LUCIANO HOGAR, S.L.

# DOCUMENTOS GDPR
## Instrucciones de uso de la documentación

# INFORMES REGLAMENTARIOS

## ANÁLISIS DE RIESGOS

Es un informe obligatorio para cualquier RT y ET que sirve para analizar la probabilidad de que existan riesgos en el tratamiento, para así determinar la aplicación de medidas de seguridad adecuadas a los riesgos previstos y establecer la necesidad de llevar a cabo una evaluación de impacto relativa a la protección de datos.

# INFORMES REGLAMENTARIOS

# ANÁLISIS DE RIESGOS

## 1. Identificación de la organización Responsable del tratamiento

De conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016, la organización Responsable del tratamiento es quien determina los fines y los medios del tratamiento de datos personales (Ficheros).

| | |
|---|---|
| **Nombre fiscal** | LUCIANO HOGAR, S.L. |
| **Marca comercial** | LUCIANO HOGAR, S.L. |
| **Actividad** | COMERCIO |
| **Dirección** | CALLE MORENITO DE TALAVERA, Nº 1 - 45600 TALAVERA DE LA REINA (Toledo) |
| **Teléfono** | 925722146 |
| **E-mail** | lucianohogar@gmail.com |
| **DPO** | |

## 2. Identificación de los tratamientos de datos personales

Un fichero es un conjunto estructurado de datos personales accesibles con arreglo a criterios determinados y susceptibles de tratamiento para un fin específico.

| Tratamiento | Descripción | Tipo | Sistema | Categoría |
|---|---|---|---|---|
| LABORAL Y RR HH | Gestión administrativa y laboral del personal empleado en la organización | Responsable | Mixto | BÁSICO |
| CLIENTES Y PROVEEDORES | Gestión comercial con clientes y proveedores. Incluye datos de contacto de personas físicas que presten servicios a una persona jurídica, inclusive los profesionales individuales | Responsable | Mixto | BÁSICO |
| FISCAL Y CONTABLE | Registro de las obligaciones fiscales y contables sujetas a la actividad económica | Responsable | Mixto | BÁSICO |
| CONTACTOS | Comunicación, información y gestión sobre productos y servicios. Incluye contactos web y redes sociales | Responsable | Mixto | BÁSICO |
| REGISTRO JORNADA LABORAL | Registro horario de la jornada laboral para dar cumplimiento al RDL 8/2019, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo | Responsable | Mixto | BÁSICO |

## 3. Protección de datos desde el diseño y por defecto

De conformidad con el artículo 25 del Reglamento (UE) 2016/679, de 27 de abril de 2016 (GDPR), la protección de datos desde el diseño y por defecto se basa en la implementación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que entrañe el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, alcance, contexto y fines del tratamiento.

El Responsable del tratamiento ha analizado el cumplimiento de las siguientes medidas de seguridad, desde el diseño y por defecto, en todas las fases del tratamiento:

- **Finalidad del tratamiento:**
  - Tratamiento de los datos para fines determinados, explícitos y legítimos.
  - No realización de tratamientos posteriores de manera incompatible con dichos fines.
- **Minimización de datos:**
  - Obtención de datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Exactitud de datos**
  - Existencia de mecanismos adecuados para actualizar los datos.
- **Confidencialidad del tratamiento:**
  - Existencia de acuerdos de confidencialidad con el personal autorizado.
  - Existencia de contratos de protección de datos con los intervinientes en el tratamiento (encargados del tratamiento, corresponsables del tratamiento y destinatarios de datos).
  - Existencia de transmisiones de datos a países fuera de la UE.
- **Integridad y seguridad de los datos:**
  - Existencia de medidas de seguridad en los equipos y soportes informáticos, mobiliario y departamentos que contienen datos personales para restringir el acceso a personas no autorizadas y evitar que los datos sean accesibles a un número indeterminado de personas sin la intervención humana.
  - Existencia de medidas adecuadas para garantizar permanentemente la integridad y seguridad física de los datos, la disponibilidad y resiliencia de los sistemas de tratamiento, la restauración de datos mediante copias de respaldo y la supresión efectiva de los datos o la seudonimización de los mismos.
  - Existencia de un protocolo para actuar ante las brechas de seguridad detectadas y, en el caso de producirse una violación de datos, proceder a activar los mecanismos necesarios para mitigar los riesgos que afecten a los derechos y libertades de los interesados, así como los procedimientos para la notificación de la misma a la autoridad de control y la comunicación a los interesados si fuese necesario.
- **Derechos del interesado:**
  - Existencia de un protocolo para posibilitar el ejercicio de los derechos del interesado y resolver sin dilación las solicitudes recibidas.

**4. Análisis de los riesgos del tratamiento**

De conformidad con el artículo 32 del Reglamento (UE) 2016/679, de 27 de abril de 2016 (GDPR), se ha analizado el nivel de seguridad a implantar en la Organización para garantizar la protección de datos, teniendo en cuenta los altos riesgos que pueda tener el tratamiento para los derechos y libertades de los interesados, a consecuencia de:

- La destrucción accidental o ilícita de datos.
- La pérdida, alteración o comunicación no autorizada.
- El acceso a los datos cuando sean transmitidos, conservados u objeto de algún otro tipo de tratamiento.

