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	FERNANDEZ LOPEZ, LORENA
Marca comercial	
Actividad	DIETISTA-NUTRICIONISTA
Dirección	CL. EMILIO FERREIRO, 31-33 - BJ 32004 OURENSE (Ourense)
Teléfono	622633277
E-mail	info@lodelicius.com; deliciouslorenadn@gmail.com
DPO	No necesario

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.

Fichero	Descripción	Tipo	Sistema	Categoría
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
EMAIL	Gestión, respuesta y almacenamiento de las peticiones de información recibidas via email.	Responsable	Mixto	BÁSICO
VIDEOVIGILANCIA	Grabación visual de personas por motivos de seguridad	Responsable	Digital	BÁSICO
COOKIES ANALÍTICAS	Analizar los hábitos de navegación de los usuarios que visitan la página web para mejorar los servicios que se ofrecen	Responsable	Digital	BÁSICO
USUARIOS WEB	Gestión de los datos de las cuentas de usuarios registrados para acceso a la web	Responsable	Digital	BÁSICO
DIETÉTICO Y TERAPÉUTICO	Gestión de dietas y seguimientos nutricionales	Responsable	Mixto	ESPECIAL
CONTACTOS	Comunicación, información y gestión sobre productos y servicios. Incluye contactos web y redes sociales	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 DE DATOS

FICHERO 1: CLIENTES Y PROVEEDORES

Aplicación	Riesgo inicial	Medidas	Riesgo final
Finalidades			
Gestión contable, fiscal y administrativa	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Origen y procedencia de los datos			
El mismo interesado o su representante legal	Sin riesgo		Sin riesgo
Colectivos o categorías de interesados			
Clientes y usuarios	Sin riesgo		Sin riesgo
Proveedores	Sin riesgo		Sin riesgo
Datos de carácter identificativo			
DNI o NIF	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Nombre y apellidos	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Dirección postal o electrónica	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Teléfono	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Firma manual	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Otros datos tipificados			
Características personales	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Circunstancias sociales	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Información comercial	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Económicos, financieros y de seguro	Bajo	Se deben tomar medidas para que los datos no se usen para otra finalidad no autorizada.	Muy bajo
Transacciones de bienes y servicios	Bajo	Se deben tomar medidas para que los datos no se usen para otra finalidad no autorizada.	Muy bajo
Sistema de tratamiento			
Mixto	Sin riesgo		Sin riesgo
Categorías de destinatarios de cesiones			
Organizaciones o personas directamente relacionadas con el responsable	Bajo	Asegurarse de que se hayan suscrito contratos con los destinatarios de datos.	Muy bajo

FICHERO 2: FISCAL Y CONTABLE

Aplicación	Riesgo inicial	Medidas	Riesgo final
Finalidades			
Gestión contable, fiscal y administrativa	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo

Origen y procedencia de los datos			
El mismo interesado o su representante legal	Sin riesgo		Sin riesgo
Colectivos o categorías de interesados			
Clientes y usuarios	Sin riesgo		Sin riesgo
Proveedores	Sin riesgo		Sin riesgo
Datos de carácter identificativo			
DNI o NIF	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Nombre y apellidos	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Dirección postal o electrónica	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Teléfono	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Sistema de tratamiento			
Mixto	Sin riesgo		Sin riesgo
Categorías de destinatarios de cesiones			
Bancos, cajas de ahorro y cajas rurales	Bajo	Asegurarse de que se hayan suscrito contratos con los destinatarios de datos.	Muy bajo
Administración tributaria	Sin riesgo		Sin riesgo

FICHERO 3: EMAIL

Aplicación	Riesgo inicial	Medidas	Riesgo final
Finalidades			
Gestión contable, fiscal y administrativa	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Origen y procedencia de los datos			
El mismo interesado o su representante legal	Sin riesgo		Sin riesgo
Colectivos o categorías de interesados			
Clientes y usuarios	Sin riesgo		Sin riesgo
Personas de contacto	Sin riesgo		Sin riesgo
Solicitantes	Sin riesgo		Sin riesgo
Datos de carácter identificativo			
Nombre y apellidos	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Dirección postal o electrónica	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Teléfono	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Sistema de tratamiento			
Mixto	Sin riesgo		Sin riesgo

