma

- Controlar la utilización que realice de los recursos de NORD SUD LOGISTICS S.L a los que pudiera tener acceso, como el uso y gasto telefónico, la utilización de Internet, los servicios de mensajería instantánea, así como el correo electrónico, que son recursos de uso exclusivo en el ámbito profesional,
- Realizar el pago de las nóminas,
- Llevar a cabo las obligaciones existentes en materia de protección de la salud y prevención de riesgos laborales,
- Gestionar y controlar su participación, asistencia y aprovechamiento en las acciones formativas organizadas por NORD SUD LOGISTICS S.L en las que en su caso participe,
- Realizar el control del absentismo así como el cumplimiento del horario laboral,
- Remitir aquellas comunicaciones que pudieran llevarse a cabo desde NORD SUD LOGISTICS S.L ..

Asimismo, NORD SUD LOGISTICS S.L le informa que sus datos serán comunicados a las siguientes entidades:

- Tesorería General de la Seguridad Social: en cumplimiento de las obligaciones legales vigentes en materia de seguridad social.
- Agencia Estatal Tributaria: con la finalidad de llevar a cabo las obligaciones fiscales y tributarias vigentes.
- Entidades gestoras de la vigilancia de la salud: para el cumplimiento de la protección respecto a contingencias de accidentes de trabajo y enfermedad profesional en los términos previstos en la legislación vigente.
- Entidades bancarias: para realizar el ingreso de los importes de las nóminas.
- Entidades aseguradoras: con la finalidad de llevar a cabo la suscripción de pólizas de seguros entre el empleado y la entidad destinataria de los datos.

Para ejercitar los derechos de acceso, rectificación, oposición y cancelación reconocidos por la legislación vigente, el interesado deberá realizar una comunicación a la dirección indicada anteriormente, a los referidos efectos, indicando como referencia “LOPD - Personal”, adjuntando copia de su Documento Nacional de Identidad.

1.1. FIRMAS EMPLEADOS EN RÉGIMEN LABORAL

NOMBRE Y APELLIDOS	DNI	CARGO	FIRMA

2. OBLIGACIONES DE LOS EMPLEADOS CON ACCESO A DATOS

- Los usuarios del sistema, deben conocer y aceptar las normas de seguridad de la organización.
- Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas. Cumplimiento de política de “mesas limpias”.
- Las pantallas, impresoras o cualquier otro tipo de dispositivos conectados al puesto de trabajo, deberán estar ubicados en lugares que garanticen confidencialidad e impidan accesos no autorizados
- El usuario, cuando abandone su puesto de trabajo, temporalmente o al finalizar su jornada de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente
- Deberán asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del fichero, cada usuario deberá retirar los documentos conforme vayan siendo impresos.
- La conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero, quedan expresamente prohibidas.
- No podrán cambiar la configuración fija y sistema operativo de los equipos, salvo autorización del Responsable de seguridad o de las personas en las que haya delegado expresamente esta autorización.
- Cada usuario será responsable de la confidencialidad de su contraseña y, en el supuesto de que ésta sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.
- Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al Administrador del sistema, o en su caso, del registro de la misma en el registro de incidencias del fichero. En este sentido, el conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del fichero por parte de dicho usuario.
- Deberán responsabilizarse de que los soportes que contengan datos personales, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, se encuentren claramente identificados con una etiqueta externa que indique de qué fichero se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación
- Se encargarán de que aquéllos soportes que resulten reutilizables, y que hayan contenido datos personales, sean borrados físicamente antes de su reutilización, de forma que los datos que contenía anteriormente, no sean recuperables.

- Se deberá borrar o destruir todo fichero temporal o copia de trabajo, una vez que haya dejado de ser necesario para los fines que motivaron su creación.
- En los supuestos de traslado de documentación que contenga datos personales, se deberán adoptar medidas encaminadas a evitar su pérdida o robo.
- Se ocuparán de que los soportes que contengan datos personales sean almacenados en lugares a los que no tengan acceso a personas no autorizadas para el acceso a dichos datos.
- Conservarán todos los datos en el servidor de red, quedando prohibida la conservación de información en local.
- Se compromete a cumplir con el deber de secreto en relación con la información que conozca para llevar a cabo sus funciones en la entidad, subsistiendo este deber una vez finalizada la relación en virtud de la que se ha tenido conocimiento de dicha información.

El incumplimiento del presente Manual conllevará las siguientes sanciones por parte de la Entidad: (1) (1) LA ENTIDAD deberá indicar las posibles sanciones dependiendo de la gravedad y/o reiteración del incumplimiento.

3. OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD

D. /Dña. Angel Ramos con DNI 50946037W responsable de seguridad de NORD SUD LOGISTICS S.L se compromete a:

- Tramitar la firma de los contratos de encargado de tratamiento con aquellas empresas que puedan acceder a los datos de NORD SUD LOGISTICS S.L . Comprobará que dichas empresas conocedoras de datos de carácter personal tengan implantadas las mismas medidas de seguridad que las que le correspondan a la empresa responsable de los ficheros y vigilar que la empresa encargada del tratamiento utilice los datos únicamente con la finalidad autorizada.
- Coordinar la puesta en marcha de las medidas de seguridad y controlar el cumplimiento de las mismas con los responsables administrativos de los ficheros en caso de que se haya optado por designar a los mismos.
- Analizar las incidencias registradas, tomando las medidas correctoras oportunas, y adoptar las medidas preventivas que limiten esas incidencias en el futuro.
- Realizar controles periódicos de verificación del cumplimiento de la normativa especificada en el Documento de Seguridad.
- Comprobar, con una periodicidad al menos trimestral, que la lista de Usuarios autorizados se corresponde con la lista de los usuarios que realmente están accediendo a la aplicación de acceso al Fichero. El Administrador del Sistema colaborará con el Responsable de Seguridad en este sentido, además de informarle de cualquier alta, baja o modificación de la lista de Usuarios.
- Comprobará, al menos semestralmente, que el Documento de Seguridad esta actualizado.
- Cuando el nivel de seguridad sea medio o alto el responsable de seguridad analizará el informe de auditoría y comunicará las conclusiones del mismo al Responsable del Fichero para que adopte las medidas correctoras adecuadas.
- Gestionará y controlará directamente los mecanismos que registran los accesos a los Ficheros con datos de carácter personal. Además, en el caso de los datos de nivel alto, analizará mensualmente la información registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
- El responsable de seguridad comprobará trimestralmente el cumplimiento de los registros de entradas y salidas de soportes informáticos que contengan datos de nivel medio/alto.

Fdo.:

4. OBLIGACIONES DEL RESPONSABLE DEL SISTEMA INFORMÁTICO

D. / Dña. _____ con DNI _____ responsable del sistema informático de la empresa NORD SUD LOGISTICS S.L se compromete a:

- Administrar o mantener el entorno operativo del Fichero, por tanto deberá realizar un mantenimiento de los equipos y del software que contienen éstos.
- Se responsabilizará de la correcta instalación del software de acceso a los datos del Fichero, tales como aplicaciones de gestión o generadores de listados, en cada uno de los equipos.
- Controlará la particular configuración del sistema informático de la organización, con especial atención a las conexiones de red local, así como a las conexiones a redes externas.
- Debe establecer un mecanismo que impida el acceso al sistema desde cualquier puesto local o remoto a personas no autorizadas. Para ello empleará medidas de seguridad implementadas en el sistema operativo, y al menos para el acceso a datos de nivel medio/alto, limitará el número máximo de intentos fallidos de conexión. Asimismo y, en caso de ser técnicamente posible, registrando estas incidencias con detalle de fecha, hora, identificador de usuario y clave erróneas, con objeto de identificar al autor de tales intentos.
- Mantendrá una relación del personal autorizado a acceder al sistema de información, ya sea local o remotamente, con la máxima garantía de seguridad.
- Si en el momento de implantar una aplicación que acceda a los datos del Fichero precisara realizar pruebas con datos reales, solicitará autorización al responsable del Fichero y garantizará que los datos usados para las pruebas reciban el mismo tratamiento de seguridad que los originales, debiendo para ello:
- Anotar dicha circunstancia en el Documento de Seguridad.
- Realizar una copia de seguridad previamente a la realización de la pruebas
- Se encargará de comunicar al Responsable del Fichero o en su caso a la persona delegada, las modificaciones significativas realizadas en el sistema informático que da acceso a los datos del Fichero.
- Se responsabilizará de guardar y proteger las copias de seguridad, de tal forma que no puedan tener acceso a las mismas las personas no autorizadas.
- Si la aplicación o sistema de acceso al fichero utilizase ficheros temporales, ficheros de “logging”, el administrador deberá asegurarse de que esos datos no son accesibles por personal no autorizado
- Si el equipo en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros equipos conectados a la misma sea posible el acceso al fichero, el administrador deberá asegurarse de que este acceso no se permite a personas no autorizadas.
- Si la aplicación informática que permite el acceso al fichero no cuenta con un control de acceso, deberá ser el sistema operativo en el que se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control a través de códigos de usuario y contraseñas. (Esta obligación solo deberá ser cumplida por empresas con un nivel de seguridad medio o alto).

