Universidad de Valladolid

E.T.S Ingeniería Informática

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

Aplicación y Guía de la L.O.P.D. en Clínica Dental

Autor:

D. David Martín Hernández

Tutor:

D. Pablo de la Fuente Redondo

1 Índice

Resumen

En este Trabajo Fin de grado se va a realizar una guía para implantación a un supuesto de una Clínica Dental. Se definirán unos supuestos de estructura que se utilizarán para que el desarrollo de la guía de implantación (Documento de Seguridad, Anexos con formatos necesarios y Documentación complementaria) que cubra las posibles necesidades para el cumplimiento de la LOPD.

El desarrollo de este trabajo se ha propuesto como forma de conocimiento sobre la LOPD para la generación de la documentación necesaria y guía para empresas en función de los posibles datos que vaya a tratar.

Introducción

Actualmente nos encontramos en un mundo digitalizado y global. La revolución tecnológica ha hecho que a través de los diferentes sistemas de información digital los datos circulen libremente por todo el mundo.

Estos datos pueden ser tomados a través de internet en una web, por medio de los datos recogidos en un formulario en papel que hemos rellenado, el TPV (Terminal Punto de Venta) en el que hemos realizado un pago en la tienda de toda la vida, en las cámaras de seguridad de los establecimientos por los que pasamos al dar un paseo… Y como estos ejemplos miles de casos en los que dejamos una información en manos de terceros.

Pero, ¿esos datos como se utilizan? ¿Conocemos el uso de la información que entregamos? ¿Se realiza algún control del tratamiento realizado?

¿Cómo se protege la información que entregamos o se obtiene de nuestra persona?

Es difícil de contestar, pues no podemos concretar el uso que se realiza de todos los datos que facilitamos.

Damos datos a través de las redes (Internet) en páginas de todo el mundo, y no existe una regulación global al respecto, si no que cada país tiene o no su propia regulación.

Para este cometido de regulación y control del tratamiento de los datos, en España se creó la Ley Orgánica de Protección de Datos, o comúnmente conocida por su acrónimo L.O.P.D.

¿Qué es la L.O.P.D?

La L.O.P.D. es la Ley Orgánica de Protección de Datos que regula la recogida, tratamiento y eliminación de los datos de carácter personal por parte de las empresas españolas. Se busca garantizar el uso correcto, la privacidad y derechos fundamentales de las personas físicas.

Es de obligatorio cumplimiento por parte de las empresas o personas que recaben información de carácter personal, y el incumplimiento de la misma conllevará sanciones.

La ley establece unas obligaciones por parte de las empresas:

- Adopción de todas las medidas de seguridad detalladas en la Ley
- Registro y notificación de los ficheros a la Agencia de Protección de Datos (APD)
- Desarrollo de un Documento de Seguridad y la actualización del mismo durante el tiempo en el que se desarrolle la actividad.
- Generar todos los documentos y contratos incluyéndoles las clausulas descritas por la LOPD

La ley determina las medidas a cumplir y divide los datos en niveles de seguridad (alto, medio y bajo) con el fin de determinar métodos a emplear en cada uno de los casos.

Al igual que los niveles las sanciones están clasificadas en tres niveles y que están tipificadas entre 900 y 600.000 € de sanción.

Historia de la LOPD

En España, previamente a la LOPD se aprobó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, o conocida como LORTAD, la cual detalla medidas sobre el uso de la informática para salvaguardar la intimidad de los usuarios.

La LORTAD tuvo su desarrollo reglamentario, con el Real Decreto 994/1999, de 11 de junio: Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal (RMS).

Pocos meses después se aprobó la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre (LOPD) y que amplia y desarrolla con mayor detalle el tratamiento completo de los datos de carácter personal, ya estén automatizados estos datos o en cualquier otro formato.

Por su lado la LOPD tuvo su desarrollo reglamentario en el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), que es la ley existente en la actualidad.

La LOPD en el mundo

En la actualidad nuestros datos de carácter personal pueden estar siendo tratados en otros países fuera de España, pues vivimos en un mundo totalmente globalizado.

La compra en una página web extranjera, o el alquiler de un coche en un viaje a otro país, son casos en los que nuestros datos han quedado en manos de empresas que no están obligadas a cumplir las leyes de protección de datos contempladas en la LOPD.

En cuanto al Unión Europea, se aseguran y se tratan los datos de forma correcta y adaptada a los estándares de la LOPD, pues la ley publicada en Europa Directiva 95/46/CE que entró en vigor en 1995 y que posteriormente se traspuso en 1998, es la base de la adaptación que se realizó en España dando por resultado la LOPD de 1999.

En este aspecto el resto de los países tienen sus diferentes regulaciones sobre esta protección, pero desde España únicamente a día de hoy se han declarado a los siguientes países como adecuados en cuanto a la protección de los datos de carácter personal:

Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda

Conllevando aun así, en la transferencia de datos con cualquiera de los países anteriores y en el EEE el cumplimiento de un contrato conforme a la LOPD.

Alcance del Proyecto

En este proyecto se va a realizar el Documento de Seguridad para una Clínica Dental, para el cumplimiento de la LOPD por parte de esta Clínica.

Se van a añadir complementariamente a este documento unas plantillas para el cumplimiento de cada una de las medidas indicadas en el documento, como hojas de registros, contratos, inventarios…

Para la realización de este proyecto se van a declarar unos supuestos sobre los que trabajar y que son totalmente ficticios y no hacen referencia a una Clínica real.

Supuestos

Para realizar un documento de seguridad de la LOPD de una clínica dental, vamos a especificar unos supuestos para poder acotar el desarrollo de ese documento.

- Se realizará sobre una empresa ficticia “Clínica Dental Sonrisa”.

- Las dos personas responsables se llamarán Juan y María.

- La empresa tendrá dos sedes en la ciudad (direcciones ficticias).

- Los dueños de la empresa son 2 personas que a la vez son odontólogos en la empresa.

- Estará formada por 6 empleados cada una de las clínicas, 12 en total. En cada clínica hay una recepcionista, dos odontólogos generales (uno de ellos en cada establecimiento es socio), un ortodontista, un auxiliar de odontología y un higienista-esterilización.

- Para cirugías maxilofaciales que no pueden realizar los odontólogos de la clínica, se trabaja con un cirujano y un anestesista externos que realizarán las cirugías maxilofaciales dos días a la semana.

- Todo el material que se utiliza en las clínicas es comprado al mismo proveedor “MercaDental”.

- La empresa tiene contratado con una empresa externa el servicio de limpieza fuera del horario de atención por la empresa “CleanWorks” la cual estima que esa limpieza se realiza por una persona en cada clínica.

- Existe una web para publicitarse y contacto por parte de los clientes con las clínicas. Y un buzón de correo electrónico.

- Tienen un software hecho a medida en el que almacenan los historiales clínicos de cada paciente y están conectadas entre las sedes para consultarlas desde cualquiera de las dos clínicas.

- Se contrató a una empresa para soporte a la red, web, software y BBDD bajo notificación de incidencia. Esta empresa creo el software y proporciona también la red, y el almacenamiento y dominio de la web y la BBDD del software. La empresa de soporte informático se llama “NetWorks”.

- En papel se obtiene el formulario inicial, con los datos personales y la contestación de las preguntas

respecto a la salud que se necesitan conocer previamente a cualquier tratamiento, con la firma de consentimiento y veracidad de esos datos. Y también quedarán en papel los diferentes consentimientos en los tratamientos que precisen de los mismos.

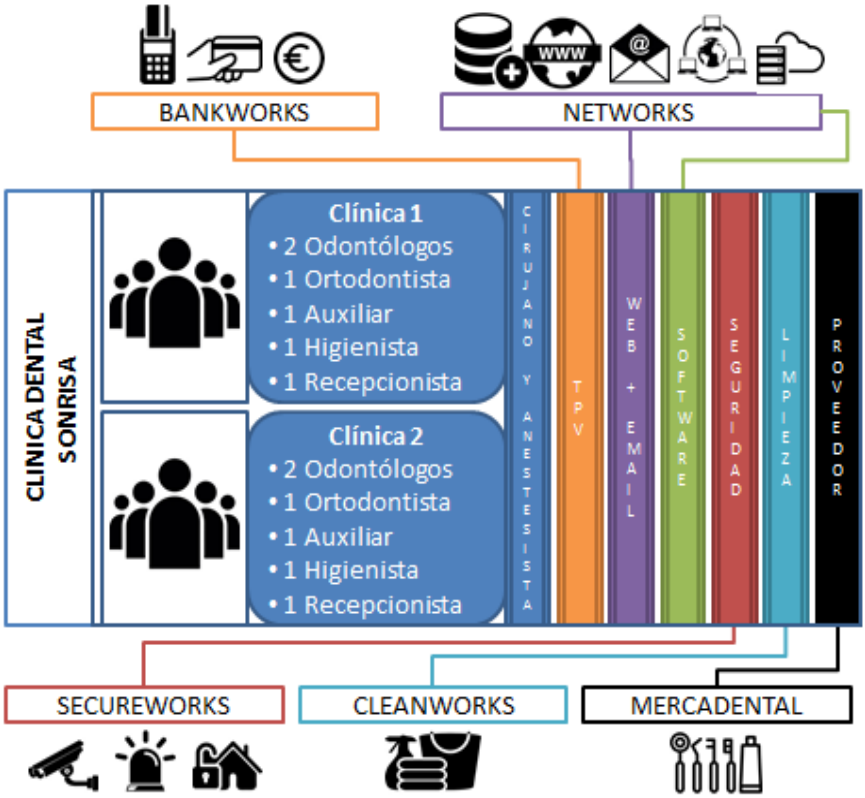
- Todos los documentos en papel comentados anteriormente se digitalizan a través de la impresora multifunción para dejarlo en el expediente digital del cliente.