Para ello, se ha analizado la probabilidad/gravedad de riesgos que conlleva el tratamiento en seis apartados:

1. **Estructura de datos.**
2. **Cumplimiento normativo.**
3. **Organización.**
4. **Recursos.**
5. **Seguridad desde el diseño y por defecto.**
6. **Amenazas.**

La probabilidad/gravedad de riesgos se ha clasificado de la siguiente forma:

1. **Muy bajo** (tratamiento sin riesgos)
2. **Bajo** (tratamiento con pocos riesgos y asumible si se cumple la normativa de protección de datos)
3. **Medio** (tratamiento susceptible de algún riesgo, que precisa de procesos de verificación de las medidas adoptadas)
4. **Alto** (tratamiento susceptible de un alto riesgo, que precisa aplicar medidas adecuadas de seguridad y valorar la necesidad de realizar una evaluación de impacto)
5. **Muy Alto** (tratamiento con un alto riesgo, que precisa realizar una evaluación de impacto)

En las tablas siguientes se detallan todas las actividades de tratamiento de manera que se identifican los riesgos iniciales (en el momento del análisis), las medidas de seguridad adoptadas y los riesgos finales (una vez aplicadas dichas medidas). En el apartado 6 se detallan las amenazas identificadas en los apartados anteriores cuando el riesgo inicial es medio, alto o muy alto.

# 1. ESTRUCTURA DEL TRATAMIENTO

## TRATAMIENTO 1: LABORAL Y RR HH

| Aplicación | Categorías de datos | Tratamientos específicos |
|---|---|---|
| **Finalidades** | | |
| Recursos humanos | | |
| Gestión de nóminas | | |
| Prevención de riesgos laborales servicio externo | | |
| **Origen y procedencia de los datos** | | |
| El mismo interesado o su representante legal | | |
| **Colectivos o categorías de interesados** | | |
| Empleados | | |
| **Datos de carácter identificativo** | | |
| DNI o NIF | BÁSICO | |
| Nombre y apellidos | BÁSICO | |
| Dirección postal o electrónica | BÁSICO | |
| Teléfono | BÁSICO | |
| Firma manual | BÁSICO | |
| Núm. de SS o mutualidad | BÁSICO | |
| **Otros datos tipificados** | | |
| Características personales | BÁSICO | |
| Académicos y profesionales | BÁSICO | |
| Detalles de empleo | BÁSICO | |
| Económicos, financieros y de seguro | BÁSICO | |
| Transacciones de bienes y servicios | BÁSICO | |
| **Sistema de tratamiento** | | |
| Mixto | | |

## TRATAMIENTO 2: CLIENTES Y PROVEEDORES

| Aplicación | Categorías de datos | Tratamientos específicos |
|---|---|---|
| **Finalidades** | | |
| Gestión contable, fiscal y administrativa | | |
| **Origen y procedencia de los datos** | | |
| El mismo interesado o su representante legal | | |

| | | |
|---|---|---|
| **Colectivos o categorías de interesados** | | |
| Clientes y usuarios | | |
| Proveedores | | |
| **Datos de carácter identificativo** | | |
| DNI o NIF | BÁSICO | |
| Nombre y apellidos | BÁSICO | |
| Dirección postal o electrónica | BÁSICO | |
| Teléfono | BÁSICO | |
| Firma manual | BÁSICO | |
| **Otros datos tipificados** | | |
| Características personales | BÁSICO | |
| Circunstancias sociales | BÁSICO | |
| Información comercial | BÁSICO | |
| Económicos, financieros y de seguro | BÁSICO | |
| Transacciones de bienes y servicios | BÁSICO | |
| **Sistema de tratamiento** | | |
| Mixto | | |
| **Categorías de destinatarios de cesiones** | | |
| Organizaciones o personas directamente relacionadas con el responsable | | |

## TRATAMIENTO 3: FISCAL Y CONTABLE

| Aplicación | Categorías de datos | Tratamientos específicos |
|---|---|---|
| **Finalidades** | | |
| Gestión contable, fiscal y administrativa | | |
| **Origen y procedencia de los datos** | | |
| El mismo interesado o su representante legal | | |
| **Colectivos o categorías de interesados** | | |
| Clientes y usuarios | | |
| Proveedores | | |
| **Datos de carácter identificativo** | | |
| DNI o NIF | BÁSICO | |
| Nombre y apellidos | BÁSICO | |
| Dirección postal o electrónica | BÁSICO | |
| Teléfono | BÁSICO | |
| **Sistema de tratamiento** | | |

| | | |
|---|---|---|
| Mixto | | |
| **Categorías de destinatarios de cesiones** | | |
| Bancos, cajas de ahorro y cajas rurales | | |
| Administración tributaria | | |

## TRATAMIENTO 4: CONTACTOS

| Aplicación | Categorías de datos | Tratamientos específicos |
|---|---|---|
| **Finalidades** | | |
| Publicidad y prospección comercial | | |
| **Origen y procedencia de los datos** | | |
| El mismo interesado o su representante legal | | |
| **Colectivos o categorías de interesados** | | |
| Clientes y usuarios | | |
| Personas de contacto | | |
| Solicitantes | | |
| **Datos de carácter identificativo** | | |
| DNI o NIF | BÁSICO | |
| Nombre y apellidos | BÁSICO | |
| Dirección postal o electrónica | BÁSICO | |
| Teléfono | BÁSICO | |
| **Otros datos tipificados** | | |
| Información comercial | BÁSICO | |
| **Sistema de tratamiento** | | |
| Mixto | | |

## TRATAMIENTO 5: REGISTRO JORNADA LABORAL

| Aplicación | Categorías de datos | Tratamientos específicos |
|---|---|---|
| **Finalidades** | | |
| Recursos humanos | | |
| Gestión de nóminas | | |
| | | |
| **Origen y procedencia de los datos** | | |
| El mismo interesado o su representante legal | | |
| | | |
| **Colectivos o categorías de interesados** | | |
| Empleados | | |

| | | |
|---|---|---|
| **Datos de carácter identificativo** | | |
| DNI o NIF | BÁSICO | |
| Nombre y apellidos | BÁSICO | |
| Identificador de usuario | BÁSICO | |
| | BÁSICO | |
| | BÁSICO | |
| **Sistema de tratamiento** | | |
| Mixto | | |
| **Categorías de destinatarios de cesiones** | | |
| Interesados legítimos | | |
| Organismos de la Seguridad Social | | |
| | | |
| | | |