FICHERO 4: VIDEOVIGILANCIA

Aplicación	Riesgo inicial	Medidas	Riesgo final
Finalidades			
Videovigilancia	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Fines de interés público basados en la legislación vigente	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Origen y procedencia de los datos			
El mismo interesado o su representante legal	Sin riesgo		Sin riesgo
Colectivos o categorías de interesados			
Empleados	Sin riesgo		Sin riesgo
Clientes y usuarios	Sin riesgo		Sin riesgo
Proveedores	Sin riesgo		Sin riesgo
Personas de contacto	Sin riesgo		Sin riesgo
Datos de carácter identificativo			
Imagen	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Otros datos tipificados			
Características personales	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Sistema de tratamiento			
Automatizado	Sin riesgo		Sin riesgo

FICHERO 5: COOKIES ANALÍTICAS

Aplicación	Riesgo inicial	Medidas	Riesgo final
Finalidades			
Publicidad y prospección comercial	Bajo	- Obtener el consentimiento explícito del interesado. - No utilizar los datos para otros fines no autorizados.	Muy bajo
Origen y procedencia de los datos			
El mismo interesado o su representante legal	Sin riesgo		Sin riesgo
Colectivos o categorías de interesados			
Clientes y usuarios	Sin riesgo		Sin riesgo
Datos de carácter identificativo			
Dirección IP	Bajo	No utilizar los datos para otros fines no autorizados.	Bajo

Sistema de tratamiento			
Automatizado	Sin riesgo		Sin riesgo
Categorías de destinatarios de cesiones			
Organizaciones o personas directamente relacionadas con el responsable	Bajo	Asegurarse de que se hayan suscrito contratos con los destinatarios de datos.	Muy bajo

FICHERO 6: USUARIOS WEB

Aplicación	Riesgo inicial	Medidas	Riesgo final
Finalidades			
Gestión datos usuarios web	Bajo	No utilizar los datos para otros fines no autorizados.	Bajo
Origen y procedencia de los datos			
El mismo interesado o su representante legal	Sin riesgo		Sin riesgo
Colectivos o categorías de interesados			
Clientes y usuarios	Sin riesgo		Sin riesgo
Solicitantes	Sin riesgo		Sin riesgo
Datos de carácter identificativo			
DNI o NIF	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Nombre y apellidos	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Dirección postal o electrónica	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Teléfono	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Sistema de tratamiento			
Automatizado	Sin riesgo		Sin riesgo
Categorías de destinatarios de cesiones			
Organizaciones o personas directamente relacionadas con el responsable	Bajo	Asegurarse de que se hayan suscrito contratos con los destinatarios de datos.	Muy bajo

FICHERO 7: DIETÉTICO Y TERAPÉUTICO

Aplicación	Riesgo inicial	Medidas	Riesgo final
Finalidades			
Gestión y control sanitario	Bajo	Se deben tomar medidas para que el tratamiento se realice con el consentimiento explícito del interesado y para no permitir el acceso a los datos por parte de personas no autorizadas.	Muy bajo
Historial clínico	Bajo	Se deben tomar medidas para que el tratamiento se realice con el consentimiento explícito del interesado y para no permitir el acceso a los datos por parte de personas no autorizadas.	Muy bajo

Origen y procedencia de los datos			
El mismo interesado o su representante legal	Sin riesgo		Sin riesgo
Colectivos o categorías de interesados			
Clientes y usuarios	Sin riesgo		Sin riesgo
Pacientes	Sin riesgo		Sin riesgo
Padres o tutores	Sin riesgo		Sin riesgo
Solicitantes	Sin riesgo		Sin riesgo
Datos de carácter identificativo			
Nombre y apellidos	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Dirección postal o electrónica	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Teléfono	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Marcas físicas	Bajo	Siempre que el tratamiento permita la identificación unívoca de la persona, se deben tomar medidas para que el tratamiento se realice con el consentimiento explícito del interesado y no se usen los datos para otra finalidad no autorizada.	Muy bajo
Otros datos especialmente protegidos			
Salud	Bajo	- Obtener el consentimiento explícito del interesado para fines determinados. - Controlar el destino de los datos para garantizar que no se usen para otros fines no autorizados. - Implementar mecanismos que impidan el acceso a datos por parte de personas no autorizadas. - Seudonimizar los datos para que, si se produce un acceso no autorizado, este no tenga efectos para el interesado.	Muy bajo
Otros datos tipificados			
Características personales	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Sistema de tratamiento			
Mixto	Sin riesgo		Sin riesgo