- Se tiene un Terminal Punto de Venta contratado con "BankWorks" que permite el pago a través de Visa, Mastercard y American Express además del pago en efectivo.

- Se tiene alarma y cámaras de videovigilancia 24h en las clínicas, contratadas con una empresa de seguridad, "SecureWorks".

Arquitectura Clínica

Se presenta la arquitectura de la Clínica en el siguiente gráfico, en el que la parte interna esta en azul oscuro y en el resto de colores se indican los vínculos con agentes externos.



MANUAL DE IMPLEMENTACIÓN DE LA LOPD

Documento de Seguridad y Anexos

Documento de Seguridad

El Documento de Seguridad contendrá las normativas técnicas y organizativas para el cumplimiento de la LOPD en la Clínica.

El cumplimiento es obligatorio para todo el personal de la clínica que intervenga en el tratamiento de los datos de carácter personal. El responsable de la información debe informar y facilitar este documento para su posterior cumplimiento de todo lo detallado a todo el personal. Debe ser leído completo para que se tenga el conocimiento de todas las reglas o medidas que hay que cumplir.

Anexos

Anexo A. Relación de Ficheros

En este apartado se definirán los diferentes ficheros y su relación con la empresa. La empresa tendrá que solicitar a la AEPD que se envíe por correo postal el RGPD que habrá que indicar en este documento.

Anexo B. Estructura de Ficheros y/o Base de Datos

En este anexo se detallara la arquitectura de la Base de Datos (BBDD). Se deberá verificar por parte del responsable de esta información que esta actualizado.

También se generara en este anexo el Registro de Versiones del Documento de Seguridad.

Anexo C. Recursos Protegidos

Inventario Software: En este anexo se definirán los programas propios o externos. También se incluirá la web.

Inventario Hardware: Se detallaran los diferentes dispositivos hardware en el que se utilizarán los datos de carácter personal.

Inventario Documentos Físicos: Se inscribirán todos los archivadores y fichas que contienen la información de carácter personal.

Puestos de Trabajo: Describir los puestos de trabajo que existen en la empresa.

Anexo D. Organización de Empresa

Se describirá el organigrama, los diferentes perfiles que hay en la empresa y dispositivos que existen en la empresa.

Anexo E. Personal Autorizado

En este apartado se registrará a toda persona, ya sea interna o externa, que tenga acceso a los datos de carácter personal.

Personal interno:

- Nombre, apellidos
- DNI
- Puesto/rol
- Fecha de alta en la empresa
- Firma de cláusula de confidencialidad
- Información autorizada a acceder
- Tipología de permisos: Lectura, captura, modificación, borrado, copia…

- Tipología de acceso: Acceso físico, mediante algún soporte o SW, web…
- Autorización de salida de ficheros de las oficinas o dispositivos de la empresa.

Personal externo (Empresas ajenas y colaboradores):

- Nombre de empresa/Razón Social
- CIF
- Nivel de Seguridad de datos
- Firma contrato de tratamiento datos en base a LOPD
- Tipología de permisos: Lectura, captura, modificación, borrado, copia…
- Tipología de acceso: Acceso físico, mediante algún soporte o SW, remoto o en la oficina…

Anexo F. Gestión de Soportes

Se tendrá en este apartado las indicaciones para el registro de todos los soportes existentes durante la existencia de la información.

También se describirán los formularios de salida y entrada de soportes o información de nivel medio y/o alto.

Anexo G. Gestión de Incidencias

Se llevará un registro de todas las incidencias notificadas o descubiertas internamente, como la solución aplicada para solventarlas.

Anexo H. Derechos ARCO

En este anexo se facilitara el modelo a rellenar para solicitar los Derechos ARCO. Este modelo deberá estar disponible para su disposición por parte de los afectados a través de cualquier soporte.

Además de este formato la empresa podrá crear otros medios de solicitud siempre que sean gratuitos y fáciles.

Documentación Complementaria

Información a Clientes

Se expondrá un cartel informativo a los clientes en el que se informa que se aplica la LOPD en el tratamiento de sus datos de carácter personal en la empresa.

Pie de Página de Facturas y Documentos

Se detallará el pie de página a incluir en todas las facturas y documentos emitidos por la empresa para el cumplimiento de la LOPD

Información Web

La web informará del cumplimiento de la LOPD en el tratamiento de toda la información de carácter personal que introduzcan los usuarios en la web. Para ello se tendrá que aceptar de manera obligatoria antes del envío de la

información que se acepta y se conoce que la empresa utiliza la información bajo la LOPD.

Cláusula Genérica de Legitimación de Email

Se deberá añadir a todos los correos que salgan del dominio de la oficina o emails personales que se utilicen para fines laborales referentes a la clínica, un aviso legal donde se especificara el uso de los datos que se realizan por la empresa respetando la LOPD.

Documento de Recepción y Conocimiento LOPD

En este apartado toda persona interna o externa que tenga tratamiento con los datos de carácter personal deberá primeramente firmar un documento donde certifique que ha recibido y tiene el conocimiento del contenido del documento de seguridad facilitado por la empresa.

Videovigilancia

Si se tienen dispositivos de videovigilancia se deben registrar en la Agencia Española de Protección de Datos. Aunque el dispositivo no esté en uso, si se dispone de un equipo de videovigilancia se deberá exponer el cartel informativo que indicara el cumplimiento con la normativa de la LOPD y que se encuentra en el apartado de Documentación Complementaria “Videovigilancia”.

Y complementario al cartel se deberá tener un Modelo de Clausula Informativa a disposición de toda persona que la solicite que también está en el apartado Documentación Complementaria “Videovigilancia” del Documento de Seguridad.

DOCUMENTO DE SEGURIDAD

Índice

Normativa

2 Datos Generales

DATOS DE LA EMPRESA	
Razón Social	Clínica Dental Sonrisa
Dueño/s	Juan y María
Dirección Sede 1 Principal	Calle Ficticia 1, 47001, Valladolid
Dirección Sede 2	Calle Falsa 1, 47002, Valladolid
Correo Electrónico	email@email.com
Responsable Fichero	Juan y María

3 Introducción

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Reglamento de desarrollo de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, recogen las

medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

Este Documento deberá mantenerse permanente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial

4 Ámbito

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de “Clínica Dental Sonrisa”, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo

dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

NIVEL ALTO. Ficheros o tratamientos con datos:

- De ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico
- Recogidos con fines policiales sin consentimiento de las personas afectadas
- Derivados de actos de violencia de género

NIVEL MEDIO. Ficheros o tratamientos con datos:

- Relativos a la comisión de infracciones administrativas o penales
- Que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito)
- De Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias
- De entidades financieras para las finalidades relacionadas con la prestación de servicios financieros
- De Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias
- De mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social
- Que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas

- De los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización

NIVEL BÁSICO. Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros
- Se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero
- En los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de

invalidez, con motivo del cumplimiento de deberes públicos.

Cada uno de los ficheros que contengan datos de carácter personal deberá clasificarse y optar por las medidas necesarias en función del nivel de seguridad que requiera el contenido.

Cabe recordar que los niveles son acumulativos por lo que el nivel medio comprende a lo definido en medio y básico, y el nivel alto lo especificado en los tres niveles, alto, medio y básico.

5 Medidas, Normas, Procedimientos, Reglas y Estándares de Seguridad

5.1 Identificación y Autenticación de personal autorizado

Las personas autorizadas para el tratamiento de la información de carácter personal, deberá seguir ciertas normas de seguridad.

En el acceso a los dispositivos informáticos y otros soportes deberán contar con medidas de seguridad que no permitan a personas no autorizadas disponer de la información protegida.

5.1.1 Asignación y Mantenimiento de Contraseñas

Cada una de las personas autorizadas deberá tener una contraseña personal e intransferible para el acceso a la información protegida.

Para ello se definen las siguientes características en la elección de la contraseña y de su mantenimiento.

Longitud Contraseña: 8 caracteres

Obligaciones de caracteres: Al menos contendrá una mayúscula, una minúscula y un número.

Palabras a elegir: Evitar el uso de palabras de uso común, el año actual, el mes actual, fechas de cumpleaños, aniversarios..., nombres de familiares, parejas, amigos, mascotas, famosos…

Repetición: La contraseña no podrá coincidir en 6 caracteres y orden a las 10 contraseñas anteriores. Evitar secuencias entre las contraseñas (por ejemplo: Aerfg123, Aerfg456, Aerfg789…)

Cambio de contraseña: El sistema solicitara el cambio de contraseña cada 3 meses y avisará con 15 días de antelación de la caducidad de la contraseña actual realizando una cuenta regresiva.

Intentos de acceso: Se limitará el número de intentos de acceso a 5 errores seguidos, para evitar programas de fuerza bruta que buscan acceder de manera fraudulenta. En caso de bloquearse la contraseña,

deberá reportarlo al responsable del fichero o administrador del sistema.

Sesión activa: Se configuraran los sistemas para que tras 5 minutos de inactividad el sistema bloquee el acceso solamente a través de contraseña. Los usuarios deben de ser responsables de bloquear el sistema siempre que abandonen el puesto donde se encuentre el dispositivo. Si desconocen el procedimiento de bloqueo deberán preguntárselo al responsable del fichero o al administrador del sistema.

