

**DOCUMENTO DE SEGURIDAD**

**Proyecto Técnico para mejorar la infraestructura turística en la ciudad de Jaén**

**Technical Project to improve the tourist infrastructure in the city of Jaén**

Realizado por:

Juan Francisco Abán Fontecha

Cristobal Rodriguez Alba

**INTRODUCCIÓN**

De acuerdo al modelo escogido para desarrollar este documento que es el de la Agencia Española de Protección de Datos (AEPD) dice que el RLOPD específica que se puede disponer de un solo documento que incluya todos los ficheros y tratamientos con datos personales de los que una persona física o jurídica sea responsable, un documento por cada fichero o tratamiento, o los que determine el responsable atendiendo a los criterios organizativos que haya establecido. Cualquiera de las opciones puede ser válida. En este caso se ha optado por el primer tipo, organizando el "documento de seguridad" en dos partes: en la primera se recogen las medidas que afectan a todos los sistemas de información de forma común con independencia del sistema de tratamiento sobre el que se organizan: informatizado, manual o mixto, y en la segunda se incluye un anexo por cada fichero o tratamiento, con las medidas que le afecten de forma concreta. Además, se han especificado aquellas medidas que afectan sólo a ficheros automatizados y las que afectan a los no automatizados de forma exclusiva.

El modelo se ha redactado con el objeto de recopilar las exigencias mínimas establecidas por el Reglamento. Es posible y recomendable incorporar cualquier otra medida que se considere oportuna para aumentar la seguridad de los tratamientos, o incluso, adoptar las medidas exigidas para un nivel de seguridad superior al que por el tipo de información les correspondería, teniendo en cuenta la infraestructura y las circunstancias particulares de la organización.

Dentro del modelo se utilizarán los siguientes símbolos convencionales:

<comentario explicativo>: Entre los caracteres "<" y ">", se encuentran los comentarios aclaratorios sobre el contenido que debe tener un campo. Estos textos no deben figurar en el documento final, y deben desarrollarse para ser aplicados a cada caso concreto.

NIVEL MEDIO: con esta marca se señalarán las medidas que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad medio.

NIVEL ALTO: Con esta marca se señalarán las medidas que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad alto.

AUTOMATIZADOS: Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a ficheros informatizados o automatizados.

MANUALES: Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a ficheros manuales o no automatizados.

Las medidas que no van precedidas de ninguna de estas marcas deben aplicarse con carácter general, tanto a ficheros o tratamientos automatizados como no automatizados y con independencia del nivel de seguridad.

**DOCUMENTO DE SEGURIDAD**

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el RLOPD recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD.

El contenido de este documento queda estructurado como sigue:

* Ámbito de aplicación del documento.
* Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
* Información y obligaciones del personal.
* Procedimientos de notificación, gestión y respuestas ante las incidencias.
* Procedimientos de revisión.

Anexo I. Descripción de ficheros.

Anexo II. Nombramientos.

Anexo III. Autorizaciones de salida o recuperación de datos.

Anexo IV. Delegación de autorizaciones.

Anexo V. Inventario de soportes.

Anexo VI. Registro de Incidencias .

Anexo VII. Encargados de tratamiento.

Anexo VIII. Registro de entrada y salida de soportes.

Anexo IX. Medidas alternativas.

1. **Ámbito de la Aplicación del documento.**

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de Juan Francisco Abán Fontecha, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este

documento, con indicación del nivel de seguridad correspondiente, son los

siguientes:

* Fichero de BBDD de Lugares: Este fichero se encuentra en un sistema automatizado, donde se encuentra toda la información acerca de los lugares que se pueden visitar.
* Fichero de BBDD de Registro: Este fichero contiene la información de la gente que se registra en nuestra aplicación, esto nos permite almacenar su información para posteriores visitas a nuestra aplicación así como identificar comentarios, dado que los datos pedidos a los usuarios de nuestra aplicación son: Nombre, Apellidos, Dirección, Teléfono y/o correo electrónico.

Ambos ficheros tienen un nivel de seguridad básico según establece el artículo 80, del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD).