FICHERO 8: CONTACTOS

Aplicación	Riesgo inicial	Medidas	Riesgo final
Finalidades			
Publicidad y prospección comercial	Bajo	- Obtener el consentimiento explícito del interesado. - No utilizar los datos para otros fines no autorizados.	Muy bajo
Origen y procedencia de los datos			
El mismo interesado o su representante legal	Sin riesgo		Sin riesgo
Colectivos o categorías de interesados			
Clientes y usuarios	Sin riesgo		Sin riesgo

Personas de contacto	Sin riesgo		Sin riesgo
Solicitantes	Sin riesgo		Sin riesgo
Datos de carácter identificativo			
DNI o NIF	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Nombre y apellidos	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Dirección postal o electrónica	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Teléfono	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Otros datos tipificados			
Información comercial	Bajo	No utilizar los datos para otros fines no autorizados.	Muy bajo
Sistema de tratamiento			
Mixto	Sin riesgo		Sin riesgo

2. CUMPLIMIENTO NORMATIVO

FICHERO 1. CLIENTES Y PROVEEDORES

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Principios del tratamiento				
Legitimación del tratamiento (licitud)	**Tratamiento lícito SIN NECESIDAD DE CONSENTIMIENTO** por un INTERÉS LEGÍTIMO del Responsable del tratamiento o Tercero	Bajo	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.	Muy bajo
Finalidad del tratamiento (limitación de los fines)	Gestión COMERCIAL	Sin riesgo		Sin riesgo
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Bajo	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.	Muy bajo
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Bajo	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Muy bajo
Conservación de datos (limitación del plazo de conservación)	Conservados INDEFINIDAMENTE mientras sea necesario para mantener el fin del tratamiento	Bajo	Revisar periódicamente que siga existiendo una relación indefinida entre RT e Interesado para mantener el fin del tratamiento.	Muy bajo
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Bajo	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Muy bajo
Responsabilidad del tratamiento				
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Bajo	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Muy bajo
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento	Sin riesgo		Sin riesgo
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento	Sin riesgo		Sin riesgo
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal	Sin riesgo		Sin riesgo

Política de información				
Transparencia de la información	Se facilita la información de forma clara por ESCRITO O por MEDIOS ELECTRÓNICOS	Bajo	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Muy bajo
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	Bajo	Asegurarse de que se facilite la información del tratamiento al interesado.	Muy bajo
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información en el momento de la obtención de datos	Bajo	Asegurarse de que se comunique la información del tratamiento en el momento de la obtención de datos.	Muy bajo
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal	Sin riesgo		Sin riesgo
Política de seguridad				
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE ejercer los derechos del interesado	Bajo	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Muy bajo
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Bajo	Asegurarse de que las medidas implementadas sean las adecuadas.	Muy bajo
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	Bajo	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.	Muy bajo
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Bajo	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.	Muy bajo
Medidas de protección de datos				
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Bajo	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Muy bajo
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Muy bajo
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Bajo	Comprobar que las medidas aplicadas son adecuadas.	Muy bajo