Cada persona con contraseña deberá ocuparse de salvaguardar que las contraseñas no sean de conocimiento de otras personas, no apuntarlas en lugares visibles y reportar al responsable del fichero o administrador del sistema la pérdida de la contraseña para modificar el acceso con la mayor brevedad.

5.1.2 Control de Acceso a la Información

Se deben configurar los diferentes dispositivos/soportes que contengan información protegida, de manera que cada usuario solo pueda acceder a la información a la que está autoriza y tener únicamente, en la medida de lo posible, los permisos para realizar las acciones sobre la información a la que fue autorizado.

Cualquier persona no autorizada deberá solicitar al responsable de la información y rellenar el formulario de alta de usuario para su identificación y autorización. Estas personas tienen que tener justificada la necesidad de acceso a la información y deben estar actualmente empleadas en la empresa o en colaboradores externos autorizados.

El software que contiene los datos de carácter personal o en fichas de registro físicos se guardará el acceso de cada persona que ha accedido (ID usuario, tipo de acceso, fichero accedido, fecha y hora, autorizado o denegado el acceso, fecha y hora de finalización de acceso)

Se deberá revisar por parte del Responsable de Seguridad los registros de acceso y generar un informe como se indica en el Anexo F de Gestión de Soportes

Todas las personas de colaboradores externos deberán cumplir toda la normativa igual que el personal propio de la empresa.

5.1.3 Alta y/o Baja de usuarios

Las altas y bajas de los usuarios deberán contener la metodología de acceso a los datos que estén autorizados a tratar, como definir en este formulario el tipo de acceso permitido. Adjuntado en el Anexo E.

5.2 Soportes y Puestos de Trabajo

Se detallaran siempre los soportes tanto físicos como automáticos, además de los puestos de trabajo de la empresa. Todos ellos están inventariados en el Anexo C.

5.2.1 Soportes

En este apartado se obliga a tener un inventario de los soportes, manuales o informatizados (tanto de software como de hardware).

Se deberán clasificar los soportes por la naturaleza de los mismos y los datos que contienen. Se deberán de proveer de las medidas de seguridad necesarias en función del nivel de seguridad de la información.

Todos los soportes deberán estar identificados a través del inventario y con un ID único, el cual debe constar en el soporte para poder identificarlo. Este identificador será relevante únicamente para las personas que puedan tener acceso al inventario, siendo para el resto de personas no autorizas una serie de números y/o letras que no tienen ningún sentido, con el fin de salvaguardar el contenido de los soportes.

5.2.2 Puestos de Trabajo

Se describirán los puestos de trabajo que comprenden a la empresa, indiferentemente del personal que ocupen esos puestos.

Las personas asignadas a los puestos de trabajo, son responsables de la información que esos puestos contienen y recogen. Deberán salvaguardar la información de personas no autorizadas y autorizar únicamente a las personas que necesiten el acceso a la información protegida.

5.3 Centros de Tratamiento y Almacenamiento de la Información

Se debe tener un control y medidas de seguridad necesarias en todos los centros de Tratamiento/Almacenamiento de los datos de carácter personal.

Cualquier extracción de la información fuera de estos centros deberá ser autorizado expresamente por el

responsable de la información y llevando un registro en todo momento de que uso, quien y donde se realiza el tratamiento de la información. Se deberá estipular el tiempo de validez de la autorización para la salida de la información de esos centros.

5.3.1 Salida de los ficheros fuera de los centros autorizados.

Cualquier salida de la información protegida de los centros autorizados donde se almacenan o tratan, deberá ser autorizada expresamente por el responsable de los ficheros.

Para este acuerdo se anexa un modelo de autorización para la salida de la información de dichos centros. Estas salidas deberán controlarse, al igual que el regreso de la información una vez finalizada la tarea que se autorizó para salir.

Este modelo estará en el Anexo F del documento como “Solicitud de Entrada/Salida Soportes”.

5.3.2 Traslado de Información Protegida

Hay que poner un especial énfasis en el cuidado de la información durante el traslado desde los centros autorizados a otros externos. Se deberán reportar inmediatamente cualquier eventualidad ocurrida durante el traslado, como pérdidas, robos o daños a la información.

5.4 Eliminación o borrado de soportes y documentos

Todo soporte o documento que se quiera eliminar deberá ser autorizado por el responsable de la información.

La eliminación de información informatizada deberá de realizarse de manera que no se pueda acceder nuevamente a la información desde el momento en el que se autoriza su eliminación. Por ello no basta con el borrado lógico que sigue dejando accesible el fichero hasta que se sobrescribe.

Respecto a los ficheros que se encuentren en un soporte físico deberán eliminarse por medio de la trituración o incineración de los mismos.

5.5 Ficheros Temporales o Copias de Documentos

La creación de ficheros temporales o la realización de copias de documentos serán autorizadas por el responsable de la información. Se deberá exponer el motivo de la realización del mismo, y una vez finalizada la tarea por la que se precisó la realización de estos ficheros temporales o copias deberán ser eliminados de manera adecuada como se expone en el punto anterior.

Durante toda la existencia de estos archivos se deberán cumplir las normas y reglas descritas en este documento como el resto de información de carácter personal.

5.6 Copias de Seguridad (Backups)

Deben regularse copias de seguridad de los datos informatizados. Estos respaldos deberán realizarse de manera periódica (se recomienda diaria) con al menos una copia semanal.

Si la información no ha sufrido ninguna modificación desde la última copia de seguridad, se puede no realizar el

respaldo. Estas copias de seguridad deberán de estar disponibles, y el responsable de la implantación del protocolo y la realización de las mismas tendrá que asegurarse que ante la necesidad de realizar una recuperación con estas copias, estas dejen el sistema en el mismo punto del momento de la realización del backup.

La realización deberá ser programada de manera automática, y no ser necesaria la intervención de ningún empleado. Se deberán realizar sobre soportes diferentes al que se encuentren los originales siempre que sea posible.

Si existe algún problema en la realización de estos respaldos, deberá de informarse a los responsables de la información, abrir una incidencia y describir las medidas adoptadas para la resolución.

5.6.1 Verificación de Copias de Seguridad

Se deberán realizar comprobaciones semestrales de funcionamiento de la realización de las copias de seguridad.

Se aconseja que la prueba se realice en un dispositivo diferente al que esta la información y si no, esta

comprobación se deberá realizar justo después de la última copia de seguridad realizada, para una vez comprobada la restauración de una copia aleatoria, se pueda volver al último punto del sistema sin perder ningún dato.

5.6.2 Almacenamiento de Copias de Seguridad

El almacenamiento de las copias realizadas deberá ser siempre un lugar protegido. Deberán de ponerse medidas de acceso a la información para evitar daños por pérdidas o accesos no autorizados.

Se registrará cada copia de seguridad en los anexos de Inventario de Soportes.

5.6.3 Eliminación de Copias de Seguridad

Las copias de seguridad deberán de ser eliminadas al igual que el resto de archivos con datos de carácter personal, y también ser autorizado por el responsable del fichero.

5.7 Gestión de Incidencias

5.7.1 Definición

Para la RLOPD una incidencia es “cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal”, en los diferentes ámbitos, como la integridad, confidencialidad y disponibilidad de la información protegida.

5.7.2 Procedimiento de notificación

Cualquier persona que trabaje con los datos que detecte una posible incidencia, deberá comunicar inmediatamente al responsable del fichero tal incidencia.

Este responsable deberá analizar el impacto e iniciar el proceso de resolución de la anomalía para eliminar o disminuir el posible daño.

5.7.3 Registro de la Incidencia

Una vez notificada, se deberá registrar la incidencia en el Inventario de Incidencias que se encuentra en el Anexo G.

En ella se incluirán el tipo de incidencia, fecha y hora en la que se detectó, persona responsable de la información, persona que da el aviso, posibles consecuencias, y finalmente cuando se resuelva se anotaran las medidas y soluciones aplicadas para la incidencia.

5.8 Revisión y Actualización del Documento de Seguridad

Durante la existencia de la empresa y por lo tanto del documento de seguridad, se deberá mantener este último siempre actualizado y con revisiones por parte de los responsables de la información.

Cualquier modificación, eliminación o añadido que se aplique al documento, deberá informarse a todos los empleados para que tengan conocimiento del mismo. Este

documento deberá estar siempre disponible para su consulta por parte de las personas que trabajan con los datos de carácter personal.

Esta responsabilidad de revisión y actualización se podrá delegar por parte del responsable del documento a otro empleado.

6 Obligaciones y Funciones del Personal

6.1 Carácter General

Todas las personas que tengan acceso, sin distinción entre personal interno o externo, están obligados al cumplimiento de todo lo redactado en este documento y a lo especificado en al RLOPD vigente en cada momento.

Se deberán reportar incidencias, pedir las autorizaciones correspondientes, registros de información de control, informar de cambios o modificaciones, protección de la información de carácter personal… de la misma manera que se detalla en el documento y en la ley.

6.2 Responsable del Fichero

Las personas que tengan el rol de Responsable del fichero, deberán desarrollar, implantar, revisar, actualizar y controlar las medidas a realizar para el cumplimiento de la ley.

El responsable del fichero es también el responsable jurídico de los daños causados por el no cumplimiento por parte de la empresa la ley de protección de datos.

Complementario a esto el responsable del fichero deberá designar a los responsables de seguridad de la información.

