Aspectos Sociales, Legales, Éticos y Profesionales de la Informática

Prácticas de laboratorio

Convocatoria ordinaria

Universidad de Oviedo
Escuela de Ingeniería Informática

Trabajo de ASLEPI

Auditoría del RGPD/RMS

CASO 02
Clínica Dental

Dana Álvarez Murillo	Alejandro Campa Martínez	Omar Teixeira González
UO278249	UO282874	UO281847

Curso 2023-2024

Hoja de aclaraciones

Q1: ¿Cuándo un nuevo paciente se da de alta, los datos personales, la información clínica básica y los datos bancarios, se guardan todos en el mismo fichero digital?
A1: *Sí, todo en la misma base de datos.*

Q2: ¿Dónde se almacenan estos datos? ¿Están todos en la base de datos de la aplicación Vitaldent?
A2: *Sí, todos en la misma base de datos.*

Q3: ¿Existen registros físicos de los empleados en la clínica? ¿Cómo se manejan y protegen estos registros?
A3: *Los registros están todos en la misma base de datos, en servidores dentro de territorio UE, no hay nada físico en los ordenadores, físicamente sólo fichas de empleado para necesidades de contacto, guardados en un armario bajo llave.*

Q4: ¿Hay un sistema específico para el registro de citas de los pacientes? ¿En qué formato se almacenan estos datos?
A4: *El registro de pacientes es mediante consultas a la base de datos con el software de la compañía (Web).*

Q5: ¿Qué medidas de seguridad física existen en las instalaciones de la clínica dental? ¿Cómo se protegen los archivos físicos?
A5: *Los archivos físicos, si existen, están bajo llave en un armario.*

Q6: ¿Quién es responsable de recoger los datos de nuevas altas de pacientes y empleados?
A6: *Personal de administración.*

Q7: ¿La misma aplicación que gestiona las citas también se utiliza para la gestión de pacientes? ¿Qué datos maneja esta aplicación?
A7: *Misma aplicación. Usa datos personales como nombre, apellidos, dirección, fechas de nacimiento y patologías bucodentales.*

Q8: ¿Cuáles son las medidas de seguridad actuales implementadas en la base de datos de Vitaldent?
A8: *ISO 27001.*

Q9: ¿Existe un procedimiento establecido para realizar copias de seguridad de los ficheros?
A9: *Tienen un sistema de backup monitorizado.*

Q10: ¿La clínica dental realiza alguna formación o capacitación periódica para los empleados sobre la importancia de la protección de datos y el cumplimiento del RGPD?
A10: *Al inicio se les da una formación en el RGPD.*

Índice

1 INFORME DE AUDITORÍA

1.1 ALCANCE

1.1.1 Objeto

El propósito de este informe es cumplir con la solicitud de la empresa **Donte Group S.L.U. (VITALDENT)** de llevar a cabo una auditoría de los datos proporcionados en el marco del Reglamento General de Protección de Datos (RGPD) [1]. Concretamente esta auditoría se realizará sobre la sede en Asturias del solicitante.

1.1.2 Normativa

El presente informe de auditoría tiene como objetivo verificar el cumplimiento de la normativa actual en materia de seguridad y protección de datos personales, específicamente en el ámbito de una clínica dental. Se han considerado las siguientes regulaciones como referencia:

- Reglamento (UE) 2016/679 General de Protección de Datos (RGPD).
- Ley Orgánica 15/1999 de Protección de Datos Personales (LOPD).
- Reglamento de Desarrollo de la LOPD en Medidas de Seguridad (R.D 1720/2007).

El análisis se centra en asegurar el adecuado tratamiento de datos personales de personas físicas, garantizando el cumplimiento integral de las disposiciones legales establecidas en dichas normativas.

1.1.3 Fecha de la auditoría

El presente documento se realiza a principios de marzo con objetivo de entregar al cliente el documento final para el *martes, 21 de mayo de 2024* como fecha límite.

1.1.4 Identificación del responsable del tratamiento

DONTE GROUP S.L.U. (VITALDENT)	
NIF:	B87619698
DIRECCIÓN:	Parque Empresarial La Finca C/ Paseo del Club Deportivo, s/n. Bloque 3 – Planta Segunda (28233 - Pozuelo de Alarcón) Madrid.
TELÉFONO:	91 375 65 60
CORREO ELECTRÓNICO PARA EJERCICIO DE DERECHOS RELACIONADOS CON LA PROTECCIÓN DE DATOS:	lopd@vitaldent.com

Tabla 1

1.1.5 Identificación del delegado de protección de datos

SEGURIDAD Y PRIVACIDAD DE DATOS S.L. (FORLOPD)	
NIF:	B98689920
DIRECCIÓN:	Avenida Calle Menorca 19, EDIFICIO AQUA MULTIESPACIO, planta 17, (46023 – Valencia).
TELÉFONO:	963 12 28 68
CORREO ELECTRÓNICO DE CONTACTO:	infodpo@forlopd.es

Tabla 2

1.2 SITUACIÓN ACTUAL

1.2.1 Actividad de la empresa

Vitaldent es la compañía líder en España en el sector de la salud dental, con más de 380 clínicas en todo el país. Ofrece servicios integrales de odontología, desde diagnóstico hasta tratamientos innovadores, con un enfoque en la calidad y la accesibilidad para todos.