**Fig. 1. Logo de la Ley de Protección de Datos (L.O.P.D)**

*En el Anexo I se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.*

1. **Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.**

*Identificación y autenticación*

* ***Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales.***

Las medidas que se tendrán en cuenta para acceder a los ficheros de seguridad son varios, a pesar de ser una empresa pequeña, la persona encargada de la protección de los ficheros no tendrá acceso directo a estos, ya que se encuentran albergados en un equipo remoto, localizado en un edificio situado en Jaén en el Polígono de los Olivares Calle Huelma, número 30.



**Fig.2. Localización del edificio donde se encuentran los ficheros**

Dichos ficheros se encuentran en un servidor con grandes medidas de seguridad, como son sala con acceso biométrico y asegurado con contraseñas con una longitud de 8 caracteres mínimo en el que se deben usar minúsculas, mayúsculas, caracteres especiales y números.

Dada la importancia de estos para nuestra aplicación y en concreto para nuestra empresa decidimos además asegurar el edificio con seguridad privada contratada a la empresa Prosegur, este viene con vigilancia 24 horas por cámaras instaladas en las mediaciones y conectadas de manera directa con el cuerpo de policía nacional de la ciudad.

****

**Fig. 3. Logo de Prosegur y del Cuerpo de policía Nacional Español.**

* ***Control de acceso.***

El personal sólo accederán a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados como acceso a la sala donde se encuentra la BBDD a personal autorizado, el acceso a la BBDD de manera remota se hará de manera controlada y sólo por usuarios con usuario y contraseña en esta evitando así intrusiones de terceros y de usuarios sin permiso.

Exclusivamente la persona autorizada para conceder, alterar o anular el acceso autorizado está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del fichero.

Los controles de concesión, alteración y anulación sobre los datos, recaerán sobre el responsable del fichero o base de datos, en este caso es Juan Francisco Abán Fontecha, este es el único usuario con claves para el acceso a la base de datos, que al menos una vez al día hará una conexión remota a esta para aprobar la modificación de datos y anulación de los mismos.

La concesión o alta de usuarios se hará de manera automática, si los datos introducidos pasan los filtros correspondientes en el formulario de alta, permitiéndonos así un poco de libertad y un poco más de agilidad a la hora de registrarse en nuestra aplicación.

En el Anexo I, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista deberá mantenerse actualizada.

* ***Gestión de soportes y documentos.***

Como bien explicamos arriba los documentos en los que se almacenará la BBDD se encontrarán en un edificio con alta seguridad, pero al menos una vez cada dos meses se hará una comprobación de su funcionamiento y de las copias de seguridad en el mismo servidor.

El acceso y realización de dichas comprobaciones se hará por el encargado del fichero designado por la empresa, y este será el unico que tendra un acceso fisico a los ficheros y soportes, sin permitir nunca la salida de dichos soportes fuera de este edificio, tanto es así que no se permitirá entrar con soportes informáticos en la sala.

**

**Fig. 4. Imagen de gestión documental.**

* ***Registro de entrada y salida de soportes.***

Tal como explicamos en el apartado anterior no se permitirá la salida de los soportes del edificio, cada año deberemos ir cambiando los soportes, o cuando estos se averíen.



Estos soportes se someterán a su destrucción en el propio edificio donde se encuentra una máquina EBA 0101HDP para tal uso, evitando así la salida de dichos elementos del servidor.

Antes de hacer uso de esta se debe rellenar el registro automatizado que se encuentra en la entrada de cada sala indicando que se hará entrada de un nuevo dispositivo y salida de otro, procediéndose a su destrucción.

**Fig. 5.EBA 0101HDP.**

Al igual que en la salida se destruye dicho soporte, en la entrada de necesitar un nuevo soporte se procede a formatear a bajo nivel todos aquellos soportes que entren, evitando así la entrada de datos al servidor.

* ***Almacenamiento de la información.***

La información estará almacenada como ya hemos comentado en el servidor, este dispone de un NAS de 12 bahías en concreto el modelo, *QNAP TVS-1282T* dadas sus características este es ideal para lo que necesitamos, es de propiedad de la empresa OleoTourist S.L. por lo que el encargado de su mantenimiento y del buen funcionamiento tiene que pertenecer a dicha empresa, usa una interfaz Thunderbolt lo que nos permitirá una comunicación más rápida y directa a la hora de solicitar datos.