En este caso, se detallan los responsables del fichero en el apartado 1 del documento en Datos Generales.

6.3 Responsable de Seguridad

El responsable de Seguridad designado por el Responsable del fichero, deberá ocuparse del documento de seguridad en el que se recojan las medidas y normativa al respecto y que será de obligado cumplimiento por parte de todo el personal interno o externo mientras hagan algún tratamiento con los datos de carácter personal.

Será responsabilidad suya que el resto del personal tenga total conocimiento de todas las medidas y cualquier actualización en los procedimientos.

Todas las incidencias aun después de resueltas deberán de revisarse y crear métodos de contingencia para el futuro en caso de ser necesario.

Tendrá que aprobar o elegir a los administradores de los sistemas informáticos que deben aplicar la normativa en esos soportes.

Se deberá auditar interna o externamente el cumplimiento y correcto funcionamiento de los reglamentos definidos y su uso. Se deberán realizar las auditorías al menos cada dos años.

Será el responsable de la restauración de los datos desde los respaldos realizados.

La lista de autorizados deberá ser revisada periódicamente para verificar el correcto acceso a la información.

Satisfacer a los usuarios correctamente los derechos de Acceso, Rectificación, Cancelación y Oposición.

Ante cualquier mandato por parte de la AEPD el deberá de controlar el cumplimiento de esta indicación.

6.4 Administradores de Sistemas

Los Administradores del Sistema serán designados o contaran con la aprobación del Responsable de Seguridad.

Estos deberán cumplir con toda la normativa creada por el responsable de Seguridad sobre los sistemas que den acceso a datos de carácter personal.

Si se encuentra cualquier anomalía, deberán reportar la incidencia y aplicar si existiera en ese momento las medidas de contingencia necesarias.

Deberán mantener el control sobre las reglas de contraseñas o medidas de acceso a los sistemas informáticos para cumplir la normativa.

La realización de los respaldos de información (backups) será de su obligación y reportar cualquier problema en su realización o almacenamiento y seguridad.

6.5 Todo el personal (interno o externo)

Todas las personas (internas o externas) deberán cumplir con lo descrito en este documento y la normativa vigente siempre que se traten con datos de carácter personal. Todas estas personas tienen acceso al documento en cualquier momento que lo requieran.

Las personas autorizadas son las únicas que podrán acceder a la información protegida. Si se detecta un acceso no autorizado deberá ser notificado.

Cualquier persona deberá mantener la confidencialidad de la información aun después de abandonar la empresa.

Se tendrán que reportar cualquier tipo de incidencia que se detecte.

Se acataran todas las directrices y normativas de seguridad descritas en el documento que implemente la empresa.

Todos los soportes y la información contenida en ellos se utilizarán únicamente para el fin para el que han sido facilitados y la tarea a la que se ha autorizado a cada persona.

No se podrán crear ningún fichero de carácter personal sin la autorización del Responsable de Seguridad o del Fichero.

Todos los daños causados por el no cumplimiento de lo descrito en el documento o en la ley vigente, será responsabilidad de la persona que infrinja la normativa.

El puesto de trabajo de cada trabajador será responsabilidad suya el mantener medidas para no facilitar accesos no autorizados a la información. Siempre que se abandone el puesto de trabajo deberá de quedar protegido el acceso a la información. Si el trabajador envía documentos o información de carácter personal a las impresoras de la empresa deberá acudir a la recepción de esta para evitar ser interceptada por personal no autorizado. Además en el puesto de trabajo nunca deberá estar información protegida a la vista de cualquier persona que no sea autorizada o el propio afectado.

Se cumplirá la normativa de contraseñas y estas deberán mantenerse siempre en secreto.

La instalación de cualquier programa o aplicación no autorizada por el Responsable de Seguridad o Administrador del Sistema deberá pedirse su evaluación y

posterior autorización antes de instalarla, para evitar posibles riesgos de seguridad.

La información protegida que no esté informatizada, estando en soporte físico, deberá mantenerse siempre bajo acceso protegido (llaves, candados, claves numéricas, accesos por tarjeta o biométricos…).

7 Derechos de Acceso, Rectificación, Cancelación y Oposición

7.1 Introducción

Los Derechos de Acceso, Rectificación, Cancelación y Oposición, también conocidos como Derechos ARCO (acrónimo de las iniciales de cada derecho) son los derechos que tienen los afectados por la información.

Los afectados o personas que han facilitado la información o hace referencia a ellas, tienen derechos sobre la información que facilitaron y el Responsable del Fichero tendrá que encargarse de que se atienden sus derechos.

Cualquier petición de un usuario/afectado sobre los derechos ARCO deberán ser atendidos según el artículo 25.2 de la LOPD.

Si los datos necesitaran alguna corrección se actuaría como se indica en el artículo 25.3 de la LOPD.

Para poder hacer uso de sus derechos, las personas deberán identificarse adecuadamente. Solamente en caso

de incapacidad o minoría de edad, lo podrá hacer su representante legal. Se podrá también delegar el derecho en otra persona aun estando con las capacidades plenas, a través de los medios legales de cesión de poderes a través de notarios o juzgados.

Los derechos son independientes entre sí, por lo que la aplicación de uno de ellos no implica la obligación o prohibición de realizar ningún otro.

No existirá contrapartida por la aplicación de ninguno de los derechos.

La empresa deberá poner un medio sencillo para poder aplicar los derechos por parte de los afectados.

En el Anexo H se incluye una plantilla para solicitud, que deberá estar disponible para los afectados a través de cualquier medio por donde se recoja la información. Se pueden incluir otros formularios siempre que sean fáciles y gratuitos para que los afectados soliciten sus derechos.

Los derechos tienen un plazo de atención estipulados y sobre los cuales si no se cumplen el afectado podrá instar a la AEPD para la tutela como indica el artículo 18 de la LOPD.

7.2 Derecho de Acceso

En la LOPD se reconoce en el artículo 15.1 el derecho del afectado por solicitar y acceder de manera gratuita a la información con datos de carácter personal que hayan sido almacenados o tratados por parte de la empresa.

Se pedirá al usuario que se identifique el afectado, y siempre que no se deniegue por una identificación incorrecta, la empresa deberá facilitar la información que solicita el afectado. Además se deberá incluir los tratamientos que se hayan realizado con ella y el fin para el que se recabo la información.

La atención se deberá realizar en un mes desde que se recibe la solicitud.

7.3 Derecho de Rectificación

Según la LOPD en su artículo 16.2 los afectados tendrán derecho a la rectificación o cancelación de su información de carácter personal.

Para ello el afectado deberá identificarse adecuadamente, y se realizarán las rectificaciones indicadas en el plazo máximo de 10 días desde la recepción de la solicitud.

Esta rectificación podría ser denegada si la identificación no es correcta, o los datos a rectificar no corresponden con la realidad o si la ley refiere a la empresa responsable el impedimento de revelar el tratamiento de los datos.

7.4 Derecho de Cancelación

Al igual que en el derecho de rectificación, en el artículo 16.2 se reconoce el derecho a cancelación por parte de los afectados.

La solicitud de este derecho deberá acompañarse siempre de la identificación correcta del afectado y la información a cancelar. Se atenderá de la manera oportuna y correcta en un plazo de 10 días desde la recepción de la solicitud.

Se podrá denegar el derecho por identificación incorrecta, o cuando los datos estén en un procedimiento administrativo en el momento de la petición, o depende de más afectados, o si por ley o una relación contractual entre la empresa y usted que justifique su salvaguarda.

Cancelar la información supone un bloqueo de la información durante el plazo que estipula la ley que deben conservarse información por posibles procedimientos administrativos o penales. Después del bloque únicamente podrán utilizarse estos datos para esos fines. Una vez cumplido el plazo podrán destruirse.

7.5 Derecho de Oposición

El derecho de Oposición de un afectado está recogido en el artículo 34 de la LOPD, definiendo como el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la

concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el art. 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el art. 36 de este reglamento.

El afectado deberá identificarse correctamente en la solicitud del derecho. Este se atenderá en el plazo de 10 días desde la recepción de la solicitud.

Se pude denegar la solicitud si no se identifica correctamente, o no expone motivos fundados y legítimos que justifiquen su derecho, o si la ley ampara a la empresa para la no aplicación de este derecho sobre la información solicitada.

ANEXOS

1 Anexo A. Relación de Ficheros

Se describirán todos los ficheros con datos de carácter personal.

Nombre del fichero	Tipo de Fichero	Nivel de Seguridad	Código RGPD	Fecha

2 Anexo B. Estructura de Ficheros y/o Base de Datos

2.1 Estructura Ficheros

UBICACIÓN

Nombre: **NIF/CIF:**

Dirección:

Localidad: **Código postal:**

Provincia: **País:**

Teléfono: **Fax:** **E-mail:**

ENCARGADO

Nombre: **NIF/CIF:**

Dirección:

Localidad: **Código postal:**

Provincia: **País:**

Teléfono: **Fax:** **E-mail:**

(Ejemplo con Fichero de Proveedores/Clientes para datos

en la Estructura del fichero o Base de Datos)

SISTEMA DE TRATAMIENTO

Tipo de Sistema de Tratamiento
- Mixto

ESTRUCTURA

Datos de carácter identificativo
- DNI / NIF
- Nombre y apellidos
- Dirección (postal, electrónica)
- Teléfono

Otros Datos Tipificados
- Características personales
- Circunstancias sociales
- Información comercial
- Económicos, financieros y de seguros
- Salud
- Transacciones de bienes y servicios

Finalidades
- Gestión de clientes, contable, fiscal y administrativa

ORIGEN Y PROCEDENCIA DE LOS DATOS

Procedencia de los datos
- El propio interesado o su representante legal

Colectivos o Categorías de interesados
- Clientes y usuarios
- Proveedores

CESIÓN O COMUNICACIÓN DE DATOS

Categorías de Destinatarios de Cesiones

- Organizaciones o personas directamente relacionadas con el responsable
- Administración tributaría, Bancos, cajas de ahorros y cajas rurales

2.2 Versiones Documento de Seguridad

Responsable del fichero	Cambios Realizados	Versión Fichero	Fecha Modificación

3 Anexo C. Recursos Protegidos

Se deberán replicar cada uno de los apartados tantas veces como existan recursos de ese tipo en la empresa.