1.2.2 Organización de la empresa y equipamiento

Respecto a la organización, Vitaldent opera bajo un modelo de negocio mixto, combinando clínicas propias con franquicias. La sede central se encuentra en Pozuelo de Alarcón (Madrid), desde donde se gestionan aspectos como marketing, compras, formación y soporte a las clínicas. Cada clínica, ya sea propia o franquicia, cuenta con un equipo de profesionales de la salud dental, incluyendo odontólogos, higienistas y auxiliares.
Además, Vitaldent se enorgullece de utilizar tecnología de vanguardia en sus clínicas. Esto incluye:

- **Equipos de radiodiagnóstico:** Radiografías digitales y ortopantomografías para un diagnóstico preciso y rápido.
- **Escáneres intraorales:** Para tomar impresiones digitales en 3D, mejorando la precisión y comodidad de los tratamientos.
- **Láser dental:** Utilizado en diversas intervenciones, como cirugía, blanqueamiento y tratamiento de encías.
- **Sillones dentales ergonómicos:** Para garantizar la comodidad del paciente durante los procedimientos.
- **Software de gestión dental:** Para optimizar la gestión de citas, historiales clínicos y facturación.

Además, también invierte en la formación continua de su personal para garantizar que estén al día con las últimas técnicas y tecnologías en el campo de la odontología

1.2.3 Gestión de información de la empresa

Vitaldent ha implementado un sistema de gestión de la información basado en la nube de Microsoft, llamado Proyecto Apolo, con el objetivo de optimizar sus procesos y mejorar la toma de decisiones. Este sistema integra diferentes herramientas:

- **Dynamics 365 Finance & Operations:** Permite automatizar y modernizar las operaciones financieras, supervisar el rendimiento en tiempo real y realizar estimaciones a futuro.
- **Dynamics 365 Customer Engagement:** Personaliza la atención al cliente y facilita la comunicación entre las clínicas y los pacientes.
- **Microsoft Teams:** Mejora la comunicación interna y la colaboración entre los diferentes equipos y clínicas.

1.3 FICHEROS OBJETO DE LA AUDITORÍA

1.3.1 Clasificación de los ficheros

1.3.1.1 Fichero de datos de pacientes

Fichero: PACIENTES.
Tratamientos: GESTIÓN DE PACIENTES.
Ubicación Principal: BASE DE DATOS DE LA APLICACIÓN VITALDENT.
Finalidad: ALMACENAMIENTO DE DATOS PERSONALES, INFORMACIÓN CLÍNICA BÁSICA Y DATOS BANCARIOS DE LOS PACIENTES.
Medidas de Seguridad: ALTO.
Contenido: DNI, NOMBRE, APELLIDOS, DIRECCIÓN, FECHA DE NACIMIENTO, TELÉFONO, EMAIL, HISTORIAL CLÍNICO, DATOS BANCARIOS.

Tabla 3

1.3.1.2 Fichero de empleados

Fichero: LABORAL.
Tratamientos: GESTIÓN DEL PERSONAL.
Ubicación Principal: BASE DE DATOS DE LA APLICACIÓN VITALDENT.
Finalidad: ALMACENAMIENTO DE DATOS PERSONALES Y REGISTROS RELACIONADOS CON EL PERSONAL EMPLEADO EN LA CLÍNICA DENTAL.
Medidas de Seguridad: MEDIO.
Contenido: DNI, NOMBRE, APELLIDOS, DIRECCIÓN, FECHA DE NACIMIENTO, TELÉFONO, EMAIL, INFORMACIÓN LABORAL (PUESTO, SALARIO, HORARIO), DATOS BANCARIOS (PARA EL PAGO DE NÓMINAS).

Tabla 4

1.3.1.3 Fichero de citas de pacientes

Fichero: CITAS PACIENTES.
Tratamientos: GESTIÓN DE PACIENTES.
Ubicación Principal: BASE DE DATOS DE LA APLICACIÓN VITALDENT.
Finalidad: REGISTRO Y GESTIÓN DE CITAS DE LOS PACIENTES EN LA CLÍNICA DENTAL.
Medidas de Seguridad: ALTO.
Contenido: DNI, FECHA Y HORA DE LA CITA, TIPO DE CITA, INFORMACIÓN SOBRE EL TRATAMIENTO.

Tabla 5

1.3.1.4 Fichero físico de empleados (registros físicos y fichas de contacto)

Fichero: RECURSOS HUMANOS.
Tratamientos: GESTIÓN DEL PERSONAL.
Ubicación Principal: ARCHIVO FÍSICO, GUARDADOS EN UN ARMARIO BAJO LLAVE EN LAS INSTALACIONES DE LA CLÍNICA DENTAL.
Finalidad: ALMACENAMIENTO DE REGISTROS FÍSICOS Y FICHAS DE CONTACTO DEL PERSONAL EMPLEADO EN LA CLÍNICA DENTAL.
Medidas de Seguridad: BÁSICO.
Contenido: FICHAS DE CONTACTO CON DNI, NOMBRE, APELLIDOS, DIRECCIÓN, TELÉFONO, EMAIL.