# 2. CUMPLIMIENTO NORMATIVO

## 1. LABORAL Y RR HH

| Concepto | Aplicación | Medidas | Cumplimiento |
|---|---|---|---|
| **Principios del tratamiento** | | | |
| **Legitimación del tratamiento (licitud)** | Para la ejecución de un CONTRATO o precontrato con el interesado (artículo 6.1.b GDPR) | Comprobar que se informe debidamente del tratamiento en el mismo contrato. | Si |
| **Finalidad del tratamiento (limitación de los fines)** | Gestión LABORAL | | Si |
| **Limitación del tratamiento (minimización de los datos)** | Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines | Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise. | Si |
| **Actualización de datos (exactitud)** | EXISTEN PROCEDIMIENTOS para la actualización de datos | Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos. | Si |
| **Conservación de datos (limitación del plazo de conservación)** | Conservados mientras existan prescripciones legales que dictaminen la custodia | Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente. | Si |
| **Protección de datos (integridad y confidencialidad)** | EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción | Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos. | Si |
| **Responsabilidad del tratamiento** | | | |
| **Personal autorizado** | Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento | Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro. | Si |
| **Encargados del tratamiento (ET)** | **Los datos SON TRATADOS por Encargados del tratamiento** y EXISTEN CONTRATOS que garanticen medidas de seguridad adecuadas para la protección de datos y los derechos de los interesados | Asegurarse de que los Encargados del tratamiento hayan firmado los contratos de protección de datos y de que se guarden en un lugar seguro. | Si |
| **Corresponsables del tratamiento (CoRT)** | Los datos NO SON TRATADOS por Corresponsables del tratamiento | | Si |
| **Destinatarios de datos** | Los datos NO SON COMUNICADOS a terceros, salvo obligación legal | | Si |
| **Política de información** | | | |

| | | | |
|---|---|---|---|
| **Transparencia de la información** | Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS | Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. | Si |
| **Información básica del tratamiento** | **Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado | Asegurarse de que se facilite la información del tratamiento al interesado. | Si |
| **Comunicación de la información al interesado** | **Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos | Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos. | Si |
| **Comunicación de datos a terceros** | Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal | | Si |
| **Política de seguridad** | | | |
| **Derechos de los interesados** | Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado. | Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados. | Si |
| **Desde el diseño y por defecto** | SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto | Asegurarse de que las medidas implementadas sean las adecuadas. | Si |
| **Riesgos del tratamiento** | SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados | Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados. | Si |
| **Violaciones de la seguridad** | EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad | Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización. | Si |
| **Medidas de protección de datos** | | | |
| **Acceso a documentos** | SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas | Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas. | Si |
| **Acceso a equipos y redes informáticas** | SE ACCEDE mediante usuario y contraseña personalizados | Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas. | Si |
| **Seguridad de la contraseña** | Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.) | Comprobar que las medidas aplicadas son adecuadas. | Si |
| **Protección de equipos y redes informáticas** | SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados | Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.) | Si |

| | | | |
|---|---|---|---|
| **Copias de respaldo** | SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad | Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad. | Si |
| **Transporte y transmisión de datos** | LO REALIZA personal autorizado con medidas de seguridad | Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas. | Si |
| **Conservación de datos** | Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos | Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas. | Si |
| **Destrucción de datos** | SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.) | Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas. | Si |

## 2. CLIENTES Y PROVEEDORES

| Concepto | Aplicación | Medidas | Cumplimiento |
|---|---|---|---|
| **Principios del tratamiento** | | | |
| **Legitimación del tratamiento (licitud)** | Por un INTERÉS LEGÍTIMO del Responsable del tratamiento o Tercero (artículo 6.1.f GDPR) | Asegurarse de que el tratamiento sea pertinente y adecuado y de que se estime necesario o conveniente para el desarrollo de la actividad del Responsable, siempre y cuando no prevalezcan los intereses o los derechos y libertades del interesado, especialmente si es un niño. | Si |
| **Finalidad del tratamiento (limitación de los fines)** | Gestión COMERCIAL | | Si |
| **Limitación del tratamiento (minimización de los datos)** | Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines | Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise. | Si |
| **Actualización de datos (exactitud)** | EXISTEN PROCEDIMIENTOS para la actualización de datos | Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos. | Si |
| **Conservación de datos (limitación del plazo de conservación)** | Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia | Revisar periódicamente que siga existiendo una relación indefinida entre RT e Interesado para mantener el fin del tratamiento. | Si |

| | | | |
|---|---|---|---|
| **Protección de datos (integridad y confidencialidad)** | EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción | Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos. | Si |
| **Responsabilidad del tratamiento** | | | |
| **Personal autorizado** | Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento | Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro. | Si |
| **Encargados del tratamiento (ET)** | Los datos NO SON TRATADOS por Encargados del tratamiento | | Si |
| **Corresponsables del tratamiento (CoRT)** | Los datos NO SON TRATADOS por Corresponsables del tratamiento | | Si |
| **Destinatarios de datos** | Los datos NO SON COMUNICADOS a terceros, salvo obligación legal | | Si |
| **Política de información** | | | |
| **Transparencia de la información** | Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS | Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. | Si |
| **Información básica del tratamiento** | **Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado | Asegurarse de que se facilite la información del tratamiento al interesado. | Si |
| **Comunicación de la información al interesado** | **Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos | Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos. | Si |
| | **Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos | Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos. | Si |
| **Comunicación de datos a terceros** | Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal | | Si |
| **Política de seguridad** | | | |
| **Derechos de los interesados** | Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado. | Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados. | Si |
| **Desde el diseño y por defecto** | SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto | Asegurarse de que las medidas implementadas sean las adecuadas. | Si |