SEDES EMPRESA	
Nombre Sede	
Responsable	
Dirección	
Localidad	
Provincia	
Código Postal	
País	
Teléfono	
Fax	
Email	
ALMACENES DATOS	
Responsable	
Dirección	
Localidad	
Provincia	
Código Postal	
País	
Teléfono	
Fax	

Email	
Tipología de datos	
Nivel Seguridad	
SOPORTE HARDWARE	
Responsable	
Sede	
Marca	
Modelo	
Tipología de hardware	
SOPORTE SOWFTARE	
Responsable	
Sede	
Software	
Versión	
Tipología de software	

4 Anexo D. Organización de la Empresa

En este Registro se detallaran los diferentes roles dentro de la empresa en temas de RLOPD. Se pueden repetir tantas veces como existan personas con los roles y se deberá mantener un histórico de todos los puestos.

Puesto	Persona	ID Usuario	Fecha Alta	Fecha Baja
Responsable Fichero				
Responsable Fichero				
Responsable Seguridad				
Administrador Sistema				
Responsable ARCO				

5 ANEXO E. Personal Autorizado

5.1 Alta de Empleado / Permisos Sobre Ficheros

ALTA EMPLEADO / PERMISOS SOBRE FICHEROS **Ref.**

Adjuntar con el documento de alta de empleado.

Fecha: Hora:

Datos del fichero (sobre el que se conceden los permisos):

Nombre:

Descripción:

Datos Del empleado (persona a la cual se quiere conceder los permisos):

Nombre:

DNI:

Gestiona el alta (persona que ejecuta el procedimiento de añadir permisos):

Nombre:

Cargo:

Permisos concedidos:

Acceso al programa _____ que manipula el fichero. Lectura ___ Escritura ___

Perfil al que se ajusta: _____

Configuración. SI ___ NO ___

Acceso a todos los datos del programa Listar ___ Insertar ___ Modif. ___ Borrar ___

Acceso al Módulo _____ Listar ___ Insertar ___ Modif. ___ Borrar ___

Acceso al Módulo _____ Listar ___ Insertar ___ Modif. ___ Borrar ___

Acceso al Módulo _____ Listar ___ Insertar ___ Modif. ___ Borrar ___

Acceso al Módulo _____ Listar ___ Insertar ___ Modif. ___ Borrar ___

Acceso al Módulo _____ Listar ___ Insertar ___ Modif. ___ Borrar ___

Copias de respaldo. Creación ___ Restauración ___ Denegado ___

Acceso al ordenador _____

Grupos a los que pertenece: _____

Configuración. SI ___ NO ___

Acceso a todos los datos del equipo Control Total ___ Lectura ___ Escritura ___ Denegado ___

Acceso a la Carpeta _____ Control Total ___ Lectura ___ Escritura ___ Denegado ___

Acceso a la Carpeta _____ Control Total ___ Lectura ___ Escritura ___ Denegado ___

Acceso a la Carpeta _____ Control Total ___ Lectura ___ Escritura ___ Denegado ___

Acceso a la Carpeta _____ Control Total ___ Lectura ___ Escritura ___ Denegado ___

Copias de respaldo. Creación ___Restauración ___Denegado ___

Adicionalmente al registro de alta anterior, se muestra a continuación un modelo de documento para realizar el contrato por ambas partes para la autorización de acceso a la información.

En _____ a __ de _____ de 20__.

REUNIDOS

De una parte D. _____, mayor de edad, con D.N.I. _____, y con domicilio a efecto del presente contrato en _____ y, de otra, D. _____, mayor de edad, con D.N.I. _____, y con domicilio a efecto del presente contrato en _____.

INTERVIENEN

D. _____ en su calidad de _____, en representación de CLINICA DENTAL SONRISA con C.I.F. _____ y domicilio en _____ (en lo sucesivo, _____)

D. _____ en su calidad de _____, en representación de _____ con

C.I.F. _____ y domicilio en _____ (en lo sucesivo, _____).

MANIFIESTAN

I.- El presente contrato se ha establecido para la _____, por lo que _____ deberá facilitar a _____ datos de carácter personal de terceros relacionados con aquélla y que son sujetos de relación jurídica negocial y/o laboral.

Los expresados datos se incorporan a un fichero cuyo titular es CLINICA DENTAL SONRISA por lo que está obligado a protegerlos en los términos previstos por la legalidad vigente.

II.- Estos datos deben ser sometidos a tratamiento por _____ para el cumplimiento por éste de sus obligaciones contractuales.

Por ello, y de acuerdo con lo establecido en el artículo 12 de la Ley Orgánica de Protección de datos de Carácter personal, _____, en su condición de encargado del tratamiento, asume expresamente las siguientes

CLÁUSULAS

PRIMERA – TRATAMIENTO DE DATOS PERSONALES.

El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

SEGUNDA – FINALIDADES DEL TRATAMIENTO.

El encargado del tratamiento no aplicará o utilizará los datos con fin distinto al que figure en dicho contrato, ni los comunicará ni siquiera para su conservación, a otras personas.

TERCERA – MEDIDAS DE SEGURIDAD.

1. El encargado del tratamiento adoptará las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado y que atenderán, necesariamente, lo previsto en Real Decreto 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

2. El encargado del tratamiento no registrará datos de carácter personal si los ficheros no reúnen las condiciones necesarias con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipo, sistemas y programas.

3. El encargado del tratamiento asegura que los ficheros y las personas que intervengan en el tratamiento cumplirán los requisitos y condiciones exigibles.

CUARTA – CUMPLIMIENTO DE OBLIGACIONES.

1. El responsable del fichero se reserva el derecho de verificar, por sí o por empresa o personal especializados, el cumplimiento por el encargado del tratamiento de las medidas y compromisos en esta cláusula establecidos.

2. El encargado del tratamiento soportará íntegra y directamente las responsabilidades que del incumplimiento de la presente cláusula se deriven, incluyendo las posibles sanciones.

3. Asimismo, el incumplimiento por _____ permitirá a CLINICA DENTAL SONRISA resolver el contrato sin indemnización ni preaviso algunos, debiendo, además, _____, resarcir a CLINICA DENTAL SONRISA

por los daños y perjuicios que del incumplimiento se pudieren derivar.

QUINTA – DURACIÓN DEL CONTRATO

La duración del presente contrato será de un año a partir de la fecha del mismo, prorrogándose automáticamente por plazos iguales, siempre y cuando se siga manteniendo la vigente relación entre CLINICA DENTAL SONRISA y _____(TERCERO)_____.

SEXTA – CONTROVERSIAS Y JURISDICCIÓN

Para las controversias que pudieren surgir con ocasión del presente contrato, las partes, con renuncia de su fuero propio, se someten expresamente a los Juzgados y Tribunales de _____.

Y en prueba de conformidad con todo ello firman el presente documento por duplicado ejemplar y a un solo efecto en el lugar y fecha expresados en el encabezamiento.

CLINICA DENTAL SONRISA _____

Fdo. _____ Fdo._____

5.2 Baja Empleado

SOLICITUD DE BAJA DE UN EMPLEADO **Ref.**

Fecha: _____ Hora: _____

Datos Del empleado (persona a la cual se quiere dar de baja):

Nombre: _____

DNI: _____ Ref: _____

Puesto de trabajo (persona de la cual se recogen los datos):

Cargo: _____

Sucursal: _____

Departamento: _____

Solicita la baja (persona que indica se realice la baja del empleado):

Nombre: _____

DNI: _____

Cargo: _____

Gestiona la baja (persona que realiza el procedimiento de baja de un empleado):

Nombre: _____

Cargo: _____

Resultado de la baja:

Marcar si se informa a las personas adecuadas y si se anulan los permisos del empleado en cuestión.

Permisos anulados:

Usuario autorizado sobre ordenadores.	SI ___	NO ___
Permisos sobre fichero / programa _____	SI ___	NO ___
_____	SI ___	NO ___
(lista de ficheros afectados) _____	SI ___	NO ___
Permiso del usuario sobre otros recursos (fotocopiadoras, etc).	SI ___	NO ___
Eliminación de los datos del empleado.	SI ___	NO ___
Eliminación de la lista de acceso al soporte papel.	SI ___	NO ___
Eliminación de la lista de acceso a los soportes informáticos.	SI ___	NO ___

Informar de la baja:

Superior inmediato.	SI ___	NO ___
Persona gestiona la lista acceso al papel.	SI ___	NO ___
Persona gestiona la lista de acceso a los soportes informáticos.	SI ___	NO ___
Control de acceso a la oficina o empresa.	SI ___	NO ___
Compañeros de trabajo	SI ___	NO ___

6 Anexo F. Gestión de Soportes

6.1 Inventario de Soportes

Listar todos los soportes informáticos utilizados que contengan datos de carácter personal.