Tabla 6

1.3.2 Lista de distribución

Este informe de auditoría debe ser entregado a las siguientes personas pertenecientes a la organización del Responsable del fichero.

NOMBRE Y APELLIDOS	CARGO Y DEPARTAMENTO
JOSE ANTONIO GARCÍA PÉREZ	DTO ADMINISTRACIÓN

Tabla 7

1.3.3 Solicitud de inscripción del fichero en la AEPD

Tal y como se describe en la web de la AEPD, desde el 25 de mayo de 2018 se sustituye la necesidad de inscribir ficheros por la elaboración de un registro de actividades de tratamiento que deberá contener la información señalada en el artículo 30 del citado Reglamento [2].
Dicho registro deberá contener la siguiente información:

- Nombre y datos de contacto del responsable y del delegado de protección de datos.
- Finalidad del tratamiento.
- Descripción de las categorías de interesados y de las categorías de datos personales.
- Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- ~~(N/A). En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo2, la documentación de garantías adecuadas.~~
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

De esta manera, se plantea el siguiente registro (teniendo en cuenta que datos como el responsable y delegado del tratamiento ya han sido mencionados anteriormente, concretamente en las secciones 1.1.4 y 1.1.5).

1.3.3.1 Pacientes

ACTIVIDAD	GESTION DE PACIENTES
FINALIDAD	ALMACENAR LO RELATIVO A LOS PACIENTES, COMO DATOS PERSONALES O SU HISTORIAL CLÍNICO, ENTRE OTROS.
INTERESADOS	PACIENTES, VITALDENT
CATEGORÍA	DATOS IDENTIFICATIVOS
PLAZO CONSERVACIÓN	5 AÑOS (desde la última vez que el paciente acudió a la clínica)

Tabla 8

1.3.3.2 Empleados

ACTIVIDAD	GESTION DE EMPLEADOS
FINALIDAD	ALMACENAR LO RELATIVO A LOS EMPLEADOS, COMO DATOS PERSONALES O BANCARIOS.
INTERESADOS	EMPLEADOS, VITALDENTR
CATEGORÍA	DATOS IDENTIFICATIVOS
PLAZO CONSERVACIÓN	2 AÑOS / INDEFINIDO (siempre y cuando siga trabajando en la empresa)

Tabla 9

1.3.3.3 Citas de pacientes

ACTIVIDAD	GESTION DE PACIENTES
FINALIDAD	ALMACENAR LO RELATIVO A LAS CITAS DE LOS PACIENTES, COMO ASOCIACION CON EL PACIENTE, DOCTOR ENCARGADO DE LA CITA, FECHA Y HORA, ETC.
INTERESADOS	PACIENTES, VITALDENT
CATEGORÍA	DATOS IDENTIFICATIVOS
PLAZO CONSERVACIÓN	5 AÑOS (desde la última vez que el paciente acudió a la clínica)

Tabla 10

1.3.3.4 Empleados (físico)

Idéntico a lo visto en 0, se incluye por adjuntarlo al registro solicitado.

1.4 SUGERENCIA DE DECLARACIÓN DE FICHEROS DE DATOS

De acuerdo con la Ley Orgánica de Protección de Datos de Carácter Personal es obligatoria la declaración de todos aquellos ficheros que contengan datos de carácter personal; en caso de que estos ficheros no estén automatizados no se permitirá la declaración de los mismo.
Por lo tanto, de los ficheros anteriormente mencionados deberán declararse los ficheros de pacientes, los de citas de pacientes y los de empleados que estén en la base de datos de la aplicación Vitaldent.

1.5 DICTAMEN SOBRE LA ADECUACIÓN DE LAS MEDIDAS Y CONTROLES DEL RMS

1.5.1 Aspectos generales

Aspecto	Definición	Artículo Correspondiente	Verificación del Cumplimiento	Medidas Correctoras	Medidas Complementarias de Mejora
Seguridad del Tratamiento	Conjunto de medidas técnicas y organizativas para proteger los datos personales.	Art. 32 RGPD, Art. 89 LOPDGDD, Cap. II RMS	Se menciona la adopción de medidas de seguridad, pero sin especificar.	Detallar las medidas de seguridad implementadas (cifrado, control de acceso, etc.).	Realizar auditorías de seguridad periódicas.
Evaluación de Impacto	Análisis de los riesgos para los derechos y libertades de las personas derivados del tratamiento de datos.	Art. 35 RGPD	No se menciona la realización de evaluaciones de impacto.	Realizar evaluaciones de impacto para tratamientos de alto riesgo.	Establecer un procedimiento para la realización de evaluaciones de impacto.
Transferencias Internacionales	Envío de datos personales a países fuera del Espacio Económico Europeo.	Art. 44 y ss. RGPD	No se especifica si se realizan transferencias internacionales.	Informar sobre las transferencias internacionales y las garantías aplicadas.	Utilizar mecanismos de transferencia adecuados (cláusulas contractuales tipo, etc.).
Información a los Interesados	Comunicación clara y transparente sobre el tratamiento de datos.	Art. 13 y 14 RGPD	La política de privacidad informa sobre los aspectos básicos del tratamiento.	Mejorar la información sobre las medidas de seguridad, evaluaciones de impacto y transferencias internacionales.	Revisar y actualizar periódicamente la política de privacidad.
Registro de Actividades de Tratamiento	Documento que recoge los detalles de las actividades de tratamiento realizadas.	Art. 30 RGPD	No se menciona la existencia de un registro de actividades.	Elaborar y mantener un registro de actividades de tratamiento actualizado.	Implementar un sistema de gestión de registros.