| | | | |
|---|---|---|---|
| **Riesgos del tratamiento** | SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados | Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados. | Si |
| **Violaciones de la seguridad** | EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad | Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización. | Si |
| **Medidas de protección de datos** | | | |
| **Acceso a documentos** | SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas | Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas. | Si |
| **Acceso a equipos y redes informáticas** | SE ACCEDE mediante usuario y contraseña personalizados | Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas. | Si |
| **Seguridad de la contraseña** | Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.) | Comprobar que las medidas aplicadas son adecuadas. | Si |
| **Protección de equipos y redes informáticas** | SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados | Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.) | Si |
| **Copias de respaldo** | SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad | Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad. | Si |
| **Transporte y transmisión de datos** | LO REALIZA personal autorizado con medidas de seguridad | Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas. | Si |
| **Conservación de datos** | Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos | Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas. | Si |
| **Destrucción de datos** | SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.) | Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas. | Si |

## 3. FISCAL Y CONTABLE

| Concepto | Aplicación | Medidas | Cumplimiento |
|---|---|---|---|
| **Principios del tratamiento** | | | |
| **Legitimación del tratamiento (licitud)** | Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR) | Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también. | Si |

| | | | |
|---|---|---|---|
| **Finalidad del tratamiento (limitación de los fines)** | Gestión DOCUMENTAL | | Si |
| **Limitación del tratamiento (minimización de los datos)** | Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines | Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise. | Si |
| **Actualización de datos (exactitud)** | EXISTEN PROCEDIMIENTOS para la actualización de datos | Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos. | Si |
| **Conservación de datos (limitación del plazo de conservación)** | Conservados mientras existan prescripciones legales que dictaminen la custodia | Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente. | Si |
| **Protección de datos (integridad y confidencialidad)** | EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción | Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos. | Si |
| **Responsabilidad del tratamiento** | | | |
| **Personal autorizado** | Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento | Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro. | Si |
| **Encargados del tratamiento (ET)** | **Los datos SON TRATADOS por Encargados del tratamiento** y EXISTEN CONTRATOS que garanticen medidas de seguridad adecuadas para la protección de datos y los derechos de los interesados | Asegurarse de que los Encargados del tratamiento hayan firmado los contratos de protección de datos y de que se guarden en un lugar seguro. | Si |
| **Corresponsables del tratamiento (CoRT)** | Los datos NO SON TRATADOS por Corresponsables del tratamiento | | Si |
| **Destinatarios de datos** | Los datos NO SON COMUNICADOS a terceros, salvo obligación legal | | Si |
| **Política de información** | | | |
| **Transparencia de la información** | Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS | Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. | Si |
| **Información básica del tratamiento** | **Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado | Asegurarse de que se facilite la información del tratamiento al interesado. | Si |

| | | | |
|---|---|---|---|
| **Comunicación de la información al interesado** | **Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos | Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos. | Si |
| **Comunicación de datos a terceros** | Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal | | Si |
| **Política de seguridad** | | | |
| **Derechos de los interesados** | Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado. | Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados. | Si |
| **Desde el diseño y por defecto** | SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto | Asegurarse de que las medidas implementadas sean las adecuadas. | Si |
| **Riesgos del tratamiento** | SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados | Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados. | Si |
| **Violaciones de la seguridad** | EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad | Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización. | Si |
| **Medidas de protección de datos** | | | |
| **Acceso a documentos** | SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas | Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas. | Si |
| **Acceso a equipos y redes informáticas** | SE ACCEDE mediante usuario y contraseña personalizados | Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas. | Si |
| **Seguridad de la contraseña** | Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.) | Comprobar que las medidas aplicadas son adecuadas. | Si |
| **Protección de equipos y redes informáticas** | SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados | Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.) | Si |
| **Copias de respaldo** | SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad | Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad. | Si |
| **Transporte y transmisión de datos** | LO REALIZA personal autorizado con medidas de seguridad | Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas. | Si |

| | | | |
|---|---|---|---|
| **Conservación de datos** | Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos | Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas. | Si |
| **Destrucción de datos** | SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.) | Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas. | Si |

## 4. CONTACTOS

| Concepto | Aplicación | Medidas | Cumplimiento |
|---|---|---|---|
| **Principios del tratamiento** | | | |
| **Legitimación del tratamiento (licitud)** | Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR) | Guardar documentos probatorios del consentimiento. | Si |
| **Finalidad del tratamiento (limitación de los fines)** | Gestión COMERCIAL | | Si |
| **Limitación del tratamiento (minimización de los datos)** | Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines | Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise. | Si |
| **Actualización de datos (exactitud)** | EXISTEN PROCEDIMIENTOS para la actualización de datos | Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos. | Si |
| **Conservación de datos (limitación del plazo de conservación)** | Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia | Revisar periódicamente que siga existiendo una relación indefinida entre RT e Interesado para mantener el fin del tratamiento. | Si |
| **Protección de datos (integridad y confidencialidad)** | EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción | Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos. | Si |
| **Responsabilidad del tratamiento** | | | |
| **Personal autorizado** | Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento | Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro. | Si |
| **Encargados del tratamiento (ET)** | Los datos NO SON TRATADOS por Encargados del tratamiento | | Si |
| **Corresponsables del tratamiento (CoRT)** | Los datos NO SON TRATADOS por Corresponsables del tratamiento | | Si |