Descripción del formulario

El siguiente formulario muestra los datos a rellenar cuando un soporte informático contenga datos de carácter personal:

Referencia: Identificador del soporte.

Cantidad: Número de soportes.

Tipo soporte: En este campo se anotará de qué tipo de soporte se trata, es decir, si es un disquete, un DVD, un disco duro, USB, etc.

Contenido: Información que contiene el soporte, anotando simplemente una indicación general de la información de la que se trata, sin demasiado detalle.

Fecha: Día, mes y año en que se realiza la anotación del soporte en cuestión.

Situación / Destino**:** Lugar o situación en el que se encuentra el soporte. Se podrá anotar en este campo cualquier información que se crea conveniente que proporcione una indicación de dónde se encuentra el soporte el soporte.

Baja: Fecha en la cual el soporte va a ser desechado.

Inventario de Soportes													
	Referencia	**Cantidad**	**Tipo soporte**	**Contenido**	**Fecha**	**Situación/ Destino**	**Baja**						

6.2 Solicitud de Entrada/Salida Soportes

SOLICITUD DE ENTRADA/SALIDA SOPORTES **Nº**

Fecha: Hora:

Realiza la solicitud (persona que realiza la solicitud):

Nombre:

DNI: Teléfono/fax:

Dirección:

Tipo de solicitud:

Tipo: Solicitud de Entrada [ ]

Solicitud de Salida [ ]

Otros [ ]

Código del Soporte:

Tipo de Soporte	Fecha de Vencimiento	Contenido

Responsable de Recepción:

Nombre:

Fecha:

Datos de Envío:

Tipo de Envío:

Número de Soportes:

Comentarios sobre envío:

Autorizado por:

Fecha Autorización: Empleado:

6.3 Informe de Revisión de los Registros de Acceso

INFORME DE REVISIONES de los REGISTROS DE ACCESO Nº

Fecha: Hora:

Intervalo que corresponde: al desde hasta

Encargado del estudio y tratamiento:

Nombre:

Cargo: Responsable de Seguridad

Incidencias detectadas:

Accesos NO AUTORIZADOS al SO de…

Usuarios internos

Usuarios internos desde el exterior

Usuarios externos

Desconocidos

Accesos NO AUTORIZADOS a FICHEROS de…

Usuarios internos

Usuarios internos desde el exterior

Usuarios externos

Desconocidos

Accesos AUTORIZADOS al SISTEMA fuera de hora de…

Usuarios internos		Usuarios internos desde el exterior	
Usuarios externos		Desconocidos	

Otros

Conclusiones:

Nivel de accesos autorizados al sistema operativo

Anormalmente Bajo [ ] Normal [ ] Anormalmente Alto [ ]

Nivel de accesos NO autorizados al sistema operativo

Inexistente [ ] Bajo [ ] Alto [ ] Excesivo [ ]

Nivel de accesos autorizados a los ficheros

Anormalmente Bajo [ ] Normal [ ] Anormalmente Alto [ ]

Nivel de accesos NO autorizados a los ficheros

Inexistente [ ] Bajo [ ] Alto [ ] Excesivo [ ]

Nivel de accesos autorizados al sistema fuera de horario de oficina

Anormalmente Bajo [ ] Normal [ ] Anormalmente Alto [ ]

Nivel de accesos NO autorizados al sistema fuera de horario de oficina

Inexistente [ ] Bajo [ ] Alto [ ] Excesivo [ ]

Nivel de accesos autorizados al sistema indebidamente

Inexistente [ ] Bajo [ ] Alto [ ] Excesivo [ ]

Estudio nivel de seguridad:

Nivel de seguridad del sistema de información

Insuficiente [ ] Suficiente [ ] Notable [ ]

Motivo:

Recomendaciones:

A continuación se detalla la información para rellenar el informa anterior.

Datos Generales

Nº: Número de informe de revisiones del registro de acceso.

Fecha: Fecha en que se ha realizado el informe.

Hora: Hora en que se ha realizado el informe.

Intervalo al que corresponde:

Desde: Fecha de inicio del intervalo al que corresponde el informe.

Hasta: Fecha de fin del intervalo al que corresponde el informe.

Encargado del estudio y tratamiento:

Nombre: Nombre de la persona que realiza el informe del registro de acceso.

Cargo: Cargo de la persona que realiza el informe, que será siempre el responsable de seguridad, por lo que este campo aparece rellenado por defecto.

Incidencias Detectadas:

Accesos no autorizados al sistema operativo de…

Usuarios internos: Número de accesos no autorizados al sistema operativo realizados desde la empresa y utilizando para ello la cuenta de un usuario de la empresa. Por ejemplo, los accesos no autorizados de un empleado durante el desarrollo de su trabajo en la empresa serían accesos de usuarios internos.

Usuarios externos: Número de accesos no autorizados al sistema operativo por parte de personal ajeno a la empresa haciendo uso para ello de un usuario proporcionado por la empresa. Pertenecerían a este caso los accesos realizados por parte de clientes a los que la empresa proporciona un usuario para acceder desde Internet a consultar sus datos.

Usuarios internos desde el exterior: Número de accesos no autorizados al sistema operativo desde la cuenta de un usuario perteneciente a la empresa y que se realizan desde el exterior de la misma. Por ejemplo, el caso de un empleado que trabaja desde casa, accediendo para ello al sistema de la empresa, sería un acceso de un usuario interno desde el exterior.

Desconocidos: Número de accesos no autorizados por parte de usuarios desconocidos por la empresa. El caso de un hacker que accede desde el exterior al sistema sería un acceso por parte de un usuario desconocido.

Accesos no autorizados a ficheros de…

Usuarios internos: Número de accesos no autorizados al fichero o ficheros haciendo uso para ello de la cuenta de un usuario de la empresa y desde la empresa.

Usuarios externos: Número de accesos no autorizados al fichero o ficheros por parte de personal ajeno a la empresa con una cuenta de usuario proporcionada por la empresa.

Usuarios internos desde el exterior: Número de accesos no autorizados al fichero o ficheros desde la cuenta de un usuario perteneciente a la empresa y que se realizan desde el exterior de la empresa.

Desconocidos: Número de accesos no autorizados por parte de usuarios desconocidos por la empresa.

Accesos autorizados al sistema fuera de hora de…

Usuarios internos: Número de accesos no autorizados al sistema, que se produzcan desde la empresa pero fuera del horario normal de trabajo de la misma, haciendo uso para ello de la cuenta de un usuario de la empresa.

Usuarios externos: Número de accesos no autorizados al sistema fuera del horario normal de trabajo, por parte de personal ajeno a la empresa haciendo uso para ello de un usuario proporcionado por la empresa.

Usuarios internos desde el exterior: Número de accesos no autorizados al sistema de información de la empresa, fuera de horario de oficina, desde la cuenta de un usuario perteneciente a la empresa y que se realizan desde el exterior de la misma.

Desconocidos: Número de accesos no autorizados por parte de usuarios desconocidos por la empresa, fuera de horario de trabajo.

Otros: Cualquier otro tipo de acceso al sistema, ficheros, etc. que no esté contemplado en los casos anteriores. Deberá indicarse qué tipo de acceso es, quién lo realiza, el número de accesos realizados, si han sido autorizados o no y toda la información que se considere oportuna para su posterior estudio.

Conclusiones: En este apartado se mostrarán las conclusiones obtenidas a partir de la información recogida en el apartado anterior del informe.

Nivel de accesos autorizados al sistema operativo: Deberá decidirse si el nivel de accesos autorizados es anormalmente bajo, normal o anormalmente alto en función de las circunstancias de la empresa durante el intervalo al que corresponde el registro. Evidentemente, el nivel de accesos autorizados al sistema no será igual en el mes de noviembre que en los meses de julio y agosto ya que en estos meses baja la actividad de la empresa. Por ello, deben tenerse en cuenta todos los factores que influyan en la cantidad de accesos al sistema.

Anormalmente bajo: Se marcará esta opción cuando el nivel de accesos autorizados al sistema operativo de la empresa sea demasiado bajo con respecto a lo que se considera el nivel normal.

Normal: Se marcará esta opción cuando la cantidad de accesos autorizados realizados al sistema de información de la empresa sea el esperado y corresponda con los niveles de acceso normales para la situación de la empresa durante el periodo al que corresponde el estudio.

Anormalmente alto: Se marcará esta opción cuando el número de accesos autorizados al sistema sean excesivamente altos con respecto a lo que se considera como nivel normal.

Nivel de accesos NO autorizados al sistema operativo:

Inexistente: Se elegirá esta opción cuando no se haya producido ningún acceso no autorizado al sistema operativo.

Bajo: Se elegirá esta opción cuando se hayan producido una cantidad insignificante de accesos no autorizados al sistema operativo.

Alto: Se indicará que el nivel de accesos no autorizados al sistema operativo es alto, cuando se hayan producido un número considerable de éstos, debiendo estudiar el motivo por el que se han producido.

Excesivo: El nivel de accesos será excesivo cuando se trate de un número tal de los mismos que exija un estudio exhaustivo de los motivos de estos accesos y la adopción de medidas para evitar que vuelvan a producirse un número excesivo de los mismos.

Nivel de accesos autorizados a los ficheros: Para rellenar este apartado se seguirán los mismos criterios que los descritos anteriormente para los accesos autorizados al sistema operativo.