- Se responsabilizará del cumplimiento de los mecanismos establecidos para la asignación, distribución y cambio de contraseñas.
- Será responsable de que las contraseñas se almacenen en archivo protegido
- Deberá realizar con una periodicidad al menos semanal, una copia de seguridad a efectos de respaldo y posible recuperación de datos en caso de fallo. Podrá ser designado expresamente otro usuario para responsabilizarse de este extremo.
- Se encargará de que en caso de fallo del sistema con pérdida parcial o total de los datos, exista y se lleve a cabo un procedimiento que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del fichero al estado en que se encontraban en el momento del fallo.
- En el posible caso de no existir en la organización la figura del Administrador del Sistema, será el Responsable de Seguridad quien asuma las obligaciones anteriormente descritas.

Fdo.:

5. RESUMEN DE ALERTA SOBRE TRATAMIENTO DE DATOS.

5.1 WARNING: DATOS PERSONALES

5.1.1 INSTRUCCIONES PARA EL TRATAMIENTO DE DATOS PERSONALES

En primer lugar, cabe indicar que con anterioridad a cualquier tratamiento de datos personales sobre el que se tengan dudas, se deberá consultar al responsable de departamento. Ej.: ¿Puedo recoger estos datos? ¿Puedo enviar publicidad propia o de terceros a mi base de datos de contactos? ¿Puedo enviar una felicitación de cumpleaños a los clientes, trabajadores, etc.? ¿Puedo llevarme datos personales en papel o en USB para trabajar en casa?, etc.

En este sentido, se indican a continuación algunas recomendaciones que se deberán tener en cuenta en el tratamiento de datos personales (Cualquier información de una persona física identificada o que pueda llegar a identificarse), de conformidad con la LOPD (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal) y su normativa de desarrollo:

- Como norma general en los correos electrónicos que se envíen a varias personas, se deberán poner las direcciones de correo en Copia Oculta (CCO), salvo que se trate de empleados de la misma entidad. Ej.: Vamos a enviar un email a varios clientes y/o proveedores. En este caso, deberemos poner en copia oculta (CCO) las direcciones de cada uno de ellos.
- Los papeles que contengan datos personales deberán eliminarse en destructoras de papel cuando dejen de ser necesarios para la finalidad para la que se recogieron, y nunca deberán tirarse a la basura sin su previa destrucción. Ej.: Imprimimos un listado de participantes en un sorteo para enviarlo al notario, una vez finalizado el sorteo deberemos destruir dicho listado en destructora de papel.
- Los papeles emitidos por impresoras, faxes o máquinas multifunción, deberán ser custodiados por el empleado que los está tratando, que deberá impedir que otros empleados que no deban tener acceso a dicha información, accedan a la misma. Ej.: Imprimo un listado de empleados para chequear la entrega de nóminas, se deberá acudir a la impresora a la espera de la información evitando que terceros puedan acceder a dicho listado.
- Los empleados deberán custodiar los datos personales que traten en el ejercicio de sus funciones, impidiendo que terceros accedan, adoptando medidas como: Política de mesas limpias, cerrar con llave los cajones, armarios y archivos, bloquear la pantalla del ordenador cuando no estén presentes, mantener en secreto las contraseñas de acceso a los datos personales,… Ej.: Antes de irme a comer, deberé apagar el ordenador o bloquear la pantalla, cerrar los cajones, archivos o sala con llave y no dejaré visible mi contraseña de acceso.
- Durante los traslados de soportes con datos personales, se deberán custodiar eficazmente dichos soportes impidiendo el acceso de terceros a la información. Ej.: Si me llevo un portátil, USB o carpeta con datos personales para una reunión fuera de la oficina, el acceso a la información deberá estar bloqueado a terceros, y en cualquier caso si por ejemplo paro en una cafetería a tomarme un café, lo vigilaré en todo momento para evitar su robo o pérdida.

- Se deberá cumplir con las medidas de seguridad de los datos personales indicadas en el **"Manual de funciones y obligaciones del personal".**

Asimismo, se deberán **consultar al responsable de departamento** las medidas a adoptar siempre que:

- Se recojan datos personales. Ej.: Formularios en papel o Internet, recepción de CV, contratos, etc.
- Se envíe publicidad/información comercial (vía mail, sms, carta,...). Ej.: Mail a clientes o potenciales clientes informando de un nuevo servicio.
- Se vayan a facilitar datos a terceros (empresas, autónomos, Administraciones Públicas,…) o se envíe publicidad de dichos terceros a nuestros clientes o potenciales clientes. Ej.: Empresa de mensajería, gestoría externa, envío de publicidad de otra empresa,…
- Se vayan a utilizar datos personales con una finalidad distinta a la inicial para la que se recogieron. Ej.: Se recogieron datos de clientes con la única finalidad de prestar el servicio contratado, y posteriormente se decide utilizar esa base de datos de clientes para enviarles información de nuevos productos o servicios.
- Se traten datos que permitan elaborar perfiles de las personas (Ej.: aficiones, CV) o que se refieran a sanciones administrativas y/o penales, salud, origen racial, vida sexual, ideología, religión, creencias o violencia de género. Ej.: Tengo datos de salud de clientes o de empleados.
- Vayan a salir o entrar soportes con datos personales (ya sean en papel o automatizados: USB, portátil, CD, carpeta con papeles, etc.). Ej.: Si me llevo un USB con datos personales a casa porque debo terminar un trabajo por la noche. El responsable de departamento deberá autorizar la salida de soportes.
- Se produzca o detecte una incidencia que pueda afectar a datos personales. Ej.: Se va la luz y perdemos datos o al imprimir un listado de datos y se bloquea la impresora. En estos casos, se deberá rellenar el registro de incidencias habilitado por NORD SUD LOGISTICS S.L para ello.
- Se reciba cualquier escrito mencionando la LOPD o que el remitente sea la AEPD(Agencia Española de Protección de Datos).
- Se tenga conocimiento de que un dato ha cambiado o se haya ejercitado un derecho de cancelación, ya que los datos se deberán mantener actualizados en todo momento, y deberán ser cancelados cuando los titulares de datos ejerciten su derecho. Ej.: Si un cliente nos indica que ha cambiado de domicilio, deberemos actualizar dicho dato en todas las bases de datos de NORD SUD LOGISTICS S.L en las que nos conste ese dato.

5.1.2 EL EMPLEADO DEBERÁ

- Enviar e- mails con las direcciones de correo en Copia Oculta (CCO)
- Eliminar los papeles en destructora
- Custodiar los papeles que se emitan o reciban por impresoras, faxes, etc.
- Cumplir con la política de “mesas limpias” (guardando el papel bajo llave)
- Custodiar los soportes de datos en los traslados
- Cumplir con el “Manual de Funciones y Obligaciones del Personal”
- Consultar al Responsable del Departamento siempre que tenga dudas, y más concretamente cuando:

  - **Se recojan nuevos datos personales**
  - **Se vaya a enviar publicidad/información comercial propia o de terceros**
  - **Se vayan a facilitar datos a terceros**
  - **Se vayan a utilizar datos personales con una finalidad distinta a la inicial**
  - **Se traten datos que permitan elaborar perfiles**
  - **Vayan a salir o entrar soportes en la oficina**
  - **Se produzca o detecte una incidencia que afecte a datos personales**
  - **Se reciba cualquier escrito relativo a la LOPD**
  - **Se tenga conocimiento de que un dato ha cambiado**

6. COMPROMISO DE CONFIDENCIALIDAD Y SECRETO

COMPROMISO DE CONFIDENCIALIDAD Y SECRETO

_____de_____de_____.

REUNIDOS

De una parte, _____., con CIF.-_____ y domicilio social en _____ (en adelante, el RESPONSABLE DEL FICHERO).

Y de otra parte, D/Dña._____, mayor de edad, actuando en su propio nombre y representación (en adelante, el USUARIO).

EXPONEN

Que ambas partes se reconocen capacidad legal necesaria para suscribir el presente Contrato.