| | | | |
|---|---|---|---|
| **Destinatarios de datos** | Los datos NO SON COMUNICADOS a terceros, salvo obligación legal | | Si |
| **Política de información** | | | |
| **Transparencia de la información** | Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS | Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. | Si |
| **Información básica del tratamiento** | **Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado | Asegurarse de que se facilite la información del tratamiento al interesado. | Si |
| **Comunicación de la información al interesado** | **Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos | Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos. | Si |
| | **Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos | Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos. | Si |
| **Comunicación de datos a terceros** | Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal | | Si |
| **Política de seguridad** | | | |
| **Derechos de los interesados** | Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado. | Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados. | Si |
| **Desde el diseño y por defecto** | SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto | Asegurarse de que las medidas implementadas sean las adecuadas. | Si |
| **Riesgos del tratamiento** | SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados | Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados. | Si |
| **Violaciones de la seguridad** | EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad | Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización. | Si |
| **Medidas de protección de datos** | | | |
| **Acceso a documentos** | SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas | Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas. | Si |
| **Acceso a equipos y redes informáticas** | SE ACCEDE mediante usuario y contraseña personalizados | Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas. | Si |

| | | | |
|---|---|---|---|
| **Seguridad de la contraseña** | Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.) | Comprobar que las medidas aplicadas son adecuadas. | Si |
| **Protección de equipos y redes informáticas** | SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados | Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.) | Si |
| **Copias de respaldo** | SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad | Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad. | Si |
| **Transporte y transmisión de datos** | LO REALIZA personal autorizado con medidas de seguridad | Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas. | Si |
| **Conservación de datos** | Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos | Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas. | Si |
| **Destrucción de datos** | SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.) | Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas. | Si |

## 5. REGISTRO JORNADA LABORAL

| Concepto | Aplicación | Medidas | Cumplimiento |
|---|---|---|---|
| **Principios del tratamiento** | | | |
| **Legitimación del tratamiento (licitud)** | Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR) | Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también. | Si |
| **Finalidad del tratamiento (limitación de los fines)** | Gestión LABORAL | | Si |
| **Limitación del tratamiento (minimización de los datos)** | Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines | Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise. | Si |
| **Actualización de datos (exactitud)** | NO SE PUEDEN ACTUALIZAR los datos porque el fichero no admite manipulación | Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para no manipular los datos. | Si |

| | | | |
|---|---|---|---|
| **Conservación de datos (limitación del plazo de conservación)** | Conservados durante 4 años para el registro horario de jornada laboral | Comprobar que se hayan tomado medidas para conservar los registros de jornada durante cuatro años y que permanezcan a disposición de los trabajadores, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social | Si |
| **Protección de datos (integridad y confidencialidad)** | EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción | Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos. | Si |
| **Responsabilidad del tratamiento** | | | |
| **Personal autorizado** | Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento | Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro. | Si |
| **Encargados del tratamiento (ET)** | **Los datos SON TRATADOS por Encargados del tratamiento** y EXISTEN CONTRATOS que garanticen medidas de seguridad adecuadas para la protección de datos y los derechos de los interesados | Asegurarse de que los Encargados del tratamiento hayan firmado los contratos de protección de datos y de que se guarden en un lugar seguro. | Si |
| **Corresponsables del tratamiento (CoRT)** | Los datos NO SON TRATADOS por Corresponsables del tratamiento | | Si |
| **Destinatarios de datos** | Los datos NO SON COMUNICADOS a terceros, salvo obligación legal | | Si |
| **Política de información** | | | |
| **Transparencia de la información** | Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS | Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. | Si |
| **Información básica del tratamiento** | **Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado | Asegurarse de que se facilite la información del tratamiento al interesado. | Si |
| **Comunicación de la información al interesado** | **Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos | Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos. | Si |
| **Comunicación de datos a terceros** | Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal | | Si |
| **Política de seguridad** | | | |
| **Derechos de los interesados** | Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado. | Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados. | Si |

| | | | |
|---|---|---|---|
| **Desde el diseño y por defecto** | SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto | Asegurarse de que las medidas implementadas sean las adecuadas. | Si |
| **Riesgos del tratamiento** | SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados | Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados. | Si |
| **Violaciones de la seguridad** | EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad | Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización. | Si |
| **Medidas de protección de datos** | | | |
| **Acceso a documentos** | SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas | Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas. | Si |
| **Acceso a equipos y redes informáticas** | SE ACCEDE mediante usuario y contraseña personalizados | Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas. | Si |
| **Seguridad de la contraseña** | Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.) | Comprobar que las medidas aplicadas son adecuadas. | Si |
| **Protección de equipos y redes informáticas** | SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados | Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.) | Si |
| **Copias de respaldo** | SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad | Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad. | Si |
| **Transporte y transmisión de datos** | LO REALIZA personal autorizado con medidas de seguridad | Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas. | Si |
| **Conservación de datos** | Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos | Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas. | Si |
| **Destrucción de datos** | SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.) | Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas. | Si |

# 3. ORGANIZACIÓN

## Locales o delegaciones

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|
| **SEDE PRINCIPAL** | | | | |
| **Tipo de acceso al local** | Entrada libre con control de acceso (personal de recepción, vigilantes, etc.). | Bajo | Se deberán tomar medidas para que el control de acceso sea efectivo. | Muy bajo |
| **Sistema general de control de llaves** | Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas | Bajo | Se deberá llevar un control actualizado del personal con acceso a las llaves. | Muy bajo |
| **Otras medidas de seguridad** | NO EXISTEN medidas de seguridad. | Bajo | Se deberá evaluar la necesidad de implementar alguna medida de seguridad en el acceso a los locales. | Muy bajo |