Anormalmente bajo: Se seleccionará esta opción cuando los accesos realizados sobre al fichero o ficheros sean

demasiado escasos, teniendo en cuenta la situación particular de la empresa en el periodo en que se realizaron los accesos registrados.

Normal: Se marcará esta opción cuando la cantidad de accesos autorizados realizados al fichero o ficheros sea el esperado y corresponda con los niveles de acceso normales para la situación de la empresa durante el periodo al que corresponde el estudio.

Anormalmente alto: Se marcará esta opción cuando el número de accesos autorizados al fichero o ficheros de la empresa sean excesivamente alto con respecto a lo que se considera como nivel normal.

Nivel de accesos NO autorizados a los ficheros:

Inexistente: Se elegirá esta opción cuando no se haya producido ningún acceso no autorizado al fichero o ficheros.

Bajo: Se elegirá esta opción cuando se hayan producido una cantidad insignificante de accesos no autorizados al fichero o ficheros.

Alto: Se indicará que el nivel de accesos no autorizados al fichero o ficheros es alto, cuando se hayan producido un número considerable de éstos, debiendo estudiar el motivo de estos accesos.

Excesivo: Se considerará excesivo el nivel de accesos cuando se trate de un número tal que exija un estudio exhaustivo de los motivos de estos accesos y la adopción de medidas para evitar que vuelvan a producirse un número excesivo de los mismos.

Nivel de accesos autorizados al sistema fuera de horario de oficina: Igual que en los casos anteriores, debe tenerse en cuenta el periodo durante el que se realizan los accesos, de forma que se evalúe si la cantidad de los mismos es baja, normal o alta en función de la situación particular de la empresa en dicho periodo.

Anormalmente bajo: Se seleccionará esta opción cuando los accesos realizados al sistema fuera de horario normal de trabajo sean demasiado escasos con respecto a lo que podría esperarse.

Normal: Se marcará esta opción cuando la cantidad de accesos autorizados realizados al sistema fuera de horario de trabajo sea el esperado y corresponda con los niveles de acceso normales.

Anormalmente alto: Se marcará esta opción cuando el número de accesos autorizados al sistema fuera del horario normal de trabajo de la empresa sea excesivamente alto con respecto a lo que se considera como nivel normal.

Nivel de accesos NO autorizados al sistema fuera de horario de oficina:

Inexistente: Se elegirá esta opción cuando no se haya producido ningún acceso no autorizado al sistema fuera del horario de oficina.

Bajo: Se elegirá esta opción cuando la cantidad de accesos no autorizados al sistema fuera de horario de oficina se considere insignificante.

Alto: Se indicará que el nivel de accesos no autorizados al sistema fuera de horario normal de trabajo es alto, cuando se hayan producido un número considerable de éstos, debiendo estudiar el motivo que los causó.

Excesivo: El nivel de accesos será excesivo cuando se trate de un número tal de los mismos que exija un estudio exhaustivo de los motivos de estos accesos no autorizados al sistema fuera de horas de trabajo y la adopción de medidas para evitar que vuelvan a producirse un número excesivo de los mismos.

Nivel de accesos autorizados al sistema indebidamente: En este apartado se estudiarán los accesos que, aunque hayan sido autorizados por el sistema operativo, no deberían haberse producido. Por ejemplo, si un usuario accede a los datos de un fichero a los que se supone que no debería

tener acceso, debe anotarse en esta sección para su posterior estudio.

Inexistente: Se elegirá esta opción cuando no se haya producido ningún acceso autorizado indebido al sistema.

Bajo: Se elegirá esta opción cuando la cantidad de accesos autorizados e indebidos al sistema se considere insignificante.

Alto: Se indicará que el nivel de accesos autorizados pero indebidos al sistema es alto, cuando se hayan producido un número considerable de éstos, debiendo estudiar el motivo de estos accesos.

Excesivo: El nivel de accesos será excesivo cuando se trate de un número tal de los mismos que exija un estudio exhaustivo de los motivos de estos accesos autorizados e indebidos y la adopción de medidas para evitar que vuelvan a producirse un número excesivo de los mismos.

Estudio nivel de seguridad:

Nivel de seguridad del sistema de información: Este apartado se rellenará en función de las conclusiones que se extraigan de la información de los apartados anteriores.

Insuficiente: El nivel de seguridad será insuficiente cuando se hayan producido un número excesivo de accesos no autorizados o indebidos al sistema o al fichero o ficheros, y los niveles de acceso sean inadecuados en todos los casos o en un número importante de ellos.

Suficiente: El nivel de seguridad será suficiente cuando los niveles de accesos estén dentro de lo normal, aunque puedan haberse producido algunos accesos indebidos o no autorizados a los ficheros o al sistema.

Notable: El nivel de seguridad del sistema de información será notables, cuando todos los accesos han sido autorizados debidamente, siendo todos los niveles de acceso normales o bajos en cada caso y no se observe ninguna anomalía en cuanto a los accesos a los datos,

ficheros y sistema en el periodo de tiempo al que corresponde el informe del registro de acceso.

Motivos: En este apartado se indicarán las razones por las cuales se ha calificado el nivel de seguridad del sistema como insuficiente, suficiente o notable.

Recomendaciones: Por último, el responsable de seguridad deberá indicar las recomendaciones adecuadas encaminadas a solucionar los posibles problemas de seguridad que pudiera tener el sistema de información, en caso de ser el nivel de seguridad del mismo suficiente o insuficiente.

7 Anexo G. Gestión de Incidencias

7.1 Parte de Incidencia (Notificación)

PARTE DE INCIDENCIAS (Notificación) **Nº**

Fecha: Hora:

Localización:

Tipo de incidencia:

Tipo: Dudas sobre integridad de los datos [ ]

Fallo detectado [ ]

Ataque externo [ ]

Otros [ ]

Descripción:

Realiza la notificación:

Nombre:

Cargo:

Asignación del encargado de la gestión de la incidencia:

Fecha: Hora:

Nombre:

Cargo:

8 Anexo H. Derechos ARCO

SOLICITUD DE ACCESO **Nº**

Fecha: Hora:

Realiza la solicitud (persona que realiza la solicitud):

Nombre:

DNI: Teléfono/fax:

Dirección:

Tipo de solicitud:

Tipo: Solicitud de información sobre los datos que se tienen almacenados sobre él (consulta) [ ]

Datos incorrectos o incompletos (modificación) [ ]

Solicitud de cancelación o borrado de los datos (borrado) [ ]

Otros [ ]

Descripción:

Descripción:

Cambios:

Fichero al que afecta:		
Campo	**Nuevo Valor**	**Valor Anterior**

Completa la solicitud (empleado que rellena los campos):

Nombre: _____

Cargo: _____

Destino de la solicitud (persona que gestiona la solicitud):

Nombre: _____

Cargo: _____

Resolución de la solicitud:

Aceptar solicitud [ ] Fecha realización: _____

Empleado: _____

Denegar solicitud [ ] Motivo: _____

_____

Fecha notificación: _____ Empleado: _____

DOCUMENTACIÓN COMPLEMENTARIA

1 Información a Clientes

INFORMACIÓN A CLIENTES (CARTEL L.O.P.D.)

En cumplimiento de lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal, le informamos que sus datos personales recogidos serán tratados con arreglo a nuestra relación comercial y quedarán incorporados en los ficheros de la empresa JUAN Y MARIA, con la finalidad de prestarle nuestros servicios de clínica dental.

En este sentido, usted consiente de forma expresa a que sus datos sean tratados por la empresa para dar cumplimiento a las finalidades indicadas anteriormente así como para remitirle información relativa a los temas de especial interés para usted.

Asimismo, le informamos que usted puede ejercitar los derechos de acceso, rectificación, cancelación y oposición dirigiéndose por escrito JUAN Y MARIA con C.I.F _____ y domicilio en _____
Este establecimiento cuenta con los formularios para el ejercicio de estos derechos.

Fdo.: La dirección.

2 Pie de Página de Facturas y Documentos

Según la Ley 15/1999, de 13 de diciembre, le informamos que los datos personales que puedan constar en este documento se encuentran incorporados en un fichero propiedad de JUAN Y MARIA y n° CIF _____, con la finalidad de gestionar nuestra relación comercial y poder informarle de nuestros servicios. Si desea ejercitar sus derechos de acceso, oposición, rectificación y cancelación, lo podrá hacer dirigiéndose por escrito a la dirección _____.

3 Cláusula Genérica de Legitimación de Email

En cumplimiento de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que los datos personales que puedan figurar en esta comunicación están incorporados a un fichero creado por JUAN Y MARIA, con la finalidad de poder gestionar la relación comercial que nos vincula e informarle de nuestros servicios.

En virtud de lo dispuesto en el artículo 15 y siguientes de la LOPD y en los términos que indica su Reglamento de desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre, en cualquier momento usted podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición, dirigiéndose por escrito a la dirección _____

En cumplimiento de lo prevenido en el artículo 21 de la Ley 34 2002 de servicios de la sociedad de la información y comercio electrónico, si usted no desea recibir más información sobre nuestros servicios, puede darse de baja en la siguiente dirección de correo electrónico: INFO@CLINICADENTALSONRISA.COM

4 Documento de Recepción y Conocimiento LOPD

En cumplimiento de lo que se dispone en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), le informamos que los datos de carácter personal que nos proporcione rellenando el formulario de registro electrónico que aparece en esta página se recogerán en ficheros cuyo responsable es JUAN Y MARIA.