Tabla 11

1.5.2 Documento de seguridad

1.5.2.1 Definición

El Documento de Seguridad es un compendio de políticas, procedimientos y medidas técnicas y organizativas destinadas a proteger los datos personales gestionados por Vitaldent, asegurando el cumplimiento de las normativas vigentes en materia de protección de datos, específicamente el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos (LOPD). Este documento se revisa y actualiza periódicamente para garantizar su eficacia y adecuación a los cambios legislativos y tecnológicos.

1.5.2.2 Articulo correspondiente

Artículo 88. El documento de seguridad

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.
2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.
3. El documento deberá contener, como mínimo, los siguientes aspectos:
   a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
   b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
   c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
   d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
   e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
   f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
   g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.
4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:
   a) La identificación del responsable o responsables de seguridad.
   b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.
5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.
6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.
En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.
7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Tabla 12

1.5.2.3 Verificación del cumplimiento

Se ha constatado la existencia del Documento de Seguridad en Vitaldent y su alineación con los requerimientos del artículo 32 del RGPD. Además, se ha verificado el cumplimiento de los apartados recogidos en el artículo 88 del R.D 1720/2007:

- **Elaboración del documento:** El responsable del tratamiento ha elaborado el Documento de Seguridad, detallando todas las medidas técnicas y organizativas implementadas.
- **Actualización y revisión:** El documento se actualiza y revisa cada 6 meses. En caso de cambios significativos en los términos, se convoca una reunión del comité técnico de responsabilidad en materia de seguridad para realizar las actualizaciones pertinentes.

1.5.2.4 Medidas correctoras

Aunque la auditoría mostró un alto nivel de cumplimiento, se han implementado las siguientes medidas correctoras para abordar áreas menores de mejora:

- **Control de acceso y autenticación:** Mejoras en los procedimientos, incluyendo la implementación de autenticación multifactor.
- **Ciberseguridad:** Refuerzo de las capacidades mediante la actualización del software de seguridad y la introducción de sistemas de detección de intrusiones.
- **Capacitación:** Realización de sesiones de capacitación adicionales sobre nuevas amenazas y mejores prácticas en protección de datos.

1.5.2.5 Medidas complementarias de mejora

Para fortalecer aún más la protección de los datos personales y alinearse con las mejores prácticas del sector, se han implementado medidas complementarias:

- **Tecnologías avanzadas:** Implementación de inteligencia artificial para detectar amenazas en tiempo real y sistemas de respuesta automática.
- **Cultura organizativa:** Fomento de una cultura centrada en la protección de datos y ciberseguridad, incluyendo campañas de concienciación y formación continua.
- **Evaluaciones de impacto:** Realización de Evaluaciones de Impacto en la Protección de Datos (DPIA) para todos los nuevos proyectos y cambios significativos en el tratamiento de datos.

1.5.3 Encargado de tratamiento

1.5.3.1 Definición

Las normas en las que se establecen las responsabilidades del encargado del tratamiento se encuentran en el artículo 82 del capítulo II del título VIII del Real Decreto 1720/2007. Sobre este artículo se analizarán las responsabilidades del responsable y el cumplimiento de estas.

1.5.3.2 Articulo correspondiente

Artículo 82. Encargado del tratamiento.
1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento. Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento. 2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento. 3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento

Tabla 13

1.5.3.3 Verificación del cumplimiento

El responsable del tratamiento se trata en este caso de Donte Group S.L.U los cuales son responsables de la marca Vitaldent, en concreto, de un equipo responsable dentro de la propia empresa. Este equipo solo puede acceder a los ficheros mediante los equipos del propio local de la empresa.

También se ha constatado que no existe un documento de seguridad de los procesos que debe seguir el encargado de seguridad para tratar y sacar los ficheros de la compañía ya que esto no se contempla.

1.5.3.4 Medidas correctoras

Debería crearse un documento de seguridad para el trato de los datos personales por parte del responsable del fichero. En este se deberán recoger las medidas de seguridad pertinentes al artículo 9 para dejar constancia de su cumplimiento, aunque estas se estén cumpliendo en la actualidad.

1.5.3.5 Medidas complementarias de mejora

Aunque no sea una actividad normal en la empresa, incluir en el documento de seguridad los procesos para sacar y analizar ficheros fuera de la empresa en caso de que sea necesario sin incurrir en perdida de datos o vulneración de datos delicados.

1.5.4 Prestaciones de servicios sin acceso a datos personales

1.5.4.1 Definición

Las prestaciones de servicios sin acceso a datos personales se refieren a aquellas actividades en las que una empresa o entidad proporciona un servicio sin recopilar, procesar o almacenar datos personales de los usuarios. Esto significa que la empresa no tiene acceso a información que

pueda identificar directa o indirectamente a una persona, como nombres, direcciones de correo electrónico, números de teléfono, datos de ubicación, etc.
Cabe destacar que la política de privacidad no menciona explícitamente sobre las prestaciones de servicios sin acceso a datos personales. Sin embargo, basándonos en los puntos que sí se mencionan, podemos obtener información relativa a este apartado.