**Fig. 6.Servidor NAS QNAP TVS-1282T.**

La extracción de discos para cambiarlo es muy simple.

* ***Acceso a datos a través de redes de comunicaciones.***

La comunicación con la BBDD de manera externa solo se podrá hacer desde una serie de dispositivos preconfigurados, en este caso son:

# ***Apple MacBook Pro 13" Core i5:*** Cuya dirección MAC es *31-76-3D-4A-6B-26* este pertenece a la empresa OleoTourist S.L. y el encargado de trabajar con este es Juan Francisco Abán Fontecha.

## ***Apple MacBook Pro pantalla Retina:*** Cuya dirección MAC es *CE-6F-45-66-64-67* este pertenece a la empresa OleoTourist S.L. y el encargado de trabajar con este es Cristobal Rodriguez Alba.

El segundo solo se podrá utilizar siempre que el primero esté estropeado de cara a realizar accesos a la BBDD, ya que la única persona con acceso a esta será el encargado del fichero.

El software utilizado para almacenar la BBDD es SQL Server 2017, con la respectiva licencia que nos permite actualizarlo, este nos permite realizar:

* Soporte de transacciones.
* Soporta procedimientos almacenados.
* Incluye también un entorno gráfico de administración, que permite el uso de comandos DDL y DML gráficamente.
* Permite trabajar en modo cliente-servidor, donde la información y datos se alojan en el servidor y los terminales o clientes de la red sólo acceden a la información.
* Además permite administrar información de otros servidores de datos.

Como podemos observar nos permite trabajar modo cliente-servidor, por lo que los dispositivos comentados anteriormente tan solo son clientes para poder consultar información.

* ***Ficheros temporales o copias de trabajo de documentos.***

Este tipo de software y en concreto este tipo de servidores hacen mucho uso de ficheros temporales y copias, lo que nos permite que si nos equivoquemos dar un paso atrás y volver de nuevo a lo que teníamos anteriormente.

En nuestro caso esto puede llegar a ser un problema, por ello debemos plantearnos la necesidad de incluir en nuestro documento un plan para la eliminación de dichos ficheros, dada la información que tenemos en nuestro servidor que es de nivel bajo, no necesitamos que estos datos se eliminen de manera diaria, pero dado que se puede hacer por la no actividad de nuestra aplicación sobre todo por la noche, cada semana los miércoles alrededor de las 3 de la madrugada nuestro servidor tiene un procedimiento que nos permite eliminar ficheros temporales y copias innecesarias.

* ***Copias de respaldo y recuperación.***

La información como bien decimos en el apartado anterior no es de alto nivel, pero sí que es necesaria de cara al uso de nuestra aplicación, para evitar fallos tenemos una política de copias de respaldo, esta consiste en:

* **Identificación de copias:** Mediante una cadena alfanumérica identificamos de manera unívoca cada una de las copias de seguridad realizadas, esta cadena se compone de:

FECHA + TIPO DE COPIA + BREVE DESCRIPCIÓN

Un ejemplo de este sería:

*26112017952INCNUEVOSUSUARIOS*

Esta identificación se colocará encima de los soportes con pegatina ignífugas que se encontrarán en las mediaciones.

* **Tipos de copias:** Dado que nuestro servidor en un principio no tendrá mucho contenido, tras la implementación del sistema y su paso a producción realizaremos una copia completa, cada día se hará una copia incremental seleccionando la hora de menos actividad de nuestra aplicación.

Una vez en producción se pasará a realizar de manera semanal una copia de seguridad completa cada Miércoles en las horas de menos actividad de la app.

* **Ubicación:** Estas copias de seguridad no solo se harán de manera física, ya que de haber algún problema no dispondremos de estas, sino que usaremos el servicio de Dropbox Business con el plan Enterprise permitiendo una mejor protección de dichas copias.



**Fig. 7.Logo Dropbox Business, servicio de copias de seguridad.**

* **Tipo de soporte:** Dichas copias en el sistema online de Dropbox no conocemos el tipo de soporte, pero las copias locales realizadas en nuestro servidor se harán mediante discos SSD, dada su velocidad, la seguridad de las copias tendrá un punto extra que nos ayudará a su protección.