En virtud de lo dispuesto en el artículo 15 y siguientes de la LOPD y en los términos que indica su Reglamento de desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), en cualquier momento usted podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición, dirigiéndose por escrito a JUAN Y MARIA en la dirección _____.

El hecho que no introduzca los datos de carácter personal que aparecen en el formulario de inscripción como obligatorios podrá tener como consecuencia que no podamos atender tu solicitud.

Le rogamos que comunique inmediatamente a JUAN Y MARIA cualquier modificación de sus datos de carácter personal para que la información que contienen nuestros ficheros esté siempre actualizada y no contenga errores. Asimismo, con la aceptación de este aviso legal, reconoce que la información y los datos personales recogidos son exactos y veraces.

La recogida de sus datos de carácter personal se hace con la finalidad de responder a su consulta, transmitirte publicidad de productos, servicios e información de carácter comercial de interés de JUAN Y MARIA.

Le informamos, asimismo, que nuestro servidor enviará a su ordenador un fichero (’cookie') que, con la información que nos facilitará sobre el idioma escogido y otras opciones de navegación de las páginas que visite. En cualquier caso, usted tiene la posibilidad de configurar su ordenador de manera que rechace la instalación de estas 'cookies'.

JUAN Y MARIA se compromete a tratar de una manera absolutamente confidencial sus datos de carácter personal y a utilizarlos sólo para las finalidades indicadas. Asimismo te informamos que JUAN Y MARIA tiene implantadas las medidas de seguridad de tipo técnico y organizativas necesarias para garantizar la seguridad de sus datos de

carácter personal y evitar la alteración, la pérdida y el tratamiento y/o acceso no autorizado, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, provenientes de la acción humana o del medio físico y natural. Todo ello de conformidad con lo dispuesto en la LOPD y en su RLOPD.

D/Da._____ , acusa recibo del ejemplar del DOCUMENTO DE SEGURIDAD que le ha sido facilitado por JUAN Y MARIA, en cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre.

D/Dª._____ , manifiesta conocer y se compromete a observar en todo momento las prescripciones contenidas en el Documento de Seguridad, especialmente los apartados sobre:

- Normas, procedimientos, reglas y estándares de seguridad
- Funciones y obligaciones de personal

- Gestión de incidencias
- Derechos de los afectados

y los respectivos anexos contenidos en dicho documento, manteniendo en todo momento su deber de secreto y confidencialidad sobre los datos de carácter personal a los que tenga acceso en el ejercicio de las funciones que le hubiesen sido asignadas por JUAN Y MARIA.

FIRMA Y FECHA

5 Videovigilancia

Modelo Cláusula Informativa

Art. 3, apartado B. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

De conformidad con lo dispuesto en el art. 5.1 LO 15/1999, de 13 de diciembre, de Protección de Datos, se informa:

1. Que sus datos personales se incorporarán al fichero denominado "VIDEOVIGILANCIA", y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia.

2. Que el destinatario de sus datos personales es el dueño del establecimiento “CLINICA DENTAL SONRISA”

3. Que puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante el Responsable del Fichero.

4. Que el Responsable del Fichero es “CLINICA DENTAL SONRISA” con CIF _____, con domicilio en _____

ZONA VIDEOVIGILADA

LEY ORGANICA 15/1999, DE PROTECCIÓN DE DATOS

PUEDE EJERCITAR SUS DERECHOS ANTE:

DATOS DE LA EMPRESA RESPONSABLE DEL FICHERO

CUMPLIMIENTO CON NECESIDADES DE LA EMPRESA

Una vez creado el Documento de Seguridad, añadido Anexos y Documentación Complementaria para el cumplimiento de la LOPD necesarios para la clínica, se va a indicar como se va a cumplir con la legislación con lo desarrollado.

La empresa al tener dos oficinas tendrá que registrar cada intercambio de información física entre las sedes, quedando registradas en el Registro de Entradas y Salidas, aunque el origen y el destino siga siendo la misma empresa.

Todas las empresas externas que sirven servicios a la clínica (CleanWorks, MercaDental, SecureWorks, BankWorks, NetWorks, y el cirujano y anestesista externos) tendrán que tener conocimiento y respetar la normativa descrita en el documento de seguridad. Las personas que realicen cualquier tratamiento con datos de carácter personal deberán cumplimentar y solicitar las autorizaciones a los responsables del fichero.

Al ser una clínica Dental en la que se trata información de salud de los clientes, complementarios a grados de invalidez, los datos serán tratados como nivel alto en las fichas médicas, teniendo especial medida de seguridad en su acceso, traza y destrucción. Todas las normativas para el acceso se indican en el apartado de normativa, en él además se crearan diferentes roles en los que solamente las personas podrán acceder a la información a la que están autorizados, pues el tratamiento de los datos de nivel alto estarán restringidos a las personas que realmente los necesiten. La traza y tratamiento se dará seguimiento con la cumplimentación de las autorizaciones, logs de acceso informático, y registros en los inventarios donde se almacenara físicamente también la información, como en la recogida de datos inicial en la que se firman las autorizaciones y el rellenado de la encuesta de salud previa. Para la destrucción de la información en función del medio, se describe también en la normativa y se deberá ser riguroso con el método, y con la espera en plazos para su destrucción, para el cumplimiento con normativas judiciales u obligaciones con los derechos ARCO.

Cualquier información de carácter personal en medio físico estará guardado bajo llave y debidamente clasificado y registrado, para su tratamiento y acceso.

Todos los medios informáticos se implementaran con las medidas descritas de acceso, antivirus y firewall, para proteger la información tanto internamente como a través de la web y correo electrónico. En todas ellas se deberán aplicar las reglas descritas, y adjuntar en emails o página web los avisos/notas informativas, que en algunos casos deberán ser aceptadas antes de que el usuario pueda continuar el tratamiento de la información.

Como se tienen medidas de seguridad en la empresa con videovigilancia, se adjunta el cartel informativo que indica que es un área videovigilado y que se cumplen con las normativas de la LOPD. Se debe asegurar que la empresa contratada cumplirá la normativa de la LOPD con el tratamiento que realice de las imágenes y que tenga en conocimiento el documento de seguridad para cumplir también siempre con cualquier regla adicional que incluya la empresa para el tratamiento de sus datos de carácter personal.

Todo registro que se deba realizar y notificar a la AGPD, se realizará a través de la red, enviando los formatos cumplimentados como solicita en su página web la AGPD, por medio de su Servicio NOTA

https://sedeagpd.gob.es/sede-electronica-web/vistas/formNOTA/servicioNOTA.jsf

en el cual se inscribirán los ficheros con certificado de firma electrónica. Sera una de las obligaciones de los responsables del fichero.

Se debe mantener el documento de seguridad actualizado a cualquier modificación en la normativa del estado y en las actividades que realice la empresa.

CONCLUSIONES

Al finalizar la realización de este proyecto en el cual me he sumergido en el mundo de la LOPD, he podido comprobar las normativas y leyes que se han definido para la protección de la información de carácter personal en España.

Hasta hace unos años el mundo de la información y la globalización de los datos crecía a un ritmo vertiginoso, pero no existía ninguna regulación al respecto. Con esta ley "Ley Orgánica de Protección de Datos" España inicia una regulación para las empresas para que los usuarios afectados estén protegidos.

Es cierto que las empresas no todas cumplen la normativa correctamente (yo diría que la mayoría) y otras incluso ni la aplican de ninguna manera. Cabe decir que una vez tengo el conocimiento de todo lo exigido por la ley y los procedimientos que se requieren para su cumplimiento, la veo una ley que únicamente empresas con una gran estructura podrían emplear personas para seguir estas normas. Una PYME (Pequeña y Mediana Empresa) en la mayoría de los casos no dispone del tiempo necesario para cumplir la ley completamente sin desatender el servicio que

ofrece o impactando en el cumplimiento de venta u objetivos.

Además no solamente las empresas tienen en la LOPD un reto a cumplir demasiado grande muchas. El control por parte de las entidades gubernamentales que deben velar por su aplicación no pueden atender correctamente este control y por ello la protección de los usuarios.

La regulación de la información de carácter personal debería ser un tema importante en los acuerdos entre países pues aunque España implanta la LOPD, hoy día por internet la información vuela a través de la red a muchos países y se debería de acordar el cumplimiento de ciertos mínimos de protección con los usuarios entre países.

En mi reflexión la resumo como un gran paso para la regulación y protección del tratamiento de información de carácter personal, pero aún con oportunidades de mejora para la facilitación en su implantación por parte de pequeñas y medianas empresas, y para el control por parte de las instituciones públicas que deben velar por su cumplimiento.

BIBLIOGRAFIA

[1] **BOE – LOPD**

https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

[2] **AEPD – Reglamento de la LOPD**

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/reglamento_lopd/index-ides-idphp.php

[3] **AEPD – Legislación y resoluciones**

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/index-ides-idphp.php

[4] **GENERACIÓN DOCUMENTOS**

http://www.haztelalopd.org/

[5] **NIVELES DE SEGURIDAD**

http://www.audidat.com/lopd/aplicacion-de-niveles-de-seguridad-en-proteccion-de-datos.html

http://www.projuri.com/niveles-proteccion-datos/

[6] **Leyes Unión Europea**

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al14012

CONTENIDO DEL CD

[1] **Memoria**

Documento que contiene la memoria del TFG

Formato: PDF / A