1.5.4.2 Artículo correspondiente

Artículo 83. Prestaciones de servicios sin acceso a datos personales
El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales. Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Tabla 14

1.5.4.3 Verificación del cumplimiento

No se puede verificar que se cumpla lo especificado en el artículo anterior porque no existe ninguna documentación relativa a las prestaciones de servicios sin acceso a datos personales, sin embargo, se comenta que no se ofrecen servicios sin el tratamiento de los datos personales

1.5.4.4 Medidas correctoras

Se debe realizar un plan para las prestaciones de servicios sin acceso a datos personales, aunque no se realicen operaciones sin uso de datos personales

1.5.4.5 Medidas complementarias de mejora

No existen

1.5.5 Delegación de autorizaciones

1.5.5.1 Definición

La Delegación de Autorizaciones se refiere al proceso mediante el cual el responsable del fichero o tratamiento puede delegar ciertas autorizaciones en otras personas designadas al efecto. Este proceso debe estar claramente documentado en el Documento de Seguridad, especificando tanto las personas habilitadas para otorgar estas autorizaciones como aquellas en las que recae la delegación. Es importante destacar que esta delegación de autorizaciones no implica una transferencia de la responsabilidad que sigue correspondiendo al responsable del fichero.

1.5.5.2 Articulo correspondiente

Artículo 84. Delegación de autorizaciones.
Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Tabla 15

1.5.5.3 Verificación del cumplimiento

El responsable de seguridad designado desempeña una variedad de funciones, incluyendo la gestión y supervisión de los protocolos de seguridad relacionados con la protección de datos de los pacientes, el control de acceso a áreas restringidas y la coordinación de medidas de emergencia.

1.5.5.4 Medidas correctoras

No existen.

1.5.5.5 Medidas complementarias de mejora

No existen por el momento, sin embargo se recuerda la necesidad de en caso de ampliar la plantilla en cuanto a la delegación se refiere se requiere documentarlo en el documento de seguridad de acuerdo con lo visto en el artículo 84 en 1.5.5.2.

1.5.6 Régimen de trabajo fuera de los locales de la ubicación del fichero

1.5.6.1 Definición

Es posible que los datos de carácter delicado sean copiados u extraídos para su tratamiento y análisis fuera del local. Las medidas de seguridad necesarias para su correcta realización se encuentran en el artículo 86.

1.5.6.2 Articulo correspondiente

Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado. 2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Tabla 16

1.5.6.3 Verificación del cumplimiento

No se permite la realización de copias ni la extracción de ficheros de carácter delicado fuera del local donde se tratan los datos.

1.5.6.4 Medidas correctoras

Se debería asegurar de que, aunque no se realicen copias de los ficheros de carácter delicado no puedan realizarse mediante un USB u otro método sin autorización previa aunque sea el propio equipo de tratado de datos.

1.5.6.5 Medidas complementarias de mejora

No existen.

1.5.7 Funciones y obligaciones del personal

1.5.7.1 Definición

El personal que maneja datos personales bajo el RGPD debe conocer y aplicar el reglamento, tratando los datos de forma lícita, leal y transparente, minimizando su uso, garantizando su exactitud y actualización, limitando su conservación, y asegurando su integridad y confidencialidad. Deben informar al responsable de cualquier incidencia, mantener la confidencialidad, recibir formación periódica, cumplir las instrucciones del responsable y colaborar con las autoridades de control. El incumplimiento puede acarrear sanciones, por lo que es crucial actuar responsablemente en la protección de datos.

1.5.7.2 Articulo correspondiente

Artículo 89. Funciones y obligaciones del personal
Funciones y obligaciones claras: El documento de seguridad detallará las funciones y responsabilidades específicas de cada usuario o perfil de usuario que tenga acceso a datos personales y sistemas de información. Esto incluye las autorizaciones delegadas por el responsable del fichero o tratamiento. **Conocimiento de las normas de seguridad:** El responsable del fichero o tratamiento se asegurará de que el personal comprenda las normas de seguridad relevantes para sus funciones, así como las posibles consecuencias de no cumplir con dichas normas.

Tabla 17

1.5.7.3 Verificación del cumplimiento

Tras la realización de la entrevista/reunión con el responsable de seguridad se pudo observar como el plan de funciones y obligaciones del personal es inexistente.

1.5.7.4 Medidas correctoras

Crear el documento de seguridad que contendrá una descripción detallada y exhaustiva de las funciones que desempeñará cada empleado en relación con el tratamiento de datos personales, incluyendo al encargado y al responsable del tratamiento. Esta descripción deberá ser redactada de forma clara y comprensible para todos los empleados, garantizando su accesibilidad en cualquier momento.

1.5.7.5 Medidas complementarias de mejora

No existen.