De estos soportes se dispondrán al menos de un par de ellos que esté disponible cerca para alguna emergencia, como ya hemos comentado anteriormente una vez que ha ocurrido con un disco y este no es apto para nuestro servidor se destruye en el mismo centro, apuntando en el mismo registro, al igual que al entrar un nuevo soporte debe ser anotado en el registro y pasarlo por el formateo a bajo nivel antes de que entré dentro del servidor, evitando así la inclusión de información en el servidor y la entrada de virus a este.

* ***Responsable de seguridad.***

El responsable designado para la seguridad y para cumplir todas estas normas es Cristobal Rodriguez Alba, este se encargará de que todas las medidas anteriores se cumplan, así como de la actualización de registros de soportes de entrada y salida.

Además tendrá la capacidad de realizar pequeñas auditorias en el centro del servidor para ver que realmente el personal de la empresa está cumpliendo con dichas normas.

Este debe fomentar la comunicación, entre empleados, para las mejoras de seguridad de la información contenida en el centro del servidor.

1. **Información y obligaciones del personal.**

* **Información al personal**

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente

procedimiento:

1. **En el tablón de anuncios de la empresa estará colgada una tabla con la normativa a cumplir y las sanciones pertinentes**.
2. **Para nuevos empleados y empleadas se les informará en la firma del contrato de las medidas oportunas a seguir y se les informará de que pueden ver en el tablón para consultas oportunas.**
3. **Para todos los empleados y empleadas de OleoTourist S.L. se realizará una asamblea tras la presentación oficial por parte del equipo directivo de esta normativa y se dará unas semanas para que puedan hacer alegaciones para mejorarla, mientras tanto esta se encontrará activa para evitar problemas de seguridad.**
4. **Por último y no menos importante, se realizarán de manera anual revisiones a dicha normativa permitiendo al igual que en el punto anterior la participación del personal, pudiendo llegar a tener una normativa muy completa y que tenga previsto cualquier fallo.**

* **Funciones y obligaciones del personal**

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.Constituye una obligación del personal notificar a Cristobal Rodriguez Alba, como responsable de seguridad, o a Juan Francisco Abán Fontecha, como responsable del fichero, las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en el apartado de “Procedimientos de notificación, gestión y respuesta ante las incidencias. ”Todas las personas deberán guardar el debido secreto y

confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Vamos a ver las funciones y obligaciones de los dos perfiles que tienen acceso a los datos de carácter personal de la empresa:

**EMPLEADO U OPERARIO:** Esté solo dispone de acceso a cierta información como el nombre de usuario, para modificar contraseña de ser solicitado por el propio usuario y previa identificación clara de este.

**RESPONSABLE DEL FICHERO:** Este es el encargado de que se mantenga cierta coherencia en la base de datos, evitando redundancias de producirse, este tiene acceso remoto a esta, además de poder realizar visitas presenciales al servidor que la contiene.

Ambos perfiles trabajan o manejan datos de carácter personal de nivel bajo, dependiendo de su contenido pudiendo llegar a ser de nivel medio, ambos al iniciar su empleo o al promocionar a este como es el caso del responsable del fichero, deben firmar previa lectura el acuerdo de confidencialidad de la empresa, que a pesar de no tener datos de alto nivel estos deben ser protegidos como si lo fuesen.

1. **Procedimientos de notificación, gestión y respuesta ante las incidencias.**

Para informar de todas las incidencias, nuestro sistema notificará automáticamente al responsable del fichero y al de seguridad informando de que ocurrió en la incidencia y cómo se dio. La gestión de la incidencia dependiendo del ámbito, es decir si se encuentra más cerca de la lógica del sistema, se encargará el *responsable del fichero*, si es más cercana a la parte física del sistema, se encargará el *responsable de seguridad*.

El responsable de la gestión de la incidencia debe solucionar inmediatamente la incidencia y dar respuesta a esta, para ello dependiendo de si ha concurrido un ataque a los datos o a la BBDD, se procederá a la investigación de cómo ocurrió y a cambiar ciertas medidas de seguridad o añadir nuevas para evitar esto.