## Departamentos

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|
| **TIENDA** | | | | |
| **Permiso:** | Limitado a personal autorizado en todo el Departamento. | Bajo | Se deberá llevar un control actualizado del personal con acceso al Departamento. | Muy bajo |
| **Acceso:** | Acceso al Departamento regido por las medidas de seguridad del Local. | Bajo | Se deberá evaluar si las medidas de seguridad del Local son suficientes para proteger los datos. | Muy bajo |
| **Control de llaves:** | Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas. | Bajo | Se deberá llevar un control actualizado del personal con acceso a las llaves. | Muy bajo |
| **Otras medidas de seguridad:** | NO EXISTEN otras medidas de seguridad. | Bajo | Se deberá evaluar la necesidad de implementar alguna medida de seguridad en el acceso a los locales. | Muy bajo |

# 3. RECURSOS

## Software

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|
| ADOBE ACROBAT (TIENDA) | | | | |
| **Control de acceso** | Acceso regido por el control de acceso a los equipos informáticos. | Bajo | Comprobar que existan métodos de identificación y autenticación para acceder a los equipos informáticos. | Muy bajo |
| **Accesos no autorizados** | No existe un control de accesos no autorizados a la aplicación | Bajo | Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados. | Muy bajo |
| **Transmisión de datos** | No se transmiten datos desde la aplicación | Muy bajo | Asegurarse que No se transmiten datos desde la aplicación. | Muy bajo |
| **Registro de accesos** | No existe un registro de accesos a la aplicación y accede más de un usuario | Bajo | Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa. | Muy bajo |
| CORREO ELECTRÓNICO (TIENDA) | | | | |
| **Control de acceso** | Acceso regido por el control de acceso a los equipos informáticos. | Bajo | Comprobar que existan métodos de identificación y autenticación para acceder a los equipos informáticos. | Muy bajo |
| **Accesos no autorizados** | No existe un control de accesos no autorizados a la aplicación | Bajo | Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados. | Muy bajo |
| **Transmisión de datos** | No se transmiten datos desde la aplicación | Muy bajo | Asegurarse que No se transmiten datos desde la aplicación. | Muy bajo |
| **Registro de accesos** | No existe un registro de accesos a la aplicación y accede más de un usuario | Bajo | Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa. | Muy bajo |
| GESTIÓN COMERCIAL (TIENDA) | | | | |
| **Control de acceso** | Acceso regido por el control de acceso a los equipos informáticos. | Bajo | Comprobar que existan métodos de identificación y autenticación para acceder a los equipos informáticos. | Muy bajo |
| **Accesos no autorizados** | No existe un control de accesos no autorizados a la aplicación | Bajo | Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados. | Muy bajo |
| **Transmisión de datos** | No se transmiten datos desde la aplicación | Muy bajo | Asegurarse que No se transmiten datos desde la aplicación. | Muy bajo |
| **Registro de accesos** | No existe un registro de accesos a la aplicación y accede más de un usuario | Bajo | Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa. | Muy bajo |

| | | | | |
|---|---|---|---|---|
| GESTIÓN CONTABLE | | | | |
| **Control de acceso** | Acceso regido por el control de acceso a los equipos informáticos. | Bajo | Comprobar que existan métodos de identificación y autenticación para acceder a los equipos informáticos. | Muy bajo |
| **Accesos no autorizados** | No existe un control de accesos no autorizados a la aplicación | Bajo | Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados. | Muy bajo |
| **Transmisión de datos** | No se transmiten datos desde la aplicación | Muy bajo | Asegurarse que No se transmiten datos desde la aplicación. | Muy bajo |
| **Registro de accesos** | No existe un registro de accesos a la aplicación y accede más de un usuario | Bajo | Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa. | Muy bajo |
| GESTIÓN DE PRIVACIDAD | | | | |
| **Control de acceso** | Acceso regido por el control de acceso a los equipos informáticos. | Bajo | Comprobar que existan métodos de identificación y autenticación para acceder a los equipos informáticos. | Muy bajo |
| **Accesos no autorizados** | No existe un control de accesos no autorizados a la aplicación | Bajo | Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados. | Muy bajo |
| **Transmisión de datos** | No se transmiten datos desde la aplicación | Muy bajo | Asegurarse que No se transmiten datos desde la aplicación. | Muy bajo |
| **Registro de accesos** | No existe un registro de accesos a la aplicación y accede más de un usuario | Bajo | Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa. | Muy bajo |
| GESTIÓN LABORAL | | | | |
| **Control de acceso** | Acceso regido por el control de acceso a los equipos informáticos. | Bajo | Comprobar que existan métodos de identificación y autenticación para acceder a los equipos informáticos. | Muy bajo |
| **Accesos no autorizados** | No existe un control de accesos no autorizados a la aplicación | Bajo | Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados. | Muy bajo |
| **Transmisión de datos** | No se transmiten datos desde la aplicación | Muy bajo | Asegurarse que No se transmiten datos desde la aplicación. | Muy bajo |
| **Registro de accesos** | No existe un registro de accesos a la aplicación y accede más de un usuario | Bajo | Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa. | Muy bajo |
| MICROSOFT OFFICE (TIENDA) | | | | |
| **Control de acceso** | Acceso regido por el control de acceso a los equipos informáticos. | Bajo | Comprobar que existan métodos de identificación y autenticación para acceder a los equipos informáticos. | Muy bajo |
| **Accesos no autorizados** | No existe un control de accesos no autorizados a la aplicación | Bajo | Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados. | Muy bajo |

| | | | | |
|---|---|---|---|---|
| **Transmisión de datos** | No se transmiten datos desde la aplicación | Muy bajo | Asegurarse que No se transmiten datos desde la aplicación. | Muy bajo |
| **Registro de accesos** | No existe un registro de accesos a la aplicación y accede más de un usuario | Bajo | Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa. | Muy bajo |