1.5.8 Registro de incidencias

1.5.8.1 Definición

El Registro de Incidencias es un sistema documentado utilizado para registrar y gestionar todas las incidencias que afecten a los datos de carácter personal dentro de la organización. Este registro incluye información detallada sobre el tipo de incidencia, el momento en que ocurrió o fue detectada, quién realizó la notificación, a quién se comunicó, los efectos resultantes y las medidas correctoras aplicadas para abordar la incidencia.

1.5.8.2 Articulo correspondiente

Artículo 90. Registro de incidencias.
Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Tabla 18

1.5.8.3 Verificación del cumplimiento

Tras la realización de la entrevista/reunión con el responsable de seguridad se pudo observar como el registro de incidencias era escaso sino inexistente, registrando lo mínimo tras detectarse una incidencia que afectase al ámbito de la seguridad de los datos, entendiendo lo mínimo como la fecha y una breve descripción de lo que fue esta incidencia.

1.5.8.4 Medidas correctoras

Tras la reunión se ha acordado una especie de plantilla para llevar a cabo el registro de incidencias, de esta forma:

IDENTIFICADOR	TITULO DESCRIPTIVO
BREVE DESCRIPCIÓN	
FECHA Y HORA EN LA QUE SE PRODUJO	FECHA Y HORA EN LA QUE FUE DETECTADA
PERSONA QUE LA DETECTÓ	PERSONA A LA QUE SE COMUNICÓ
EFECTOS CAUSADOS	
MEDIDAS CORRECTORAS APLICADAS	

Tabla 19

1.5.8.5 Medidas complementarias de mejora

Como medida predictiva de una posible caída del servidor donde se guardase este registro, se ha recomendado imprimir en físico un registro de las incidencias producidas cada 6 meses, en caso de que esto fuera necesario para un control futuro.

1.5.9 Control de acceso

1.5.9.1 Definición

Se debe mantener un control de acceso en cuanto a los datos de carácter personal para evitar la vulneración o perdida de estos. En este caso los artículos 85 y 91 determinan las medidas de seguridad necesarias.

1.5.9.2 Articulo correspondiente

Artículo 85. Acceso a datos a través de redes de comunicaciones.
Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.
Artículo 91. Control de acceso
1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. 2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. 3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. 4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero. 5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Tabla 20

1.5.9.3 Verificación del cumplimiento

La base de datos de la aplicación de Vitaldent solo puede ser accedida por el equipo de tratamiento de datos mediante una clave digital que identifica al personal. Esta base de datos está encriptada por lo que no existe otro modo de acceso.

Los ficheros físicos están guardados en un armario bajo llave localizado en la misma sala donde trabaja el equipo de tratamiento de datos de forma que nadie más pueda acceder a este.

1.5.9.4 Medidas correctoras

Los ficheros en físico deberían guardarse en una sala separada y bajo llave de donde trabaja el equipo de tratamiento de datos para mayor seguridad como recomiendo la RGPD.

1.5.9.5 Medidas complementarias de mejora

No existen.

1.5.10 Gestión de soportes y documentos

1.5.10.1 Definición

Los soportes y documentos deberán ser gestionados según lo indicado en el Artículo 92 del RGPD.

1.5.10.2 Articulo correspondiente

Artículo 92. Gestión de soportes y documentos
1. Identificación, inventario y acceso restringido: Los soportes y documentos con datos personales deben ser fácilmente identificables y estar inventariados. Su acceso debe limitarse al personal autorizado, según el documento de seguridad. 2. Excepciones justificadas: En casos donde las características físicas del soporte impidan cumplir con la identificación y el inventario, estas obligaciones pueden omitirse, siempre que se justifique en el documento de seguridad. **1.** 3. Autorización para salida de soportes: La salida de soportes y documentos con datos personales, incluyendo adjuntos en correos electrónicos, fuera de las instalaciones del responsable requiere autorización expresa o estar debidamente autorizada en el documento de seguridad. 4. Precauciones en el traslado y destrucción segura: Durante el traslado de documentos, se deben tomar medidas para evitar robos, pérdidas o accesos no autorizados. Antes de desecharlos, se debe asegurar su destrucción o borrado seguro para impedir el acceso o recuperación de la información. 5. Etiquetado para datos sensibles: Los soportes con datos especialmente sensibles pueden identificarse mediante sistemas de etiquetado claros para el personal autorizado, dificultando la identificación para personas no autorizadas.

Tabla 21

1.5.10.3 Verificación del cumplimiento

Para acceder a la base de datos alojada en el servidor, es imprescindible contar con una contraseña. Esta contraseña se modifica de forma regular por motivos de seguridad, lo que garantiza la protección de la información contenida en la base de datos.

1.5.10.4 Medidas correctoras

Es fundamental implementar medidas de protección en los documentos y archivos almacenados en los ordenadores de los empleados, dado que actualmente carecen de cualquier tipo de seguridad. Esto incluye el uso de contraseñas robustas, cifrado de datos y permisos de acceso restringidos para garantizar la confidencialidad de la información. Además, la nomenclatura de los archivos debe seguir un sistema que incorpore códigos o palabras clave que faciliten la identificación del contenido a los usuarios autorizados, sin revelar explícitamente dicho contenido, dificultando así la comprensión del contenido a personas ajenas a la organización.

1.5.10.5 Medidas complementarias de mejora

No existen.