Para responder la incidencia si esta ha ocurrido en la funcionalidad de la aplicación o en su seguridad, se procederá a realizar una actualización y a que

esta esté disponible y sea obligatorio instalarlo para que todos los usuarios puedan hacer uso de la aplicación correctamente y sepan de esta forma que la empresa da respuesta a las incidencias que ocurren para subsanarlas.

1. **Procedimientos de revisión del documento de seguridad.**

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como

consecuencia de los controles periódicos realizados. En todo caso se entenderá

como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Este documento además será revisado como ya comentamos en este mismo documento de manera anual, dado que las medidas de seguridad consideramos que necesitan cambios en este tiempo, y se pueden incluir nuevas medidas que nos ayuden en la protección de los datos. El proceso, iniciado por el Responsable de Seguridad de la Empresa, será el siguiente:

1. Aprobación de la iniciación del proceso por parte del equipo directivo.
2. Estudio y posterior modificaciones tras acuerdo por el equipo de dirección.
3. Publicación tanto en los medios físicos de la empresa como en los logicos.
4. Recepción de alegaciones al documento.
5. Estudio y posterior aprobación de dichas alegaciones.
6. Publicación oficial del documento provisional una vez con las alegaciones.
7. Aceptación del documento final por parte de toda la plantilla.
8. Publicación del documento con las nuevas modificaciones.

En este proceso tendrán cabida todas las alegaciones de cualquier persona que pertenezca a la plantilla de la empresa, pudiendo así mejorar la seguridad de la empresa desde todos los ángulos.

A pesar de este proceso y de que los datos que almacenamos no son de un nivel de seguridad medio ni alto, procederemos cada dos años a hacer una auditoría interna, que nos permita conocer en cada momento qué nivel de seguridad se mantiene en la empresa, procediéndose a dicha auditoría por parte de la plantilla que serán seleccionados de manera que todos y cada uno de los/as empleados/as de la empresa puedan realizarla, siempre que seán expertos en cada una de las partes que sean necesarias.

**ANEXO I. Descripción de ficheros.**

**Nombre del fichero o tratamiento:** ANEXO II. Nombramiento del responsable de seguridad.

**Unidad/es con acceso al fichero o tratamiento:** Unidad de Tratamiento de datos.

**Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:**

□ **Identificador:** 5448956516546F

□ **Nombre:** Nombramiento del responsable de seguridad de OLEOTOURIST S.L.

□ **Equipos empleados:** Equipos situados en el departamento de informática.

□ **Descripción**: Este documento contiene el nombramiento a cargo del responsable de la empresa OleoTourist del responsable de seguridad.

□ **Nivel de medidas de seguridad:** Básico.

□ **Tipo de fichero de BBDD:** SQL Cifrado.

**Nombre del fichero o tratamiento:** ANEXO III. Delegación de Autorizaciones.

**Unidad/es con acceso al fichero o tratamiento:** Unidad Responsable de Gestión y Planificación de actividad empresarial.

**Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:**

□ **Identificador:** 56455648516546W

□ **Nombre:** Delegación de autorización de plantilla de OLEOTOURIST S.L.

□ **Equipos empleados:** Equipos situados en cualquier departamento de la empresa.

□ **Descripción**: Este documento contiene la información necesaria para designar a otra persona que realice ciertas funciones aunque no corresponden a su puesto actual.

□ **Nivel de medidas de seguridad:** Básico.

□ **Tipo de fichero de BBDD:** Texto Plano.

**Nombre del fichero o tratamiento:** ANEXO IV. Inventario de Soportes.

**Unidad/es con acceso al fichero o tratamiento:** Unidad de seguridad.

**Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:**

□ **Identificador:** 5645564857984X

□ **Nombre:** Inventario de soportes de OLEOTOURIST S.L.

□ **Equipos empleados:** Equipos situados en el CPD(Centro de Procesamiento de Datos).

□ **Descripción**: Este documento contiene información de los soportes de los que se dispone en el servidor para el almacenamiento de información.

□ **Nivel de medidas de seguridad:** Básico.

□ **Tipo de fichero de BBDD:** Texto Plano.