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

FICHERO 2. FISCAL Y CONTABLE

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Principios del tratamiento				
Legitimación del tratamiento (licitud)	**Tratamiento lícito SIN NECESIDAD DE CONSENTIMIENTO** por una OBLIGACIÓN LEGAL del Responsable del tratamiento	Bajo	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Muy bajo
Finalidad del tratamiento (limitación de los fines)	Gestión CONTABLE, FISCAL Y ADMINISTRATIVA	Sin riesgo		Sin riesgo
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Bajo	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.	Muy bajo
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Bajo	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Muy bajo
Conservación de datos (limitación del plazo de conservación)	**Conservados durante MÁS TIEMPO DEL NECESARIO para alcanzar los fines** por una OBLIGACIÓN LEGAL	Bajo	Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente.	Muy bajo

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

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	Bajo	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.	Muy bajo
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Bajo	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.	Muy bajo
Medidas de protección de datos				
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Bajo	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Muy bajo
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Muy bajo
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Bajo	Comprobar que las medidas aplicadas son adecuadas.	Muy bajo
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Bajo	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Muy bajo
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Bajo	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Muy bajo
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Bajo	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Bajo	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Muy bajo
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Bajo	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Muy bajo

FICHERO 3. EMAIL

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Principios del tratamiento				
Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados	Bajo	Guardar documentos probatorios del consentimiento.	Muy bajo

Finalidad del tratamiento (limitación de los fines)	Gestión COMERCIAL	Sin riesgo		Sin riesgo
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Bajo	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.	Muy bajo
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Bajo	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Muy bajo
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Bajo	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Muy bajo
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Bajo	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Muy bajo
Responsabilidad del tratamiento				
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Bajo	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Muy bajo
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento	Sin riesgo		Sin riesgo
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento	Sin riesgo		Sin riesgo
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal	Sin riesgo		Sin riesgo
Política de información				
Transparencia de la información	Se facilita la información de forma clara por ESCRITO O por MEDIOS ELECTRÓNICOS	Bajo	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Muy bajo
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	Bajo	Asegurarse de que se facilite la información del tratamiento al interesado.	Muy bajo
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información en el momento de la obtención de datos	Bajo	Asegurarse de que se comunique la información del tratamiento en el momento de la obtención de datos.	Muy bajo

Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal	Sin riesgo		Sin riesgo
Política de seguridad				
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE ejercer los derechos del interesado	Bajo	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Muy bajo
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Bajo	Asegurarse de que las medidas implementadas sean las adecuadas.	Muy bajo
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	Bajo	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.	Muy bajo
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Bajo	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.	Muy bajo
Medidas de protección de datos				
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Muy bajo
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Bajo	Comprobar que las medidas aplicadas son adecuadas.	Muy bajo
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Bajo	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Muy bajo
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Bajo	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Muy bajo
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Bajo	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Bajo	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Muy bajo

FICHERO 4. VIDEOVIGILANCIA

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final

Principios del tratamiento				
Legitimación del tratamiento (licitud)	**Tratamiento lícito SIN NECESIDAD DE CONSENTIMIENTO** para el cumplimiento de un cometido de INTERÉS PÚBLICO	Bajo	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Muy bajo
Finalidad del tratamiento (limitación de los fines)	Seguridad y VIGILANCIA	Sin riesgo		Sin riesgo
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Bajo	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.	Muy bajo
Actualización de datos (exactitud)	NO SE PUEDEN ACTUALIZAR los datos porque el fichero no admite manipulación	Bajo	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para no manipular los datos.	Muy bajo
Conservación de datos (limitación del plazo de conservación)	Conservados durante un máximo de 30 días para fines de videovigilancia	Bajo	Comprobar que se supriman en el plazo máximo de un mes desde su captación, salvo que se conserven para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tenga conocimiento de la existencia de la grabación	Muy bajo
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Bajo	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Muy bajo
Responsabilidad del tratamiento				
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Bajo	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Muy bajo
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento	Sin riesgo		Sin riesgo
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento	Sin riesgo		Sin riesgo
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal	Sin riesgo		Sin riesgo
Política de información				

