DOCUMENTO DE SEGURIDAD

Fecha Versión V9: mayo 2021

ÍNDICE

1. HISTORIAL DE REVISIONES

Versión	Fecha	Modificaciones realizadas
V0		Edición inicial
V1	30/01/2007	
V2	31/08/2009	Cambio de Responsable de Seguridad LOPD. Nuevo Responsable Iñaki Irigoyen. Revisión del documento tras auditoria
V3	31/12/2010	Cambio de Responsable de Seguridad LOPD. Nuevo Responsable Ana Isabel Vega
V4	31/12/2012	Supresión fichero Proveedores
V5	3/02/2015	Alta fichero ACCESOS INDIVIDUALES
V6	18/10/2017	Se incorpora el Historial de revisiones En las descripciones de los ficheros se incluye si los soportes son automatizados o no automatizados
V7	27/11/2018	Revisión y Adecuación RGPD
V8	Abril 2019	Revisión y adecuación nueva norma LOPD 2018
V9	Mayo 2021	Actualización de personas y accesos

2. INTRODUCCIÓN

El presente documento y sus anexos, han sido redactados en cumplimiento de lo dispuesto en el Reglamento (UE) 2016/679 de protección de datos de carácter personal y recoge la política de protección de datos de la empresa así como las medidas de índole técnica y organizativa necesarias para garantizar la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal.

El presente manual de protección de datos responde a la necesidad de la empresa como responsable del tratamiento de cumplir con las obligaciones derivadas del Reglamento (UE) 2016/679 de protección de datos de carácter personal, teniendo en cuenta la infraestructura y las circunstancias particulares de la organización.
El Responsable del Tratamiento, según el Reglamento (UE) 2016/679 de protección de datos, es la persona física y/o jurídica, privada o pública, que decide sobre el tratamiento de los datos. Esta responsabilidad debe desarrollarla durante toda la "vida" del dato, es decir, desde que este entra a formar parte del sistema de información hasta la eliminación del mismo.

Su condición de Responsable hace que está sujeto a los requerimientos establecidos en la normativa y que, en consecuencia, tenga que observar cuantas obligaciones disponga el Reglamento.

3. POLÍTICA DE PROTECCIÓN DE DATOS como Responsable de Tratamiento

OSARTEN Koop. E. . Osarten Kooperatiba Elkartea con NIF / CIF: F-20757779 Código de Actividad principal: 720 Dirección: PASEO JOSÉ MARÍA ARIZMENDIARRIETA, nº 1.
Localidad: 20500 - MONDRAGÓN. GUIPUZCOA (ES)
Teléfono: 943.79.00.90
Delegada de Protección de Datos : dpo@osarten.com
Web: www.osarten.com

Para el desarrollo de sus actividades la empresa cuenta con los siguientes centros de trabajo:

Centro principal.

OSARTEN aplica el principio de responsabilidad activa en el tratamiento de sus datos de carácter personal, manteniendo una constante puesta al día y una promoción de la mejora continua del sistema de protección de datos. Mantiene toda la documentación y los registros a disposición de la autoridad de control y de los encargados del tratamiento aportando las evidencias que demuestren su firme compromiso con la protección de los datos de carácter personal.
OSARTEN garantiza:

- el respeto a las libertades y los derechos fundamentales de las personas físicas
- que los datos son tratados de manera lícita, leal y transparente
- que los datos tratados son exactos, adecuados, pertinentes y limitados en relación con los fines para los que son recogidos
- que los fines para los que son recogidos son explícitos y legítimos y que no son tratados de manera incompatible con dichos fines.
- que los datos no se mantendrán más allá del tiempo necesario para los fines para los que han sido recabados
- las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

En aquellos tratamientos de datos que entrañen un alto riesgo para los derechos y libertades de las personas OSARTEN realizará una evaluación de impacto conforme se recoge en el presente manual.

Las normas expuestas en el presente Manual de Seguridad afectan a todas las estructuras y, por tanto, deberán ser acatadas por todos los usuarios de los sistemas informáticos de la Entidad.

OSARTEN de conformidad con el art. 37 del Reglamento (UE) 2016/679, el Consejo de Dirección de Osarten Koop. Elkartea por acuerdo de 23 de julio de 2018 nombró a su delegada de Protección de Datos de la Cooperativa. Dicho nombramiento se comunicó debidamente a la Agencia Española de Protección de Datos.

4. OBJETO DEL DOCUMENTO

El presente Manual tiene por objeto recopilar la normativa y procedimientos vigentes en la Entidad, en todo lo relacionado con las medidas de seguridad y dar cumplimiento a los requerimientos exigidos por el RGPD

El Manual se mantendrá actualizado y se revisará cada vez que se efectúen cambios en los sistemas de información o en la organización del mismo.

En relación con la estructura de este Documento y teniendo en cuenta la posibilidad que, en el futuro, puedan darse cambios sustanciales en relación con los sistemas de información manejados, el Manual ofrecerá un marco estable pero a su vez flexible, en lugar de una descripción estática de las medidas de seguridad implantadas, en cuyo caso se podría ver sometido a continuas actualizaciones.