Que debido al desempeño de las funciones que el USUARIO realiza a favor del RESPONSABLE DEL FICHERO, el USUARIO tendrá acceso a sistemas y soportes en los que se contiene información relativa a datos de carácter personal.

Que de conformidad con el artículo 10 de la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de carácter personal, el USUARIO es consciente de su obligación al secreto profesional respecto a los datos de carácter personal que trate y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el RESPONSABLE DEL FICHERO.

Que ambos suscriben el presente COMPROMISO DE CONFIDENCIALIDAD Y SECRETO, el cual aceptan expresamente y de acuerdo a las siguientes:

CLÁUSULAS

PRIMERA. El USUARIO se compromete a cumplir con las políticas, normas y procedimientos determinados por el RESPONSABLE DEL FICHERO, así como con todas las medidas de seguridad que este establezca para garantizar la confidencialidad y secreto de toda la información que sea considerada " confidencial ".

A estos efectos, será considerada información confidencial:

Cualquier información concerniente a una persona física identificada o identificable, es decir, datos de carácter personal.

Cualquier información interna de la organización, como por ejemplo, desarrollos, ideas, invenciones, dibujos, diseños, procedimientos, fórmulas, datos, programas, descubrimientos, secretos comerciales, listas de precios, información financiera, plantillas, presupuestos, nombres de clientes y/o proveedores, estadísticas, objetivos, etc.

SEGUNDA. El USUARIO se compromete al más estricto secreto profesional respecto a toda la información confidencial a la que tenga acceso con motivo del desempeño de sus funciones, comprometiéndose a no divulgarla, publicarla, cederla, venderla, ni de otra forma, directa o indirecta, ponerla a disposición de Terceros, ni siquiera de otros sujetos que trabajen para el RESPONSABLE DEL FICHERO, que no estén autorizados a acceder a dicha información.

TERCERA. El USUARIO se obliga a acceder a la información confidencial que sea estrictamente necesaria para el desempeño de sus funciones y que previamente haya autorizado el RESPONSABLE DEL FICHERO, así como a utilizar los datos exclusivamente para los fines y funciones que fueron recabados, no utilizándolos para ninguna otra finalidad.

CUARTA. El USUARIO se compromete a comunicar todas aquellas incidencias que se produzcan en la organización y que afecten o puedan afectar a la seguridad de los datos de carácter personal objeto del tratamiento.

QUINTA. El USUARIO será responsable de cualquier daño que pudiera derivarse del incumplimiento de los compromisos anteriores, así como de resarcir las indemnizaciones, sanciones y daños o perjuicios que se pudieran ocasionar, tanto a Terceros como al RESPONSABLE DEL FICHERO, como consecuencia de dicho incumplimiento.

SEXTA. Que el cumplimiento de las obligaciones contenidas en este Compromiso subsistirá aún después de finalizar la relación laboral o profesional entre el USUARIO y el RESPONSABLE DEL FICHERO.

SÉPTIMA. El RESPONSABLE DEL FICHERO comunica al USUARIO que sus datos personales formarán parte de un fichero del que es titular, con la finalidad de gestionar la relación laboral o profesional que les une. El USUARIO declara estar informado de sus derechos de acceso, rectificación, cancelación, y oposición dirigiéndose a la siguiente dirección:_____

OCTAVA. El USUARIO se compromete al cumplimiento de las funciones y obligaciones específicas que están recogidas en las “Funciones y obligaciones del personal“, incluido en el Documento de Seguridad y que el USUARIO ha recibido.

Para que conste y en prueba de conformidad de ambas partes, firman el presente Contrato por duplicado, en el lugar y fecha indicados en el encabezado.

Fdo. Fdo.

6 EMPRESAS CON ACCESO A DATOS

LISTADO DE ENCARGADOS DEL TRATAMIENTO

1. **CONTRATO DE TRATAMIENTO DE DATOS POR CUENTA DE TERCEROS**

LISTADO DE ENCARGADOS DEL TRATAMIENTO

Encargado	Servicio que presta	Ficheros accedidos	Acceso remoto SI/NO
Oclem	Servicios LOPD y Consultoría	Nóminas y personal	**No**
Ferluval S.L	Gestoría	Nóminas y personal	**No**
Visegur S.L	Empresa de Videovigilancia	Videovigilancia	**No**

1. CONTRATO DE TRATAMIENTO DE DATOS POR CUENTA DE TERCEROS

En _____ a __ de _____ de 2016

REUNIDOS

DE UNA PARTE

NORD SUD LOGISTICS S.L (en adelante, EL RESPONSABLE), con CIF B85512788 y domicilio en: Calle Bronce 33-34 CP:28890 Loeches , representada por el abajo firmante en calidad de apoderado.

DE OTRA PARTE

_____. (en adelante, EL ENCARGADO) con CIF _____, y con domicilio en: _____ (Madrid) representada por el abajo firmante en calidad de apoderado.

MANIFIESTAN

a. Que el Responsable de los Ficheros es titular, entre otros, de los ficheros de datos de carácter personal indicados en la Estipulación Novena.

b. Que el Encargado del Tratamiento viene prestando servicios de al Responsable de los Ficheros, para cuyos fines ha necesitado acceder a los datos que se encuentran contenidos en los Ficheros estipulados en la novena cláusula de este contrato.

c. Que, ambas partes se reconocen mutuamente la capacidad legal necesaria para contratar y obligarse, y, en especial, para celebrar el presente Contrato, llevándolo a efecto conforme a las siguientes

ESTIPULACIONES

PRIMERA.- EL ENCARGADO se compromete a guardar la máxima reserva y secreto sobre la información clasificada como confidencial. Se considerará información confidencial cualquier dato al que EL ENCARGADO acceda en virtud del presente contrato y/o en el acuerdo general que regula los servicios a prestar por parte de EL ENCARGADO a EL RESPONSABLE, en especial la información y datos propios de EL RESPONSABLE a los que haya accedido o acceda durante la ejecución del mismo. No tendrán el carácter de confidencial todas aquellas informaciones y datos que fueran de dominio público o que estuvieran en posesión de EL ENCARGADO con anterioridad a iniciar la prestación de sus servicios y hubieran sido obtenidas por medios lícitos.

SEGUNDA.- La obligación de confidencialidad recogida en el presente contrato tendrá carácter indefinido, manteniéndose en vigor con posterioridad a la finalización, por cualquier causa, de la relación entre las partes.

TERCERA.- EL RESPONSABLE, es, con carácter único, quien decidirá sobre la finalidad, contenido y uso de EL FICHERO al que acceda EL ENCARGADO como resultado de las actividades realizadas por éste.

CUARTA.- EL ENCARGADO accederá a EL FICHERO únicamente, cuando sea imprescindible para el buen desarrollo de los servicios acordados entre las partes.

QUINTA.- EL ENCARGADO, se obliga a respetar todas las obligaciones que pudieran corresponderle como encargado del tratamiento con arreglo a las disposiciones de la LOPD y cualquier otra disposición o regulación complementaria que le fuera igualmente aplicable.

SEXTA.- EL ENCARGADO en su condición de encargado del tratamiento, únicamente tratará los datos conforme a las instrucciones que reciba expresamente de EL RESPONSABLE.

SÉPTIMA.- EL ENCARGADO no destinará, aplicará o utilizará los datos a los que tenga acceso con fin distinto al expresamente indicado en el presente contrato, o de cualquier otra forma que suponga un incumplimiento de las instrucciones expresas que EL RESPONSABLE, en su condición de responsable del tratamiento, le proporcione.

OCTAVA.- EL ENCARGADO se compromete a no revelar, transferir, ceder o de otra forma comunicar EL FICHERO o los datos en él contenidos, ya sea verbalmente, por escrito, por medios electrónicos, papel o mediante acceso informático, ni siquiera para su conservación, a ningún tercero. A tal efecto EL ENCARGADO sólo podrá permitir el acceso a los datos a aquellos empleados que tengan la necesidad de conocerlos para la prestación de los servicios contratados.

NOVENA.- EL ENCARGADO se obliga al cumplimiento de las obligaciones derivadas de la normativa de protección de datos y más concretamente, en lo que se refiere a la implantación de las medidas de seguridad que se indican a continuación según lo dispuesto en el RD 1720/07. Asimismo, EL ENCARGADO garantiza el mantenimiento de estas medidas de seguridad así como cualesquiera otras que le fueran impuestas, de índole técnica y organizativas, necesarias para garantizar la seguridad, presente y futura, de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural, conforme a lo establecido en la normativa sobre protección de datos de carácter personal.