Transparencia de la información	Se facilita la información de forma clara mediante ICONOS FORMALIZADOS	Bajo	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Muy bajo
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	Bajo	Asegurarse de que se facilite la información del tratamiento al interesado.	Muy bajo
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información en el momento de la obtención de datos	Bajo	Asegurarse de que se comunique la información del tratamiento en el momento de la obtención de datos.	Muy bajo
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal	Sin riesgo		Sin riesgo
Política de seguridad				
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE ejercer los derechos del interesado	Bajo	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Muy bajo
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Bajo	Asegurarse de que las medidas implementadas sean las adecuadas.	Muy bajo
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	Bajo	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.	Muy bajo
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Bajo	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.	Muy bajo
Medidas de protección de datos				
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Muy bajo
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Bajo	Comprobar que las medidas aplicadas son adecuadas.	Muy bajo
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Bajo	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Muy bajo
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Bajo	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Muy bajo

Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Bajo	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Bajo	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Muy bajo

FICHERO 5. COOKIES ANALÍTICAS

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Principios del tratamiento				
Legitimación del tratamiento (licitud)	Consentimiento INEQUÍVOCO mediante una clara acción del interesado	Bajo	Guardar registros probatorios del consentimiento	Muy bajo
Finalidad del tratamiento (limitación de los fines)	Analizar los hábitos de navegación de los usuarios que visitan la página web	Bajo		Muy bajo
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Bajo	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.	Muy bajo
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Bajo	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Muy bajo
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Bajo	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Muy bajo
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Bajo	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Muy bajo
Responsabilidad del tratamiento				
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Bajo	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Muy bajo

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	Bajo	Asegurarse de que los Encargados del tratamiento hayan firmado los contratos de protección de datos y de que se guarden en un lugar seguro.	Muy bajo
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento	Sin riesgo		Sin riesgo
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal	Sin riesgo		Sin riesgo
Política de información				
Transparencia de la información	Se facilita la información de forma clara por ESCRITO O por MEDIOS ELECTRÓNICOS	Bajo	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Muy bajo
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	Bajo	Asegurarse de que se facilite la información del tratamiento al interesado.	Muy bajo
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información en el momento de la obtención de datos	Bajo	Asegurarse de que se comunique la información del tratamiento en el momento de la obtención de datos.	Muy bajo
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal	Sin riesgo		Sin riesgo
Política de seguridad				
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE ejercer los derechos del interesado	Bajo	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Muy bajo
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Bajo	Asegurarse de que las medidas implementadas sean las adecuadas.	Muy bajo
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	Bajo	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.	Muy bajo
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Bajo	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.	Muy bajo
Medidas de protección de datos				

Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Muy bajo
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Bajo	Comprobar que las medidas aplicadas son adecuadas.	Muy bajo
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Bajo	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Muy bajo
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Bajo	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Muy bajo
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Bajo	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Bajo	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Muy bajo

FICHERO 6. USUARIOS WEB

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Principios del tratamiento				
Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados	Bajo	Guardar documentos probatorios del consentimiento.	Muy bajo
Finalidad del tratamiento (limitación de los fines)	Gestión COMERCIAL	Sin riesgo		Sin riesgo
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Bajo	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.	Muy bajo
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Bajo	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Muy bajo
Conservación de datos (limitación del plazo de conservación)	Conservados INDEFINIDAMENTE mientras sea necesario para mantener el fin del tratamiento	Bajo	Revisar periódicamente que siga existiendo una relación indefinida entre RT e Interesado para mantener el fin del tratamiento.	Muy bajo

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

Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Bajo	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.	Muy bajo
Medidas de protección de datos				
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Muy bajo
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Bajo	Comprobar que las medidas aplicadas son adecuadas.	Muy bajo
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Bajo	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Muy bajo
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Bajo	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Muy bajo
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Bajo	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Bajo	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Muy bajo

FICHERO 7. DIETÉTICO Y TERAPÉUTICO

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Principios del tratamiento				
Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados	Bajo	Guardar documentos probatorios del consentimiento.	Muy bajo
Finalidad del tratamiento (limitación de los fines)	Gestión y control SANITARIO	Sin riesgo		Sin riesgo
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Bajo	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.	Muy bajo

Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Bajo	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Muy bajo
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Bajo	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Muy bajo
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Bajo	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Muy bajo
Responsabilidad del tratamiento				
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Bajo	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Muy bajo
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento	Sin riesgo		Sin riesgo
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento	Sin riesgo		Sin riesgo
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal	Sin riesgo		Sin riesgo
Política de información				
Transparencia de la información	Se facilita la información de forma clara por ESCRITO O por MEDIOS ELECTRÓNICOS	Bajo	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Muy bajo
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	Bajo	Asegurarse de que se facilite la información del tratamiento al interesado.	Muy bajo
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información en el momento de la obtención de datos	Bajo	Asegurarse de que se comunique la información del tratamiento en el momento de la obtención de datos.	Muy bajo
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal	Sin riesgo		Sin riesgo
Política de seguridad				
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE ejercer los derechos del interesado	Bajo	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Muy bajo
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Bajo	Asegurarse de que las medidas implementadas sean las adecuadas.	Muy bajo

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	Bajo	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.	Muy bajo
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Bajo	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.	Muy bajo
Medidas de protección de datos				
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Muy bajo
Acceso a categorías especiales de datos	EXISTEN MEDIDAS adicionales de seguridad (llaves, restricción de acceso, seudonimización, cifrado, etc.)	Bajo	Se deberá llevar un control actualizado del personal con acceso a las categorías especiales de datos.	Muy bajo
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Bajo	Comprobar que las medidas aplicadas son adecuadas.	Muy bajo
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Bajo	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Muy bajo
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Bajo	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Muy bajo
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Bajo	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Conservación de categorías especiales de datos	Se guardan en mobiliario o departamentos CON MEDIDAS DE SEGURIDAD (llave, acceso restringido, etc.)	Bajo	Se deberá llevar un control actualizado del personal con acceso al mobiliario o departamentos que contengan categorías especiales de datos.	Muy bajo
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Bajo	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Muy bajo

FICHERO 8. CONTACTOS

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Principios del tratamiento				
Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados	Bajo	Guardar documentos probatorios del consentimiento.	Muy bajo

Finalidad del tratamiento (limitación de los fines)	Gestión COMERCIAL	Sin riesgo		Sin riesgo
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Bajo	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.	Muy bajo
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Bajo	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Muy bajo
Conservación de datos (limitación del plazo de conservación)	Conservados INDEFINIDAMENTE mientras sea necesario para mantener el fin del tratamiento	Bajo	Revisar periódicamente que siga existiendo una relación indefinida entre RT e Interesado para mantener el fin del tratamiento.	Muy bajo
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Bajo	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Muy bajo
Responsabilidad del tratamiento				
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Bajo	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Muy bajo
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento	Sin riesgo		Sin riesgo
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento	Sin riesgo		Sin riesgo
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal	Sin riesgo		Sin riesgo
Política de información				
Transparencia de la información	Se facilita la información de forma clara por ESCRITO O por MEDIOS ELECTRÓNICOS	Bajo	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Muy bajo
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	Bajo	Asegurarse de que se facilite la información del tratamiento al interesado.	Muy bajo
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información en el momento de la obtención de datos	Bajo	Asegurarse de que se comunique la información del tratamiento en el momento de la obtención de datos.	Muy bajo

Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal	Sin riesgo		Sin riesgo
Política de seguridad				
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE ejercer los derechos del interesado	Bajo	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Muy bajo
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Bajo	Asegurarse de que las medidas implementadas sean las adecuadas.	Muy bajo
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	Bajo	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.	Muy bajo
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Bajo	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.	Muy bajo
Medidas de protección de datos				
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Bajo	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Muy bajo
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Muy bajo
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Bajo	Comprobar que las medidas aplicadas son adecuadas.	Muy bajo
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Bajo	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Muy bajo
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Bajo	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Muy bajo
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Bajo	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Bajo	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Muy bajo

Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Bajo	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Muy bajo

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
CONSULTA				
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
CASA				
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