**Nombre del fichero o tratamiento:** ANEXO V. Registro de incidencias.

**Unidad/es con acceso al fichero o tratamiento:** Unidad de seguridad.

**Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:**

□ **Identificador:** 54353257984S

□ **Nombre:** Registro de incidencias de OLEOTOURIST S.L.

□ **Equipos empleados:** Cualquier equipo de la empresa.

□ **Descripción**: Este documento contiene información de las incidencias ocurridas en cualquier equipo o soporte de la empresa.

□ **Nivel de medidas de seguridad:** Básico.

□ **Tipo de fichero de BBDD:** Texto Plano.

**ANEXO II. Nombramiento del responsable de seguridad.**



**Nombramiento del responsable de seguridad de OLEOTOURIST S.L.**

El Responsable del Fichero **Don Juan Francisco Abán Fontecha** designa a ***Don Cristobal Rodriguez Alba*** como Responsable de Seguridad para todos los ficheros referenciados en el presente Documento de Seguridad. Con carácter general se encargará de coordinar y controlar las medidas estipuladas en este documento. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde a los Responsables de Ficheros y a los Encargados de Tratamiento.

Firmado:



**Don Juan Francisco Abán Fontecha**

Responsable del Fichero.

**ANEXO III. Delegación de Autorizaciones.**

Para este tipo de acciones, tenemos una plantilla, donde solo necesitamos el autor que delega la autorización, el empleado que recibe la autorización, que acción va a realizar y las firmas de ambos, dicho modelo es el siguiente:



**Delegación de Autorización de empleados de OLEOTOURIST S.L.**

**Don/Doña Nombre y Apellidos**, como **Puesto designado,** designa a ***Don/Doña Nombre y Apellidos***, como **Puesto persona asignada,** a realizar las tareas siguientes:

1-.......................................................................................................................

2-.......................................................................................................................

3-.......................................................................................................................

4-.......................................................................................................................

Dichas tareas pertenecen al **Puesto designado** pero por razones ajenas a la empresa **Don Nombre y Apellidos**, responsable de realizar dichas tareas, se encuentra inhabilitado para ello y designa a **Don/Doña Nombre y Apellidos** para que las realice en su nombre .

Firma responsable: Firma designado:

**Don/Doña Nombre y Apellidos Don/Doña Nombre y Apellidos**

**ANEXO IV. Inventario de soportes.**

En la localización del servidor como ya comentamos en el texto anterior nos encontraremos un pequeño registro que nos permitirá modificarlo cada vez que entre o salga algún soporte informático dentro de dicha sala, este deberá ser notificado a la seguridad, así como pasar por un escáner que formatee dichos discos, evitando así entrada o salida de información de dicha sala. Además de tener en cuenta la destrucción en el mismo centro de los discos erróneos o anticuados mediante la máquina situada en este.

Todo esto debe ser anotado en el registro que contiene una pequeña tabla con la información necesaria como se muestra a continuación:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID Soporte | Formato Soporte | Versión | Acción sobre soporte | Descripción de uso | Razón motivada |
| 874ADJAS | SSD | 1.0 | Destrucción | Renovar disco | Fallo físico no permite uso |

**Tabla ejemplo. Contiene información ficticia pero permite conocer de forma más cercana el uso de cada columna.**

**ANEXO V. Registro de Incidencias.**

Tenemos una plantilla donde solo necesitamos el cliente o empleado que localiza la incidencia, con su nombre y la incidencia en sí. Después de su evaluación se valorará su inmediato reparamiento. Usaremos una cola FIFO, es decir, la primera incidencia que entra es la primera en salir, dando una prioridad si lo que ocurre es algo demasiado importante como la rotura de un disco en el Servidor, este registro al igual que el inventario se conforma de una tabla con información, y sigue el modelo que podemos ver a continuación:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID Incidencia | Breve descripción | Acciones aplicadas | Acciones deseadas | Persona encargada de la incidencia | Persona responsable de la incidencia |
| 12345 | Rotura disco | Llamada por teléfono al responsable | Reposición del disco | Juan Francisco Aban Fontecha | Cristobal Rodriguez Alba |

**Tabla ejemplo. Contiene información ficticia pero permite conocer de forma mas cercana el uso de cada columna.**