1.5.11 Identificación y autenticación

1.5.11.1 Definición

La Identificación y Autenticación se refiere al conjunto de medidas y procedimientos implementados para garantizar que los usuarios que acceden al sistema de información estén correctamente identificados y autenticados de manera segura. Esto incluye la asignación de identificadores únicos a cada usuario y la implementación de mecanismos de autenticación adecuados para verificar su identidad de manera inequívoca.

1.5.11.2 Articulo correspondiente

Artículo 93. Identificación y autenticación.
1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. 2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. 3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. 4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Tabla 22

1.5.11.3 Verificación del cumplimiento

La verificación del cumplimiento revela que Vitaldent tiene procedimientos establecidos para la identificación y autenticación de usuarios, incluyendo la asignación de identificadores únicos y mecanismos de autenticación. Sin embargo, se identificaron algunas deficiencias en la implementación y gestión de contraseñas, así como en la periodicidad del cambio de estas.

1.5.11.4 Medidas correctoras

Para abordar las deficiencias identificadas, se proponen las siguientes medidas correctoras:

- **Revisión y Actualización del procedimiento de cifrado:** Se debe actualizar el cifrado de los datos de los pacientes con el uso de los últimos algoritmos de cifrado según las mejores prácticas, como puede ser *AES-256*.
- **Implementación de Políticas de Cambio de Contraseñas:** Se deben establecer políticas claras y periódicas para el cambio de contraseñas, con una frecuencia no superior a un año, y asegurar que se almacenen de forma ininteligible mientras estén vigentes.

1.5.11.5 Medidas complementarias de mejora

Como medidas extra para garantizar el correcto cumplimiento, se sugirió la implementación de un sistema de autenticación multifactorial como puede ser mediante los autenticadores de Google o Microsoft, así como una monitorización periódica de los intentos de acceso (algo que también afectaría al registro de incidencias visto en el apartado 0).

1.5.12 Copias de respaldo y recuperación

1.5.12.1 Definición

Se deben realizar copias de seguridad de la base de datos en caso de pérdida o destrucción parcial o total de los datos de carácter personal guardados en las mismas. Esto se encuentra en el artículo 94.

1.5.12.2 Articulo correspondiente

Artículo 94. Copias de respaldo y recuperación
1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. 2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad. 3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. 4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Tabla 23

1.5.12.3 Verificación del cumplimiento

Las copias de seguridad de la base de datos de la aplicación de Vitaldent se realizan cada viernes de forma automatizada. No hay evidencia de que se realice una comprobación de las copias de seguridad cada seis meses solo que el sistema siga funcionando sin consultar si la copia se ha realizado correctamente y no está corrompida.

1.5.12.4 Medidas correctoras

Crear un protocolo y nombrar a un empleado encargado de realizar la comprobación de las copias de seguridad cada seis meses.

1.5.12.5 Medidas complementarias de mejora

No existen.

1.5.13 Registro de accesos

1.5.13.1 Definición

El Registro de Accesos es un sistema que documenta cada intento de acceso a los datos personales dentro de la organización, registrando la identificación del usuario, la fecha y hora del acceso, el fichero accedido, el tipo de acceso y si fue autorizado o denegado. Este registro es crucial para garantizar la trazabilidad y seguridad de los datos personales.

1.5.13.2 Articulo correspondiente

Artículo 103. Registros de acceso.
1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. 2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. 3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. 4. El período mínimo de conservación de los datos registrados será de dos años. 5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados. 6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias: a) Que el responsable del fichero o del tratamiento sea una persona física. b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales. La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Tabla 24

1.5.13.3 Verificación del cumplimiento

Se mantiene un registro de acceso a los datos tanto físicos como a la base de datos

1.5.13.4 Medidas correctoras

No existen.

1.5.13.5 Medidas complementarias de mejora

No existen.

1.5.14 Criterios de archivo

1.5.14.1 Definición

Los Criterios de Archivo se refieren a los principios y normativas que guían el proceso de archivo de soportes o documentos relacionados con el tratamiento de datos personales. Esto incluye la conservación adecuada de los documentos, la facilidad de localización y consulta de la información, así como la garantía de los derechos de los individuos sobre sus datos.

1.5.14.2 Articulo correspondiente

Artículo 106. Criterios de archivo.
El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Tabla 25

1.5.14.3 Verificación del cumplimiento

Tras la entrevista con el responsable de seguridad se revela que Vitaldent sigue los criterios de archivo establecidos en la legislación aplicable y en sus propios procedimientos internos, de esta forma, los documentos se archivan de manera adecuada, facilitando su conservación y consulta, y se garantiza el ejercicio de los derechos de los individuos sobre sus datos.

1.5.14.4 Medidas correctoras

No existen.

1.5.14.5 Medidas complementarias de mejora

No existen realmente, aunque podría considerarse recomendable un proceso de formación periódico a los empleados, sobre todo cuando se produzcan cambios en la legislación vigente que puedan influenciar en este proceso.

1.5.15 Almacenamiento de la información

1.5.15.1 Definición

Es necesario mantener un nivel de seguridad adecuado para los archivos físicos de forma que solo sean accesibles para el personal autorizado. Esto se contempla en el artículo 107.