4. RECURSOS

Software

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
APP VIDEOVIGILANCIA (CONSULTA)				
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	Sin riesgo		Sin riesgo
Registro de accesos	No existe un registro de accesos a la aplicación (sistemas tradicionales)	Muy bajo	Plantearse la necesidad de activar un registro de accesos a la aplicación según el tipo de datos que contiene.	Muy bajo
CORREO ELECTRÓNICO (CONSULTA)				
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	Existe un control de accesos, pero NO se impiden los intentos reiterados no autorizados	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	Sin riesgo		Sin riesgo
Registro de accesos	No existe un registro de accesos a la aplicación (sistemas tradicionales)	Bajo	Plantearse la necesidad de activar un registro de accesos a la aplicación según el tipo de datos que contiene.	Muy bajo
GOOGLE DRIVE (CONSULTA)				
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	Existe un control de accesos, pero NO se impiden los intentos reiterados no autorizados	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	Sin riesgo		Sin riesgo
Registro de accesos	No existe un registro de accesos a la aplicación (sistemas tradicionales)	Bajo	Plantearse la necesidad de activar un registro de accesos a la aplicación según el tipo de datos que contiene.	Muy bajo
MICROSOFT OFFICE (CONSULTA)				

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	Sin riesgo		Sin riesgo
Registro de accesos	No existe un registro de accesos a la aplicación (sistemas TIC)	Bajo	Cuando se traten categorías de datos ESPECIALES o PENALES mediante nuevas tecnologías de la información y comunicación es recomendable registrar los accesos de los usuarios al programa.	Muy bajo
PDF (CONSULTA)				
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	Existe un control de accesos, pero NO se impiden los intentos reiterados no autorizados	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	Sin riesgo		Sin riesgo
Registro de accesos	No existe un registro de accesos a la aplicación (sistemas tradicionales)	Bajo	Plantearse la necesidad de activar un registro de accesos a la aplicación según el tipo de datos que contiene.	Muy bajo
TANITA (CONSULTA)				
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	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
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	No existe un registro de accesos a la aplicación (sistemas tradicionales)	Bajo	Plantearse la necesidad de activar un registro de accesos a la aplicación según el tipo de datos que contiene.	Muy bajo
WHATSAPP (CONSULTA)				
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	Existe un control de accesos, pero NO se impiden los intentos reiterados no autorizados	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	Sin riesgo		Sin riesgo
Registro de accesos	No existe un registro de accesos a la aplicación (sistemas tradicionales)	Bajo	Plantearse la necesidad de activar un registro de accesos a la aplicación según el tipo de datos que contiene.	Muy bajo

Hardware

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
OPO (CONSULTA)				
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
ARM OFICINA (CONSULTA)				
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

Soportes

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
DDU 1 (CONSULTA)				
Control de acceso	Guardado en Mobiliario o Departamento con medidas de seguridad.	Bajo	Asegurarse de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Sistema de etiquetado	No existe etiqueta que identifique los datos guardados	Bajo	Asegurarse de que no se puedan identificar los datos contenidos por personal no autorizado.	Muy bajo
Medidas de seguridad para el transporte fuera de la empresa	Maletín con cerramiento de seguridad.	Bajo	Se deberá llevar un control actualizado del personal con acceso al maletín.	Muy bajo
DDU 2 (CASA)				
Control de acceso	Guardado en Mobiliario o Departamento con medidas de seguridad.	Bajo	Asegurarse de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Sistema de etiquetado	Etiqueta que no identifica los datos del soporte.	Bajo	Asegurarse de que la etiqueta no pueda identificar los datos contenidos por personal no autorizado.	Muy bajo

Medidas de seguridad para el transporte fuera de la empresa	Maletín con cerramiento de seguridad.	Bajo	Se deberá llevar un control actualizado del personal con acceso al maletín.	Muy bajo

5. 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	Manualmente	Muy bajo		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	Manualmente	Muy bajo		Muy bajo
Registro de accesos a categorías especiales de datos				

¿Se lleva un registro de accesos a categorías especiales de datos?	NO SE TRATAN categorías especiales de datos.	Sin riesgo		Sin riesgo