Ficheros a los que accederá EL ENCARGADO en calidad de encargado del tratamiento y nivel de medidas de seguridad aplicables a cada uno de ellos:

Denominación del fichero	Nivel de seguridad aplicable
Nóminas y personal	Básico

DÉCIMA.- Una vez cumplida o resuelta la prestación contractual acordada entre EL RESPONSABLE y EL ENCARGADO, los datos de carácter personal serán devueltos a EL RESPONSABLE, al igual que cualquier soporte o documento en el que conste algún dato de carácter personal objeto del tratamiento, debiendo certificar inmediatamente por escrito dicha devolución, en el plazo máximo de 10 días hábiles desde la fecha de cumplimiento o resolución del contrato.

UNDÉCIMA.- De acuerdo con lo dispuesto en el artículo 82 del RD 1720/07, EL ENCARGADO asume las siguientes obligaciones:

- Si como consecuencia de los términos de la prestación de servicios acordada entre las partes EL RESPONSABLE facilitara el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a EL ENCARGADO cuando éste prestare sus servicios en los locales del primero, el personal de EL ENCARGADO se comprometerá al cumplimiento de las medidas de seguridad previstas por EL RESPONSABLE en su Documento de Seguridad.
- Si ambas partes hubieran pactado que EL ENCARGADO accediera a los datos de carácter personal o a los recursos del sistema de información de EL RESPONSABLE, el personal del primero se comprometerá al cumplimiento de las medidas de seguridad previstas por EL RESPONSABLE en su Documento de Seguridad. Asimismo, y en el presente supuesto, EL ENCARGADO no podrá incorporar tales datos a sistemas o soportes distintos de los del responsable.
- Si el servicio fuera prestado por EL ENCARGADO en sus propios locales, ajenos a los de EL RESPONSABLE, el primero deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 del RD 1720/07 o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

DUODÉCIMA.- Es obligación del Responsable de los Ficheros velar por que el Encargado del Tratamiento reúna las garantías necesarias para el cumplimiento de lo establecido en la legislación sobre protección de datos de carácter personal. A fin de cumplir con esta obligación, el Responsable de los Ficheros tendrá derecho a:

- Solicitar que el Encargado del Tratamiento exhiba la documentación preceptiva, conforme a lo establecido en el RD 1720/2007 y normativa complementaria.

DECIMOTERCERA.- Todos aquellos ficheros que sean creados e inscritos ante la Agencia Española de Protección de Datos por el Responsable de los Ficheros con posterioridad a la firma del presente Contrato y a los que el Encargado del Tratamiento tenga que tener acceso para la correcta prestación de los Servicios, quedarán sometidos a los términos previstos en este Contrato quedando obligado el Responsable de los Ficheros ha comunícaselo al Encargado del Tratamiento de manera expresa, por cualquier medio escrito, adjuntándose copia de dichas comunicaciones a este contrato como Anexos sucesivos.

DECIMOCUARTA.- EL RESPONSABLE autoriza expresamente a EL ENCARGADO a contratar con terceros cuya intervención estime oportuna para el buen desarrollo de los servicios, informándole de la identidad del tercero y de los servicios encargados. Además, EL ENCARGADO se obliga a suscribir con el tercero un contrato en el que se estipulen las obligaciones que este debe cumplir en relación a la protección de datos personales.

DECIMOQUINTA.- La totalidad de los términos y condiciones del presente documento, incluidos sus anexos, tienen carácter confidencial, estando sujetos a las obligaciones expuestas a lo largo del acuerdo.

Datos incluidos en el presente contrato

DECIMOSEXTA.- De conformidad con lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, EL RESPONSABLE con domicilio en el lugar indicado en el encabezamiento del presente contrato, informa a los intervinientes en el mismo, que los datos que figuran en él, serán incorporados a un fichero de datos de carácter personal responsabilidad de EL RESPONSABLE con la

finalidad de llevar a cabo la gestión de la relación contractual generada con la firma del presente documento.

Para ejercitar los derechos de acceso, rectificación, oposición y cancelación reconocidos por la legislación vigente, el interesado deberá realizar una comunicación a la dirección indicada anteriormente, a los referidos efectos, indicando como referencia “Protección de datos”.

FIRMAS:

EL RESPONSABLE

- NOMBRE Y APELLIDOS:

- DNI:

EL ENCARGADO

- NOMBRE Y APELLIDOS:

- DNI:

7 INFORME WEB

1. **LOPD y LSSI EN LA WEB**
2. **AVISO LEGAL**
3. **POLITICA DE COOKIES**

1. LOPD y LSSI EN LA WEB

Se recomienda que bajo los formularios (apartado contacto de la página web normalmente) donde se recaban los datos se inserten los siguientes textos resaltados en negrita:

□ **He leido y acepto la politica de proteccion de datos**

El enlace "política de protección de datos" debe dirigir a una ventana con el siguiente texto:

De conformidad con lo dispuesto en la Ley Organica 15/1999 de Proteccion de Datos de Caracter Personal, le informamos que los datos que nos proporcione en el presente formulario, se incorporaran a un fichero de datos de caracter personal, responsabilidad de NORD SUD LOGISTICS S.L domiciliada en la direccion Calle Bronce 33-34 CP:28890 Loeches . La finalidad de dichos ficheros es la gestion de los usuarios del Sitio Web, la gestion de los servicios ofrecidos a traves de dicho sitio y, en su caso, la gestion, desarrollo y cumplimiento de la relacion establecida entre NORD SUD LOGISTICS S.L y quienes aporten sus datos personales a traves del Sitio Web.

Si desea ejercitar los derechos ARCO (acceso, rectificacion, cancelacion y oposicion) le rogamos remita una comunicacion escrita y firmada a NORD SUD LOGISTICS S.L a la direccion Calle Bronce 33-34 CP:28890 Loeches , adjuntando copia de su Documento Nacional de Identidad o equivalente.

□ **Acepto recibir informacion comercial sobre las ofertas y promociones de NORD SUD LOGISTICS S.L ..**

Asimismo, se deberá resaltar de algún modo que el campo de aceptación de la política de protección de datos (primera casilla) es de obligada cumplimentación para que la empresa NORD SUD LOGISTICS S.L gestione los servicios ofrecidos a través de su web http://www.NORD SUD LOGISTICS S.L ..es/ . En caso de que no se marque la mencionada casilla no se podrá proceder por parte de NORD SUD LOGISTICS S.L a la gestión de la solicitud.

2. AVISO LEGAL

El texto de Aviso Legal debe estar visible en todas y cada una de las páginas del Sitio Web.

Aviso Legal e informacion sobre las condiciones de uso del sitio web

Datos identificativos del titular del sitio web

En cumplimiento del deber de información estipulado en el artículo 10 de la Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico, NORD SUD LOGISTICS S.L (en lo sucesivo, "NORD SUD LOGISTICS S.L ") y en calidad de titular del web site http://www.NORD SUD LOGISTICS S.L ..es/ , procede a comunicarles los datos identificativos exigidos por la referida norma:

Denominacion social: NORD SUD LOGISTICS S.L .

Domicilio social: Calle Bronce 33-34 CP:28890 Loeches

CIF: B85512788

Direccion de correo electronico: _____.

Datos de inscripcion en el Registro Mercantil: _____.

La presente información conforma y regula las condiciones de uso, las limitaciones de responsabilidad y las obligaciones que, los usuarios de la página Web que se publica bajo el nombre de dominio http://www.NORD SUD LOGISTICS S.L ..es/ , asumen y se comprometen a respetar.

Definiciones

"Página", dominio http://www.NORD SUD LOGISTICS S.L ..es/ que se pone a disposición de los Usuarios de Internet.

"Usuario", persona física o jurídica que utiliza o navega por la Página.

"Contenido", son las páginas que conforman la totalidad del dominio http://www.NORD SUD LOGISTICS S.L ..es/ , las cuales conforman la información y los servicios que NORD SUD LOGISTICS S.L pone a disposición de los Usuarios de Internet. En ellas se contienen los mensajes, textos, fotografías, gráficos, iconos, logos, tecnología, links, texturas, dibujos, archivos de sonido y/o imagen, grabaciones, software, aspecto, diseño gráfico y códigos fuente y, en general, cualquier clase de material contenido en la Página.

"Web", palabra técnica que describe el sistema de acceso a la información vía Internet, que se configura por medio de páginas confeccionadas con lenguaje HTML o similar, y mecanismos de programación tales como java, javascript, PHP, u otros, etc. En estas páginas diseñadas y publicadas bajo un nombre de dominio Internet son el resultado de la información que el titular pone a disposición de los Usuarios de Internet.

"Hiperenlace", técnica por la cual un Usuario puede navegar por diferentes páginas de la Web, o por Internet, con un simple click sobre el texto, icono, botón o indicativo que contiene el enlace.