1.5.15.2 Articulo correspondiente

Artículo 107. Dispositivos de almacenamiento
Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Tabla 26

1.5.15.3 Verificación del cumplimiento

Los documentos físicos están contenidos en un cajón cerrado al cual solo tienen acceso el equipo de encargados del tratamiento mediante una llave. Nadie sin autorización puede abrir los mismos.

1.5.15.4 Medidas correctoras

No existen.

1.5.15.5 Medidas complementarias de mejora

Guardar el cajón en una habitación distinta a donde se tratan los datos y cerrar también la puerta al almacén bajo llave de ser posible.

1.5.16 Custodia de soportes

1.5.16.1 Definición

La custodia de soportes se refiere a la responsabilidad de proteger y preservar la integridad de los medios físicos o digitales que contienen información, garantizando su disponibilidad y evitando su pérdida, deterioro o acceso no autorizado.

1.5.16.2 Articulo correspondiente

Artículo 108. Custodia de soportes.
Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Tabla 27

1.5.16.3 Verificación del cumplimiento

No se especifica en ningún lugar como se trata con la custodia de soportes

1.5.16.4 Medidas correctoras

Realizar un plan para la custodia de soportes.

1.5.16.5 Medidas complementarias de mejora

No existen.

1.6 LUGAR DE TRABAJO

La auditoría se ha llevado a cabo en las instalaciones de la empresa **Donte Group S.L.U. (VITALDENT)**, ubicada en *Calle San Bernabé, 15, 33002 Oviedo, Asturias*, con fecha del *martes, 21 de mayo de 2024*.

Este proceso se ha desarrollado mediante el uso de entrevistas con la plantilla, una revisión exhaustiva de documentos y por último, un análisis de los procedimientos actuales de la empresa relacionados con el tratamiento y la seguridad de los datos.

1.7 DOCUMENTACIÓN ENTREGADA

TITULO DEL DOCUMENTO	ORIGINAL O COPIA	BREVE REFERENCIA DEL CONTENIDO
DOCUMENTO DE SEGURIDAD	COPIA	DETALLA LAS MEDIDAS DE SEGURIDAD ADOPTADAS PARA EL TRATAMIENTO DE DATOS PERSONALES.
COMPROMISO DE CONFIDENCIALIDAD	COPIA	ESTABLECE EL COMPROMISO DE CONFIDENCIALIDAD DE LA EMPRESA CON RESPECTO A LOS DATOS PERSONALES.
LISTADO DE EMPLEADOS	COPIA	LISTADO DE LOS EMPLEADOS CON UNA RECOPILACIÓN DE LOS DATOS DE ÉSTOS.
COMUNICADO INTERNO	COPIA	DOCUMENTO UTILIZADO PARA LA COMUNICACIÓN DE LAS FUNCIONES Y OBLIGACIONES RELATIVAS A LA LOPD.
REGISTRO DE FORMACIÓN	ORIGINAL	DOCUMENTO DONDE SE REGISTRA LA FORMACIÓN RELATIVA A LA LOPD DADA AL PERSONAL DE VITALDENT EN EL MOMENTO DE ACCESO AL EMPLEO.

Tabla 28

1.8 CONCLUSIÓN

Después de llevar a cabo la auditoría en las instalaciones de **Donte Group S.L.U. (VITALDENT)** ubicadas en Oviedo, Asturias, el martes 21 de mayo de 2024, se ha obtenido una visión integral de los procedimientos relacionados con el tratamiento y la seguridad de los datos. Mediante entrevistas con el personal, revisión exhaustiva de documentos y análisis de los procesos actuales, se ha evaluado el grado de cumplimiento con el Reglamento General de Protección de Datos (**RGPD**) y se han identificado áreas de mejora.

Se ha observado un buen nivel de cumplimiento en varios aspectos, como la identificación y autenticación de usuarios, el control de acceso, la gestión de soportes y documentos, y el almacenamiento de información. Además, se han establecido procedimientos adecuados para la delegación de autorizaciones y la custodia de soportes.

Sin embargo, se han identificado deficiencias y áreas de mejora en otros aspectos, como la falta de un plan de funciones y obligaciones del personal, la necesidad de mejorar el registro de incidencias y el control de cambios de contraseñas, y la ausencia de un plan para la custodia de soportes.

En resumen, aunque se han encontrado aspectos positivos en el cumplimiento de las normativas de protección de datos, existen áreas específicas que requieren atención y mejoras para garantizar un cumplimiento total y efectivo del RGPD. Es crucial que la empresa tome medidas correctivas y establezca procesos de mejora continua para garantizar la protección adecuada de los datos personales y el cumplimiento continuo de las regulaciones vigentes.

2 ANEXOS

2.1 BIBLIOGRAFÍA

[1] Unión Europea, *Reglamento General de Protección de Datos,* 2016.

[2] Agencia Española de Protección de Datos, «Inscripción de ficheros,» 2019. [En línea]. Available: https://www.aepd.es/inscripcion-de-ficheros. [Último acceso: 20 Mayo 2024].

[3] Donte Group S.L.U., «Vitaldent.com,» 20 05 2024. [En línea]. Available: https://www.vitaldent.com/es/. [Último acceso: 20 5 2024].