## Hardware

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|
| PC TIENDA (TIENDA) | | | | |
| **Control de acceso** | Usuario y contraseña personalizados. | Bajo | Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos. | Muy bajo |

## Mobiliario

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|
| CAJ TIENDA (TIENDA) | | | | |
| **Control de acceso** | Cerrado sin mecanismo de seguridad. | Bajo | Se deberán emplear mecanismos que dificulten e impidan el acceso a personal no autorizado mediante llaves u otros dispositivos similares. | Muy bajo |

# SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO

## CONFIDENCIALIDAD DE LA INFORMACIÓN

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|
| **Información del tratamiento al interesado** | | | | |
| **¿Se informa al interesado de los detalles del tratamiento?** | Sí, con cláusulas personalizadas de protección de datos. | Bajo | Asegurarse de que se facilite la información específica del tratamiento de forma clara y transparente. | Muy bajo |
| **¿Se informa al interesado de los derechos que le asisten?** | Sí, con cláusulas personalizadas de protección de datos. | Bajo | Asegurarse de que se facilite la información de todos los derechos que asisten al interesado. | Muy bajo |
| **Transporte y transmisión de datos** | | | | |
| **Transporte de los soportes dentro de la empresa** | Por personal autorizado por el Responsable del tratamiento con medidas de seguridad. | Bajo | Se deberá llevar un control actualizado del personal autorizado y que garantice que las medidas de seguridad son adecuadas. | Muy bajo |
| **Transporte de los soportes fuera de la empresa** | Por personal autorizado por el Responsable del tratamiento con medidas de seguridad. | Bajo | Se deberá llevar un control actualizado del personal autorizado y que garantice que las medidas de seguridad son adecuadas. | Muy bajo |
| **Procedimientos con datos automatizados (digital)** | | | | |
| **Acceso durante el tratamiento digital (pantallas)** | Se tratan impidiendo la visión de los datos a personas no autorizadas. | Bajo | Asegurarse de que se tomen medidas de seguridad que impidan la visión de la información a personas no autorizadas. | Muy bajo |
| **Almacenamiento de los soportes digitales** | Se guardan en un Mobiliario y/o Departamento con medidas de seguridad. | Bajo | Asegurarse de que las medidas de seguridad adoptadas sean adecuadas. | Muy bajo |
| **Destrucción de soportes digitales** | Destructora de soportes digitales. | Bajo | Asegurarse de que el personal use la destructora cuando se desea eliminar información. | Muy bajo |
| **Procedimientos con datos no automatizados (documentos)** | | | | |
| **Acceso durante el tratamiento manual (documentos)** | Se tratan impidiendo el acceso a los datos a personas no autorizadas. | Bajo | Asegurarse de que se tomen medidas de seguridad que impidan la visión de la información a personas no autorizadas. | Muy bajo |
| **Almacenamiento de documentos** | Se guardan en un Mobiliario y/o Departamento con medidas de seguridad. | Bajo | Asegurarse de que las medidas de seguridad adoptadas sean adecuadas. | Muy bajo |
| **Destrucción de documentos** | Destructora de papel. | Bajo | Asegurarse de que el personal use la destructora cuando se desea eliminar información. | Muy bajo |
| **Otras medidas de seguridad** | | | | |

| | | | | |
|---|---|---|---|---|
| **¿Se lleva un registro de accesos a categorías especiales de datos?** | NO SE TRATAN categorías especiales de datos. | Muy bajo | Asegurarse que no se tratan datos de categoría especial. | Muy bajo |

## SISTEMAS DE INFORMACIÓN

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|
| **Acceso a equipos informáticos** | | | | |
| **Control de acceso a equipos informáticos** | Usuario y contraseña personalizados. | Bajo | Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos. | Muy bajo |
| **Control de acceso a ficheros con datos personales** | Acceso a los ficheros y/o programa mediante contraseña. | Bajo | Se deberá llevar un control actualizado del personal con acceso a las aplicaciones informáticas. | Muy bajo |
| **Otros tipos de acceso a equipos informáticos** | Ninguno | Muy bajo | Asegurarse que no existe ningún otro sistema de acceso. | Muy bajo |
| **Acceso a redes informáticas** | | | | |
| **Acceso directo a los sistemas de información (conexión de red)** | Usuario y contraseña personalizados. | Bajo | Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos. | Muy bajo |
| **Acceso inalámbrico a los sistemas de información (Wifi, Bluetooth, etc.)** | Acceso restringido por clave de seguridad. | Bajo | Cambiar la clave de seguridad ofrecida por el proveedor para evitar que sea usada por personas no autorizadas. | Muy bajo |
| **Acceso remoto a los sistemas de información** | Usuario y contraseña personalizados. | Bajo | Se deberá llevar un control actualizado del personal con acceso remoto a los sistemas. | Muy bajo |
| **Cifrado de las conexiones remotas** | Sí. | Bajo | Comprobar que la conexión remota esté cifrada punto a punto. | Muy bajo |
| **Sistema de identificación y autenticación** | | | | |
| **Sistema de identificación (USUARIO)** | Palabra identificativa y personalizada para cada usuario. | Bajo | Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos. | Muy bajo |
| **Sistema de autenticación (CONTRASEÑA)** | Contraseña personalizada para cada usuario. | Bajo | Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente. | Muy bajo |
| **Cifrado de la contraseña** | La contraseña está cifrada | Bajo | Comprobar que el cifrado de la contraseña no pueda descifrarse. | Muy bajo |
| **Combinación de caracteres** | La contraseña se compone al menos de 8 caracteres, con algún número, mayúscula, minúscula y símbolo o carácter especial | Bajo | Comprobar que el sistema no deje guardar una contraseña insegura. | Muy bajo |
| **Intentos reiterados de acceso** | Se ha implementado un sistema que impide los intentos reiterados no autorizados | Bajo | Comprobar que el sistema avise al RT de los intentos no autorizados. | Muy bajo |

| | | | | |
|---|---|---|---|---|
| **Caducidad de la contraseña** | La contraseña se cambia al menos una vez al año | Bajo | Comprobar que el sistema obligue a cambiar la contraseña periódicamente. | Muy bajo |