"Cookies", medio técnico para la "trazabilidad" y seguimiento de la navegación en los sitios Web. Son pequeños ficheros de texto que se escriben en el ordenador del Usuario. Este método tiene

implicaciones sobre la privacidad, por lo que NORD SUD LOGISTICS S.L avisará oportuna y fehacientemente de su utilización en el momento en que se implanten en la Página.

Condiciones de uso

La simple y mera utilización de la Página otorga la condición de usuario de la Página, bien sea persona física o jurídica, y obligatoriamente implica la aceptación completa, plena y sin reservas de todas y cada una de las cláusulas y condiciones generales incluidas en el Aviso Legal. Si el Usuario no estuviera conforme con las cláusulas y condiciones de uso de este Aviso Legal, se abstendrá de utilizar la Página.

Este Aviso Legal está sujeto a cambios y actualizaciones por lo que la versión publicada por NORD SUD LOGISTICS S.L puede ser diferente en cada momento en que el Usuario acceda al Portal. Por tanto, el Usuario debe leer el Aviso Legal en todas y cada una de las ocasiones en que acceda a la Página.

A través de la Página, NORD SUD LOGISTICS S.L facilita a los Usuarios el acceso y la utilización de diversos Contenidos publicados por medio de Internet por NORD SUD LOGISTICS S.L o por terceros autorizados.

El Usuario esta obligado y se compromete a utilizar la Página y los Contenidos de conformidad con la legislación vigente, el Aviso Legal, y cualquier otro aviso o instrucciones puestos en su conocimiento, bien sea por medio de este aviso legal o en cualquier otro lugar dentro de los Contenidos que conforman la Página, así como con las normas de convivencia, la moral y buenas costumbres generalmente aceptadas.

A tal efecto, el Usuario se obliga y compromete a NO utilizar cualquiera de los Contenidos con fines o efectos ilícitos, prohibidos en el Aviso Legal o por la legislación vigente, lesivos de los derechos e intereses de terceros, o que de cualquier forma puedan dañar, inutilizar, sobrecargar, deteriorar o impedir la normal utilización de los Contenidos, los equipos informáticos o los documentos, archivos y toda clase de contenidos almacenados en cualquier equipo informático propios o contratados por NORD SUD LOGISTICS S.L ., de otros Usuarios o de cualquier usuario de Internet (hardware y software).

El Usuario se obliga y se compromete a no transmitir, difundir o poner a disposición de terceros cualquier clase de material contenido en la Página, tales como informaciones, textos, datos, contenidos, mensajes, gráficos, dibujos, archivos de sonido y/o imagen, fotografías, grabaciones, software, logotipos, marcas, iconos, tecnología, fotografías, software, enlaces, diseño gráfico y códigos fuente, o cualquier otro material al que tuviera acceso en su condición de Usuario de la Página, sin que esta enumeración tenga carácter limitativo.

Asimismo, de conformidad con todo ello, el Usuario no podrá:

- Reproducir, copiar, distribuir, poner a disposición o de cualquier otra forma comunicar públicamente, transformar o modificar los Contenidos, a menos que se cuente con la autorización escrita y explícita de NORD SUD LOGISTICS S.L , que es titular de los correspondientes derechos, o bien que ello resulte legalmente permitido.
- Suprimir, manipular o de cualquier forma alterar el "copyright" y demás datos identificativos de la reserva de derechos de NORD SUD LOGISTICS S.L o de sus titulares, de las huellas y/o identificadores digitales, o de cualesquiera otros medios técnicos establecidos para su reconocimiento.

El Usuario deberá abstenerse de obtener e incluso de intentar obtener los Contenidos empleando para ello medios o procedimientos distintos de los que, según los casos, se hayan puesto a su disposición a este efecto o se hayan indicado a este efecto en las páginas Web donde se encuentren los Contenidos o, en general, de los que se empleen habitualmente en Internet a este efecto siempre que no entrañen un riesgo de daño o inutilización de la Página, y/o de los Contenidos.

Propiedad intelectual

Todas las marcas, nombres comerciales o signos distintivos de cualquier clase que aparecen en la Página son propiedad de NORD SUD LOGISTICS S.L o, en su caso, de terceros que han autorizado su uso, sin que pueda entenderse que el uso o acceso al Portal y/o a los Contenidos atribuya al Usuario derecho alguno sobre las citadas marcas, nombres comerciales y/o signos distintivos, y sin que puedan entenderse cedidos al Usuario, ninguno de los derechos de explotación que existen o puedan existir sobre dichos Contenidos.

De igual modo los Contenidos son propiedad intelectual de NORD SUD LOGISTICS S.L , o de terceros en su caso, por tanto, los derechos de Propiedad Intelectual son titularidad de NORD SUD LOGISTICS S.L o de terceros que han autorizado su uso, a quienes corresponde el ejercicio exclusivo de los derechos de explotación de los mismos en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación.

La utilización no autorizada de la información contenida en esta Web, así como la lesión de los derechos de Propiedad Intelectual o Industrial de NORD SUD LOGISTICS S.L o de terceros incluidos en la Página que hayan cedido contenidos dará lugar a las responsabilidades legalmente establecidas.

Hiperenlaces

Aquellas personas que se propongan establecer hiperenlaces entre su página Web y la Página deberán observar y cumplir las condiciones siguientes:

- No será necesaria autorización previa cuando el Hiperenlace permita únicamente el acceso a la página de inicio, pero no podrá reproducirla de ninguna forma. Cualquier otra forma de Hiperenlace requerirá la autorización expresa e inequívoca por escrito por parte de NORD SUD LOGISTICS S.L .
- No se crearán “marcos” (“frames”) con las páginas Web ni sobre las páginas Web de NORD SUD LOGISTICS S.L .
- No se realizarán manifestaciones o indicaciones falsas, inexactas, u ofensivas sobre NORD SUD LOGISTICS S.L ., sus directivos, sus empleados o colaboradores, o de las personas que se relacionen en la Página por cualquier motivo, o de los Usuarios de las Página, o de los Contenidos suministrados.
- No se declarará ni se dará a entender que NORD SUD LOGISTICS S.L ha autorizado el Hiperenlace o que ha supervisado o asumido de cualquier forma los Contenidos ofrecidos o puestos a disposición de la página Web en la que se establece el Hiperenlace.
- La página Web en la que se establezca el Hiperenlace solo podrá contener lo estrictamente necesario para identificar el destino del Hiperenlace.
- La página Web en la que se establezca el Hiperenlace no contendrá informaciones o contenidos ilícitos, contrarios a la moral y a las buenas costumbres generalmente aceptadas y al orden

público, así como tampoco contendrá contenidos contrarios a cualesquiera derechos de terceros.

Cookies

Las cookies son el medio técnico para la "trazabilidad" y seguimiento de la navegación en los Sitios Web. Son pequeños ficheros de texto que se escriben en el ordenador del Usuario. Este método tiene implicaciones sobre la privacidad, por lo que NORD SUD LOGISTICS S.L informa de que podrá utilizar cookies con la finalidad de elaborar estadísticas de utilización del sitio web así como para identificar el PC del Usuario permitiendo reconocerle en sus próximas visitas. En todo caso, el usuario puede configurar su navegador para no permitir el uso de cookies en sus visitas al web site.

Disponibilidad de la Pagina

NORD SUD LOGISTICS S.L no garantiza la inexistencia de interrupciones o errores en el acceso a la Página, a sus Contenidos, ni que éste se encuentren actualizados, aunque desarrollará sus mejores esfuerzos para, en su caso, evitarlos, subsanarlos o actualizarlos. Por consiguiente, NORD SUD LOGISTICS S.L no se responsabiliza de los daños o perjuicios de cualquier tipo producidos en el Usuario que traigan causa de fallos o desconexiones en las redes de telecomunicaciones que produzcan la suspensión, cancelación o interrupción del servicio del Portal durante la prestación del mismo o con carácter previo.

NORD SUD LOGISTICS S.L excluye, con las excepciones contempladas en la legislación vigente, cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de disponibilidad, continuidad o calidad del funcionamiento de la Página y de los Contenidos, al no cumplimiento de la expectativa de utilidad que los usuarios hubieren podido atribuir a la Página y a los Contenidos.

La función de los Hiperenlaces que aparecen en esta Web es exclusivamente la de informar al usuario acerca de la existencia de otras Web que contienen información sobre la materia. Dichos Hiperenlaces no constituyen sugerencia ni recomendación alguna.