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	Sin riesgo		Sin riesgo
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 (disco duro).	Sin riesgo		Sin riesgo
Periodicidad de programación	Semanalmente, como mínimo.	Bajo	Comprobar que se realizan las copias, al menos semanalmente.	Muy bajo
Periodicidad de comprobación de datos	Como máximo, 6 meses desde la creación.	Bajo	Verificar que se realicen las comprobaciones, al menos semestralmente.	Muy bajo
Método de comprobación de datos	Apertura manual de varios archivos.	Bajo	Comprobar que la inspección de archivos contenga los datos copiados.	Muy bajo
Copias de respaldo externas				
Ubicación de las copias externas	Se guardan en un disco duro ubicado en un local o departamento distinto de donde se creó.	Muy bajo		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.	Sin riesgo		Sin riesgo
Disponibilidad de los datos				
Actualización de *software*	SE ACTUALIZAN periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles	Bajo	Comprobar que se actualicen periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.	Muy bajo
Sistemas de detección de intrusos y prevención de fuga de información	EXISTEN sistemas de protección tipo *firewall*, antivirus, *antispam*, *antiphishing, antimalware, antiransomware*, etc.	Bajo	Comprobar que se hayan implementado sistemas adecuados de detección de intrusos y de prevención de fuga de información.	Muy bajo
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	Sin riesgo		Sin riesgo
Tratamiento de datos de personas en situación de vulnerabilidad	NO SE REALIZAN tratamientos de datos de personas en situación de vulnerabilidad	Sin riesgo		Sin riesgo
Tratamiento de datos que puede invadir la intimidad de las personas	NO SE REALIZAN tratamientos que pueden invadir la intimidad de las personas	Sin riesgo		Sin riesgo
Vulneración de los derechos y libertades fundamentales	NO SE REALIZAN tratamientos que vulneren los derechos o libertades fundamentales	Sin riesgo		Sin riesgo

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

ORGANIZACIÓN

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Organización				
Política de información	EXISTE un protocolo documentado para informar y comunicar el tratamiento al interesado	Bajo	Comprobar periódicamente que haya un responsable de actualizar el protocolo y de hacer que se cumpla.	Muy bajo

Derechos del interesado	EXISTE un protocolo documentado para gestionar y registrar los derechos del interesado	Bajo	Comprobar periódicamente que haya un responsable de actualizar el protocolo y de hacer que se cumpla.	Muy bajo
Política de seguridad	EXISTE un protocolo documentado para garantizar la seguridad de los datos personales y su protección desde el DISEÑO Y POR DEFECTO	Bajo	Comprobar periódicamente que haya un responsable de actualizar el protocolo y de hacer que se cumpla.	Muy bajo
Violaciones de la seguridad	EXISTE un protocolo documentado para gestionar y registrar las violaciones de la seguridad	Bajo	Comprobar periódicamente que haya un responsable de actualizar el protocolo y de hacer que se cumpla.	Muy bajo
Formación en protección de datos	[Se facilita suficiente formación al personal autorizado para tratar datos] mediante la entrega de la política de seguridad	Bajo	Comprobar que se haya entregado la política de seguridad al personal autorizado para tratar datos.	Muy bajo
Delegado de protección de datos (DPO)	[No precisa un DPO porque la actividad principal de la empresa] CONSISTE en tratar datos personales pero NO a GRAN ESCALA, ni regulados en el art. 34 de la LOPDGDD.	Bajo	Comprobar que no exista otra actividad principal que consista en tratar datos personales a gran escala, ni regulados en el art. 34 de la LOPDGDD.	Muy bajo
Evaluación de impacto (DPIA)	[No precisa realizar una DPIA porque] el tratamiento no comporta un alto riesgo para los derechos y libertades de las personas físicas.	Bajo	Asegurarse de que el tratamiento no comporte un alto riesgo para los derechos y libertades de las personas físicas.	Muy bajo

6 AMENAZAS

1. ESTRUCTURA DE DATOS

No existen riesgos en la estructura de datos

2. CUMPLIMIENTO NORMATIVO

No existen riesgos en los recursos utilizados

3. ORGANIZACIÓN

No existen riesgos en los recursos utilizados

4. RECURSOS

No existen riesgos en los recursos utilizados

5. SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO

No existen riesgos en los recursos utilizados

No necesario