## INTEGRIDAD DE LA INFORMACIÓN

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|
| **Copias de respaldo** | | | | |
| **Ubicación de las copias** | Se guardan en un Hardware distinto del que las crea (copia de red). | Bajo | Se deberá llevar un control actualizado del personal con acceso a las copias de seguridad. | Muy bajo |
| **Periodicidad de programación** | Semanalmente, como mínimo. | Bajo | Comprobar que se realizan las copias, al menos semanalmente. | Muy bajo |
| **Periodicidad de comprobación de datos** | Diarias | Muy bajo | | Muy bajo |
| **Método de comprobación de datos** | Aplicación informática de verificación de copias. | Bajo | Comprobar que la verificación de copias contenga los datos copiados. | Muy bajo |
| **Copias de respaldo externas** | | | | |
| **Ubicación de las copias externas** | Local o departamento distinto de donde se creó. | Bajo | Asegurarse de que la ubicación tenga medidas adecuadas de seguridad. | Muy bajo |
| **Periodicidad de programación de las copias externas** | Semanalmente, como mínimo. | Bajo | Comprobar que se realizan las copias, al menos semanalmente. | Muy bajo |
| **Cifrado de los datos de las copias externas** | NO se cifran las copias porque no salen de los locales de la empresa. | Muy bajo | Asegurarse que las copias no salen de la empresa. | Muy bajo |
| **Disponibilidad de los datos** | | | | |
| **Disponibilidad de los servicios de información** | EXISTEN medidas para garantizar la disponibilidad de los datos | Bajo | Comprobar que las medidas implementadas garanticen la disponibilidad de los datos (copias de respaldo, antivirus, SAI, etc.) | Muy bajo |
| **Restauración de los servicios de información** | EXISTEN medidas para restaurar rápidamente la disponibilidad y el acceso a los datos | Bajo | Comprobar que las medidas implementadas garanticen la restauración de la disponibilidad y el acceso a los datos. | Muy bajo |
| **Resiliencia de los servicios de información** | EXISTEN medidas para anticiparse y adaptarse a cambios imprevistos en los servicios de información | Bajo | Asegurarse de que exista un protocolo para anticiparse y adaptarse a cambios imprevistos en los servicios de información. | Muy bajo |
| **Procesos de verificación, evaluación y valoración de las medidas de seguridad** | SE HAN ESTABLECIDO procesos para verificar, evaluar y valorar la eficacia de las medidas de seguridad | Bajo | Asegurarse de que exista un protocolo para verificar, evaluar y valorar la eficacia de las medidas de seguridad. | Muy bajo |

## TRATAMIENTOS ESPECÍFICOS

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|

| Tratamientos específicos | | | | |
|---|---|---|---|---|
| **Tratamiento de datos de niños menores de 14 años** | NO SE REALIZAN tratamientos de datos de niños menores de 14 años | Muy bajo | Asegurarse que NO SE REALIZAN tratamientos de datos de niños menores de 14 años. | Muy bajo |
| **Tratamiento de datos de personas en situación de vulnerabilidad** | NO SE REALIZAN tratamientos de datos de personas en situación de vulnerabilidad | Muy bajo | Asegurarse que NO SE REALIZAN tratamientos de datos de personas en situación de vulnerabilidad. | Muy bajo |
| **Tratamiento de datos que puede invadir la intimidad de las personas** | NO SE REALIZAN tratamientos que pueden invadir la intimidad de las personas | Muy bajo | Asegurarse que NO SE REALIZAN tratamientos que pueden invadir la intimidad de las personas. | Muy bajo |
| **Vulneración de los derechos y libertades fundamentales** | NO SE REALIZAN tratamientos que vulneren los derechos o libertades fundamentales | Muy bajo | Asegurarse que NO SE REALIZAN tratamientos que vulneren los derechos o libertades fundamentales. | Muy bajo |

## INTERNET

| Concepto | Aplicación | Riesgo inicial | Medidas | Riesgo final |
|---|---|---|---|---|
| **Comunicaciones electrónicas** | | | | |
| **Correo electrónico** | SE UTILIZA correo electrónico seguro mediante cifrado punto a punto. | Muy bajo | Comprobar que el servidor de correo utiliza un cifrado SSL/TLS para la transmisión de mensajes. | Muy bajo |
| **Cláusula de protección de datos** | SE HA PUBLICADO una cláusula de protección de datos con información adecuada del tratamiento. | Muy bajo | Comprobar que la cláusula de protección de datos contiene el nombre del responsable y DPO si existe, el fin y legitimación del tratamiento, los criterios de conservación de los datos, la comunicación a terceros, los derechos que asisten al usuario y los datos de contacto para ejercer los derechos. | Muy bajo |

# 6 AMENAZAS

## 1. CUMPLIMIENTO NORMATIVO

No existen riesgos en los recursos utilizados

## 2. ORGANIZACIÓN

No existen riesgos en los recursos utilizados

## 3. RECURSOS

No existen riesgos en los recursos utilizados

## SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO

No existen riesgos en los recursos utilizados