NORD SUD LOGISTICS S.L no se hace responsable de los contenidos de dichas páginas enlazadas, del funcionamiento o utilidad de los Hiperenlaces ni del resultado de dichos enlaces, ni garantiza la ausencia de virus u otros elementos en los mismos que puedan producir alteraciones en el sistema informático (hardware y software), los documentos o los ficheros del usuario, excluyendo cualquier responsabilidad por los daños de cualquier clase causados al usuario por este motivo.

El acceso a la Página no implica la obligación por parte de NORD SUD LOGISTICS S.L de controlar la ausencia de virus, gusanos o cualquier otro elemento informático dañino. Corresponde al Usuario, en todo caso, la disponibilidad de herramientas adecuadas para la detección y desinfección de programas informáticos dañinos, por lo tanto, NORD SUD LOGISTICS S.L no se hace responsable de los posibles errores de seguridad que se puedan producir durante la prestación del servicio de la Página, ni de los posibles daños que puedan causarse al sistema informático del usuario o de terceros (hardware y software), los ficheros o documentos almacenados en el mismo, como consecuencia de la presencia de virus en el ordenador del usuario utilizado para la conexión a los servicios y contenidos de la Web, de un mal funcionamiento del navegador o del uso de versiones no actualizadas del mismo.

Calidad de la Pagina

Dado el entorno dinámico y cambiante de la información y servicios que se suministran por medio de la Página, NORD SUD LOGISTICS S.L realiza su mejor esfuerzo, pero no garantiza la completa veracidad, exactitud, fiabilidad, utilidad y/o actualidad de los Contenidos.

La información contenida en las páginas que componen este Portal sólo tiene carácter informativo, consultivo, divulgativo y publicitario. En ningún caso ofrecen ni tienen carácter de compromiso vinculante o contractual.

Limitacion de responsabilidad

NORD SUD LOGISTICS S.L excluye toda responsabilidad por las decisiones que el Usuario pueda tomar basado en esta información, así como por los posibles errores tipográficos que puedan contener los documentos y gráficos de la Página. La información está sometida a posibles cambios periódicos sin previo aviso de su contenido por ampliación, mejora, corrección o actualización de los Contenidos.

Notificaciones

Todas las notificaciones y comunicaciones por parte de NORD SUD LOGISTICS S.L al Usuario realizados por cualquier medio se considerarán eficaces a todos los efectos.

Disponibilidad de los Contenidos

La prestación del servicio de la Página y de los Contenidos tiene, en principio, duración indefinida. NORD SUD LOGISTICS S.L , no obstante, queda autorizada para dar por terminada o suspender la prestación del servicio de la Página y/o de cualquiera de los Contenidos en cualquier momento. Cuando ello sea razonablemente posible, NORD SUD LOGISTICS S.L advertirá previamente la terminación o suspensión de la Página.

Proteccion de Datos de Caracter Personal

NORD SUD LOGISTICS S.L es consciente de la importancia de la privacidad de los datos de carácter personal y por ello, ha implementado una política de tratamiento de datos orientada a proveer la máxima seguridad en el uso y recogida de los mismos, garantizando el cumplimiento de la normativa vigente en la materia y configurando dicha política como uno de los pilares básicos en las líneas de actuación de la entidad.

Durante la navegación a través de la web http://www.NORD SUD LOGISTICS S.L ..es/ es posible que se soliciten datos de carácter personal a través de diferentes formularios dispuestos al efecto. Dichos datos formarán parte de los pertinentes ficheros en función de la finalidad determinada y concreta que motiva el recabo de los mismos.

De esta forma, la información particular de cada tratamiento de datos se aportará junto a cada formulario web, siendo común a todos ellos el responsable del fichero: NORD SUD LOGISTICS S.L domiciliada en la Calle Bronce 33-34 CP:28890 Loeches , así como el lugar y forma de ejercicio de los derechos de acceso, rectificación, cancelación y oposición, que deberá formalizarse mediante una comunicación escrita a la dirección indicada anteriormente incluyendo copia del DNI o documento identificativo equivalente.

En el supuesto de que aporte sus datos a través de un mensaje de correo electrónico, el mismo formará parte de un fichero cuya finalidad será la gestión de la solicitud o comentario que nos realiza, siendo aplicables el resto de extremos indicados en el párrafo anterior.

Asimismo, las condiciones generales de contratación de los servicios de NORD SUD LOGISTICS S.L contienen las características y naturaleza del tratamiento de los datos que serán desarrollados por la misma en el supuesto de que contrate cualquiera de ellos.

Por otro lado, NORD SUD LOGISTICS S.L ha implantado las medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los Datos Personales que los interesados pudieran facilitar como consecuencia del acceso a las diferentes secciones del website http://www.NORD SUD LOGISTICS S.L ..es/ , aplicando las medidas de seguridad contempladas en 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.

Jurisdiccion

Para cuantas cuestiones se susciten sobre la interpretación, aplicación y cumplimiento de este Aviso Legal, así como de las reclamaciones que puedan derivarse de su uso, todos las partes intervinientes se someten a los Jueces y Tribunales de Madrid renunciando de forma expresa a cualquier otro fuero que pudiera corresponderles.

Legislacion aplicable

El Aviso Legal se rige por la ley española.

3. POLITICA DE COOKIES

En caso de que la página web utilice cookies, se deberá informar debidamente a las personas que accedan a la página mediante un pop up que aparezca en el momento del primer acceso de la persona a la página web. Dicho aviso deberá decir lo siguiente:

“Política de cookies: Utilizamos "cookies" propias y de terceros para elaborar información estadística y mostrarle publicidad personalizada a través del análisis de su navegación. Si continúa navegando acepta su uso. **Mas informacion y politica de cookies”.**

En el texto subrayado y en negrita, deberá ponerse un enlace a la política más extensa de cookies, que deberá incluir la siguiente información:

“Una cookie es un fichero que se descarga en el ordenador/smartphone/tablet del usuario al acceder a determinadas páginas web para almacenar y recuperar información sobre la navegación que se efectúa desde dicho equipo. Para conocer más información sobre las cookies, NORD SUD LOGISTICS S.L (NORD SUD LOGISTICS S.L) le invita a acceder al siguiente enlace: http://www.iabspain.net/privacidadeninternet/usuario.

Las cookies utilizadas por nuestra página web son de los siguientes tipos:

- Cookies estrictamente necesarias para la prestación de determinados servicios solicitados expresamente por el usuario: si se desactivan estas cookies, no podrá recibir correctamente nuestros contenidos y servicios; y
- Cookies analíticas (para el seguimiento y análisis estadístico del comportamiento del conjunto de los usuarios), publicitarias (para la gestión de los espacios publicitarios en base a criterios como la frecuencia en la que se muestran los anuncios) y comportamentales (para la gestión de los espacios publicitarios según el perfil específico del usuario): si se desactivan estas cookies, el sitio web podrá seguir funcionando sin perjuicio de que la información captada por estas cookies sobre el uso de nuestra web y sobre el éxito de los anuncios mostrados en ella permite mejorar nuestros servicios y obtener ingresos que nos permiten ofrecerle de forma gratuita muchos contenidos.

La información obtenida a través de estas cookies, referida al equipo del usuario, podrá ser combinada con sus datos personales sólo si Ud. está registrado en este sitio web.

DESACTIVACIÓN DE COOKIES. El usuario podrá -en cualquier momento- elegir qué cookies quiere que funcionen en este sitio web mediante la configuración del navegador; por ejemplo:

- **Chrome,** desde http://support.google.com/chrome/bin/answer.py?hl=es&answer=95647
- **Explorer**, desde http://windows.microsoft.com/es-es/windows7/how-to-manage-cookies-ininternet-explorer-9
- **Firefox**, desde http://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-que-los-sitioswe
- **Safari,** desde http://support.apple.com/kb/ph5042

8 DERECHOS ARCO

1. PROCEDIMIENTOS DE RESPUESTA AL EJERCICIO DE DERECHOS

El afectado o interesado puede ejercitar sus derechos por cualquier medio: personalmente (in situ), carta, fax, teléfono o e-mail. La recomendación es atender con la máxima prioridad y eficiencia las solicitudes realizadas por parte de los interesados, transmitiendo seriedad y profesionalidad.

Se considera afectado o interesado a la persona física de la cual NORD SUD LOGISTICS S.L posea datos de carácter personal en un fichero propiedad del Empresa: Clientes Potenciales, Clientes, Empleados, Contactos, Proveedores y Candidatos.

RESPONSABILIDADES ANTE EL EJERCICIO DE UN DERECHO

En caso de que NORD SUD LOGISTICS S.L recibiera una comunicación, por cualquiera que sea el medio, en la que se solicitara el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, el empleado receptor de la misma lo pondrá inmediatamente en conocimiento del RESPONSABLE DE SEGURIDAD de NORD SUD LOGISTICS S.L quien procederá según el tipo de derecho solicitado por el afectado.

VERIFICACIÓN DE LOS DATOS DEL AFECTADO ANTE UNA SOLICITUD

Se debe atender la petición del interesado en todo caso. No obstante es necesario obtener la solicitud formal por escrito, conteniendo los siguientes datos:

- Indicación clara de la petición que formula.
- Domicilio a efectos de notificaciones.
- DNI o cualquier otra forma acreditativa de la personalidad del interesado.

2. PROCEDIMIENTO DE RESPUESTA AL EJERCICIO DE UN DERECHO

El afectado puede solicitar en cualquier momento y de forma totalmente gratuita, acceder, rectificar, cancelar u oponerse al tratamiento de los datos que sobre su persona obren en poder de NORD SUD LOGISTICS S.L Se designa a D./Dña._____, de NORD SUD LOGISTICS S.L como Responsable del procedimiento de forma que a través de él se canalice todo el procedimiento de ejercicio de derechos.

2.1 FASES COMUNES DEL PROCEDIMIENTO

1. Cualquier empleado deberá atender la petición del afectado en el momento de la solicitud por cualquier medio en que lo ejerciten, solicitando en cualquier caso que ejercite su derecho por escrito y adjuntando fotocopia del DNI.
2. En caso de rectificaciones de datos de carácter personal de nivel básico (salvo números de cuentas bancarias, cambios de titularidad, etc.) que se realicen por teléfono, el receptor del ejercicio de este derecho realizará comprobaciones en los datos contenidos en sus aplicaciones con el fin de comprobar la identidad del llamante. Comunicándole el empleado al interesado que sus datos han sido rectificados, y preguntándole si desea confirmación de su derecho por escrito.
3. El empleado receptor dirigirá al afectado al RESPONSABLE del procedimiento indicado.
4. En el caso de peticiones in situ por parte del afectado, estando presente el Responsable del Procedimiento, se hará entrega al afectado del formulario de ejercicio de derechos correspondiente para dejar constancia del ejercicio del derecho, y fotocopiará el DNI o documento acreditativo de la personalidad del afectado que deberá firmarlo y se le dará copia estampando el sello de NORD SUD LOGISTICS S.L .. En caso de peticiones in situ no estando presente el Responsable del Procedimiento, el empleado que atienda la solicitud del afectado deberá igualmente entregarle los formularios adecuados a cada derecho adjuntado fotocopia del documento acreditativo de la identidad del interesado, haciendo entrega inmediata al Responsable del Procedimiento a la mayor brevedad posible.
5. Todo ejercicio de derechos realizado por un afectado será puesto en conocimiento del Responsable de Seguridad y de todas aquellas empresas a las cuales se hayan cedido los datos o a empresas que accedan a los mismos.

2.2 FASES ESPECÍFICAS PARA EL ACCESO A DATOS

El afectado puede en cualquier momento solicitar acceder a los datos que sobre su persona obren en poder de NORD SUD LOGISTICS S.L .

6. El RESPONSABLE analizará la situación para comunicar la resolución al afectado antes de 30 días, a contar desde la recepción de la solicitud, procediendo según el caso.

   Es muy importante verificar si el afectado ha ejercido algún tipo de derecho con anterioridad con el fin de tener todos los datos para realizar un análisis exhaustivo de cara a la resolución.

   - En caso de tener algún dato del interesado es especialmente importante verificar que no ha solicitado previamente la cancelación de alguno de ellos (facilitar datos cuya cancelación ha sido solicitada puede suponer un grave problema).
   - Si el afectado ejerció el derecho de acceso en los últimos doce meses sólo es obligatorio acceder a la petición si se acredita un interés legítimo. No obstante, será potestad del RESPONSABLE acceder a la misma.

➢ Si la resolución es atender la solicitud, se recabarán internamente los datos necesarios, remitiendo al afectado la siguiente información:

- Datos personales con indicación de la procedencia de los mismos.
- Finalidad del tratamiento para el que fueron recogidos.
- Empresas a las que se hayan cedido los datos.

➢ Sólo será posible no atender la solicitud en los siguientes casos:

- Ha ejercido el derecho en los últimos 12 meses y no se acredita interés legítimo.
- Si existe un defecto de forma a juicio del RESPONSABLE.

En este casos se indicarán al interesado los motivos por los que no se atiende la solicitud, requiriéndole, en su caso, la subsanación de los requisitos incumplidos para atenderla. Subsanados los requisitos exigidos se dispone de 10 días para contestar.

➢ En el caso de que no se disponga de datos de carácter personal del afectado, la situación deberá igualmente ser comunicada en el plazo de 30 días.

7. La comunicación de la resolución será realizada por el RESPONSABLE al afectado por correo certificado con acuse de recibo en el de plazo máximo de 30 días desde la comunicación de ejercicio del derecho por parte del afectado.

2.3 EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL FICHERO

(2). Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma ..... C.I.F./D.N.I. .....

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en los artículos 27 y 28 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma, y en consecuencia,

SOLICITA,

Que se le facilite gratuitamente el derecho de acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se remita por correo la información a la dirección arriba indicada en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso. Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En .....a.....de.....de 20.....

Firmado

1 Se trata de la petición de información sobre los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Organismo Público o entidad privada) que es quien dispone de los datos. La Agencia Española de Protección de Datos no dispone de sus datos personales sino solamente de la ubicación del citado responsable si el fichero está inscrito en el Registro General de Protección de Datos. 2 Si Vd. desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099. 3 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

2.4 FASES ESPECÍFICAS PARA LA RECTIFICACIÓN DE DATOS

El afectado puede solicitar en cualquier momento que NORD SUD LOGISTICS S.L rectifique los datos que obren en su poder.

6. El RESPONSABLE analizará la situación para comunicar la resolución al afectado antes de 10 días a contar desde la recepción de la solicitud, procediendo según el caso:

- Si la resolución es atender la solicitud, se comunicarán al afectado los datos antiguos y los nuevos datos rectificados que, desde el momento de su solicitud, serán los que figuren en los Ficheros de NORD SUD LOGISTICS S.L .
- En este caso, sólo se podrá no atender la solicitud debido a defectos de forma requiriéndose al afectado la subsanación de los mismos. Una vez subsanados los defectos se procederá a su rectificación inmediata, comunicándole al afectado que se ha procedido a dicha rectificación en el menor tiempo posible.

7. En su caso, el RESPONSABLE velará por que en las distintas aplicaciones disponibles en NORD SUD LOGISTICS S.L se realicen las rectificaciones de los datos del afectado.

8. La comunicación de la resolución será realizada por el RESPONSABLE al afectado por correo certificado con acuse de recibo en el plazo máximo de 10 días desde la comunicación de ejercicio del derecho por parte del afectado.

2.5 FASES ESPECÍFICAS PARA LA CANCELACIÓN DE DATOS

El afectado puede solicitar en cualquier momento la cancelación de sus datos personales que obren en poder de NORD SUD LOGISTICS S.L .

7. El RESPONSABLE analizará la situación para comunicar la resolución al afectado antes de 10 días a contar desde la recepción de la solicitud, procediendo según el caso:

En este caso es necesario considerar que puede existir una obligación legal de conservación de los datos, aunque los datos no se utilizarán para fines distintos del cumplimiento de dicha obligación.

- Si la resolución es atender la solicitud, se procederá a comunicar al afectado que sus datos han sido cancelados y que NORD SUD LOGISTICS S.L no realizará ningún tratamiento de los mismos. En este caso es muy importante tener en cuenta lo siguiente:
  - Si se trata de datos que han sido cedidos o comunicados a terceras empresas, se deberá informar a las mismas para que también procedan a su cancelación en sus Ficheros.
  - No proceder al borrado físico de los datos sino a su bloqueo apartándoles de cualquier proceso o tratamiento hasta que venzan los plazos legales de prescripción de las responsabilidades derivadas de su tratamiento.
- Si la resolución es no atender la solicitud, se informará al interesado de los motivos formales por los que no se atiende la misma, requiriéndole, en su caso, la subsanación de los requisitos incumplidos para poder atender la solicitud. En caso de subsanación el RESPONSABLE deberá atender dicho derecho según el procedimiento indicado.

8. En su caso, el RESPONSABLE velará por que en las distintas aplicaciones disponibles en NORD SUD LOGISTICS S.L se realicen las indicaciones necesarias para garantizar los derechos del afectado.
9. La comunicación de la resolución será realizada por el RESPONSABLE al afectado por correo certificado con acuse de recibo en el plazo máximo de 10 días desde la comunicación de ejercicio de derecho por parte del afectado.

2.6 EJERCICIO DEL DERECHO DE CANCELACIÓN

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de cancelación: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma ..... C.I.F./D.N.I. .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I.....,

del que acompaña copia, por medio del presente escrito ejerce el derecho de cancelación, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en los artículos 31 y 32 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma y en consecuencia,

SOLICITA

Que se proceda a acordar la cancelación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recogida de esta solicitud, y que se me notifique de forma escrita el resultado de la cancelación practicada. Que en caso de que se acuerde dentro del plazo de diez días hábiles que no procede acceder a practicar total o parcialmente las cancelaciones propuestas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la citada Ley Orgánica 15/1999. Que si los datos cancelados hubieran sido comunicados previamente se notifique al responsable del fichero la cancelación practicada con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 4 de la mencionada Ley Orgánica 15/1999.

En .....a.....de.....de 20.....

Firmado

2.7 FASES ESPECÍFICAS PARA LA OPOSICIÓN AL TRATAMIENTO DE DATOS

El afectado puede oponerse al envío de publicidad o a cualquier otro tratamiento diferente a la finalidad estricta para la que se recogen los datos.

7. El RESPONSABLE analizará la situación para comunicar la resolución al afectado antes de 10 días a contar desde la recepción de la solicitud, procediendo según el caso:

- Si la resolución es atender la solicitud, se procederá a comunicar al afectado que sus datos no serán objeto del tratamiento especificado, bien con carácter general o bien para aquellos terceros que haya indicado en caso de oposición a la cesión de datos.
- Si la resolución es no atender la solicitud, se informará al interesado de los motivos formales por los que no se atiende la misma, requiriéndole, en su caso, la subsanación de los requisitos incumplidos para poder atender la solicitud.

8. En su caso, el RESPONSABLE velará por que en las distintas aplicaciones disponibles en NORD SUD LOGISTICS S.L se realicen las indicaciones necesarias para garantizar los derechos del afectado.
9. La comunicación de la resolución será realizada por el RESPONSABLE al afectado por correo certificado con acuse de recibo en el plazo máximo de 10 días desde la comunicación de ejercicio del derecho por parte del afectado.

9 Videovigilancia

1. **AMBITO OBJETIVO Y LEGITIMIZACIÓN.**
2. **INFORMACIÓN**
3. **PRINCIPIOS DE CALIDAD, PROPORCIONALIDAD Y FINALIDAD DEL TRATAMIENTO**
4. **DERECHOS DE LAS PERSONAS**
5. **CANCELACIÓN**
6. **NOTIFICACIÓN DE FICHEROS**
7. **SEGURIDAD Y SECRETO**

1. AMBITO OBJETIVOS Y LEGITIMIZACIÓN

Norma Décima. El tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. (Instrucción 1/2006, de 8 de Noviembre)

Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999.

La creación de un fichero de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

El uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido. La proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que su vulneración puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, aseos, etc... Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona.

Ámbito objetivo.

1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Legitimación.

1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

2. INFORMACIÓN

Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

A) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

B) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.

3. PRINCIPIOS DE CALIDAD, PROPORCIONALIDAD Y FINALIDAD DEL TRATAMIENTO

A) De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

B) Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

C) Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

4. DERECHOS DE LAS PERSONAS

A) Para el ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, el/la afectado/a deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada. El ejercicio de estos derechos se llevará a cabo de conformidad con lo dispuesto en la citada Ley Orgánica y su normativa de desarrollo.

B) El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

C) El/la interesado/a al que se deniegue total o parcialmente el ejercicio de los derechos señalados en el párrafo anterior, podrá reclamar su tutela ante el Director de la Agencia Española de Protección de Datos.

5. CANCELACIÓN

Los datos serán cancelados en el plazo máximo de un mes desde su captación.

6. NOTIFICACIÓN DE FICHEROS

A) La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.

B) A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

7. SEGURIDAD Y SECRETO

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior.

* Hasta la entrada en vigor de la Ley 25/2009, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios, sólo eraconforme a la legislación de protección de datos personales la utilización de dispositivos de videovigilancia si se había contratado con empresas de seguridad privada, debidamente autorizadas por el Ministerio del Interior.

Tras la entrada en vigor el 27 de diciembre de la Ley 25/2009, en cuanto a la instalación de las cámaras, de conformidad con la Ley Ómnibus que reforma la Ley de Seguridad Privada, se liberaliza esta actividad, determinando que la venta, entrega, instalación o mantenimiento de estos sistemas podrá llevarse a cabo por particulares y empresas distintas de las de seguridad privada siempre que la instalación no implique una conexión con centrales de alarma.

- Se modifica por tanto la exigencia de recurrir a empresas de seguridad autorizadas por el Ministerio del Interior y de notificar el contrato a dicho Departamento.

No obstante, la instalación de un sistema de videovigilancia conectado a una central de alarma, sí seguirá requiriendo la concurrencia de los requisitos exigidos hasta ahora; esto es, que el dispositivo sea contratado, instalado y mantenido por una empresa de seguridad privada autorizada por el Ministerio del Interior y que el contrato sea notificado a dicho Departamento.

- En todo caso, deberán cumplirse en el tratamiento de imágenes las normas establecidas en la legislación de Protección de Datos de Carácter Personal, entre las que se incluyen el deber de informar a los interesados, la inscripción de ficheros, y la implantación de medidas de seguridad.

10 Recursos informáticos protegidos

4 ENTORNOS DE LAS COMUNICACIONES.

5 EQUIPAMIENTO Y SISTEMA INFORMATICO

6 PROGRAMAS Y APLICACIONES INFORMATICAS

1. Entornos de las comunicaciones

Código elemento	**1**
Nombre del elemento	**Red privada**

Características de la comunicación	
Red privada de área local	**Red privada**
Acceso a la red desde otras redes (SI/NO)	**NO**
Acceso a Servicios de Internet (SI/NO)	**NO**
Acceso de la red a otras redes (SI/NO)	**NO**
Conexión a Internet mediante	**Fibra**
Características de la red	
Número de puntos de red existentes	**3**
Existen medidas de acceso restringido (SI/NO)	**SI**
Existen medidas de registros de accesos (SI/NO)	**NO**
Instaladas medidas Antivirus (SI/NO)	**SI**
Instaladas medidas Firewall (SI/NO)	**SI**
Instaladas medidas Proxy	**SI**

Descripción de las características generales de la comunicación (Cable, Switch, rack...)	Persona responsable del funcionamiento de los sistemas de la comunicación
Las conexiones son por cable. SWITCH	Angel Ramos
Descripción general de las medidas de seguridad, software, hardware y físicas	Notas:
Los ordenadores disponen de clave de inicio de sesión ya que todas las personas que tienen acceso a la oficina están autorizadas para manejar los datos de todos los ficheros. Existen medidas antivirus en continua actualización.	La conexión en remoto es siempre con previa autorización.

2. Equipamiento y sistema informático

En este apartado se relacionara en un listado todo el equipamiento informático con el que esta dotado el sistema de NORD SUD LOGISTICS S.L .

Código elemento	1
Nombre del elemento	PC Angel Administración
Descripción del elemento	Ordenador Portatil
Finalidad del elemento	Tratamiento y archivo de datos
Ubicación o emplazamiento del elemento	Oficina
Sistema operativo instalado	Windows 10
Relación de ficheros que se procesan en el elemento	Fichero de empleados – RRHH Fichero de Videio vigilancia
Relación de los grupos de trabajo que tienen acceso al elemento	Angel Ramos

Código elemento	2
Nombre del elemento	PC Almacén
Descripción del elemento	PC de sobremesa
Finalidad del elemento	Tratamiento y archivo de datos
Ubicación o emplazamiento del elemento	Oficina
Sistema operativo instalado	Windows 7

Relación de ficheros que se procesan en el elemento	
Relación de los grupos de trabajo que tienen acceso al elemento	Encargado de Almacén

Programas y aplicaciones informáticas

Código elemento	1
Nombre del elemento	Microsoft Office

Proveedor donde se adquirió	Finalidad y procesos del programa o aplicación informática
Microsoft	Archivo de datos y gestión de los mismos.
Fecha adquisición	
Persona o empresa a cargo del mantenimiento	Relación de ficheros que trata el programa
	Fichero de personal – RRHH Fichero de Videovigilancia
Fecha final de la garantía	

Sistema de control de acceso al programa
Identificación de usuario
SI
Límite intentos fallidos

10

Notas:
Se utiliza todo el paquete office