Del mismo modo, el Manual estará adecuado, en cada momento, a la normativa vigente en materia de Protección de Datos de Carácter Personal.

El Documento de Seguridad, así como toda la documentación anexa, se encuentra bajo la custodia de la Delegada de Protección de Datos y será puesta a disposición de la Agencia Española de Protección de Datos, si fuera requerida.

En el presente Manual de Seguridad se utilizará la siguiente terminología:

- **Fichero:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
- **Sistema de información:** conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
- **Sistema de tratamiento:** modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados
- **Tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- **Usuarios que intervienen en el tratamiento de datos personales:** todos los usuarios -empleados o colaboradores- que, en el desarrollo de sus funciones tengan acceso a la información con datos de carácter personal y tienen que cumplir con las medidas de seguridad en materia de protección de datos.

5. ÁMBITO DE APLICACIÓN

Los recursos comprendidos en el ámbito de aplicación de este Documento son todos los ficheros, las aplicaciones que los tratan, los equipos informáticos que las soportan y los locales donde están ubicados.

En este sentido, el concepto de fichero engloba todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

A continuación, se relacionan los ficheros con datos personales que se mantienen en la Entidad, con descripción del contenido, el nivel de seguridad que corresponde a cada fichero (de forma que se pueda discernir qué medidas de las contenidas en el presente Manual de Seguridad le son aplicables), junto con la razón de su clasificación y el responsable interno del fichero.

NOMBRE FICHERO	DESCRIPCION DEL FICHERO	NIVEL	RAZON DE SU CLASIFICACION	RESPONSABLE INTERNO
Clientes	Almacena los datos de las personas que tienen relación con la empresa por la contratación o precontratación de servicios. Fichero automatizado y no automatizado	Básico	Contiene datos de carácter personal	Técnico de Administración
Personal	Almacena los datos de los empleados de OSARTEN Koop. E. para la gestión de nómina, gestión de recursos humanos y contratación de personal. Fichero automatizado y no automatizado	Alto	El conjunto de datos almacenados en este fichero es suficiente para obtener una evaluación de la personalidad de la persona.	Técnico de Administración
Cargos Representativos	Almacena la relación de cargos representativos de OSARTEN Koop. E. Fichero automatizado	Básico	Contiene datos de carácter personal (artículo 4.1)	Técnico de Administración
Servicio Médico	Almacena, a través de la historia médico-laboral de cada persona, los datos de salud relativos a los trabajadores de la propia empresa y de los solicitantes individuales del servicio Fichero automatizado y no automatizado	Alto	Contiene, entre otros, datos relativos a la salud de las personas.	Directora Medicina Directora Laboratorio
Acceso Individual	Gestionar el acceso a los datos personales de salud a través del portal web de Osarten y el envío de claves a la dirección electrónica indicada Fichero automatizado y no automatizado	Alto	Datos de carácter identificativo	Directora de Laboratorio

En el Anexo de este Manual de Seguridad se contempla, de forma más detallada, el inventario de ficheros de la Entidad, así como las características de cada uno, en relación con las especificaciones de regulación vigente en materia de Protección de Datos

6. FUNCIONES Y OBLIGACIONES DEL PERSONAL

De conformidad con lo dispuesto en RGPD, las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información deben estar claramente definidas y documentadas.

El Responsable del Tratamiento adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento (MANUAL DE USUARIO PARA LA PROTECCION DE DATOS).

Las figuras definidas para el cumplimiento de esta normativa se clasifican en las siguientes categorías:

1. **Responsable del tratamiento**: la persona física o jurídica, autoridad, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

2. **Delegado de Protección de Datos**, que tiene básicamente las funciones de informar, asesorar, supervisar el cumplimiento del RGPD y cooperar con la autoridad de control Asimismo, coordina y controla las medidas de seguridad establecidas en el presente Documento. Su designación no supone, en ningún caso, una delegación de la responsabilidad que corresponde al Responsable del tratamiento.

3. **Administrador del Sistema**, que es el encargado de administrar o mantener el entorno operativo y de comunicaciones de los Ficheros.

4. **Usuarios que intervienen en el tratamiento de datos personales:** todos los usuarios -empleados o colaboradores- que, en el desarrollo de sus funciones tengan acceso a la información con datos de carácter personal y tienen que cumplir con las medidas de seguridad en materia de protección de datos.

A continuación se describen las funciones y obligaciones que tienen que cumplir:

6.1 Funciones y obligaciones del Responsable del Tratamiento

El Responsable del Tratamiento, se encargará de adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal establecidos en el Reglamento. Deberá:

Cuando hay encargado de tratamiento, entregar al ENCARGADO los datos a tratar

Realizar, cuando así proceda, una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el ENCARGADO.

Realizar las consultas previas que corresponda.

Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del ENCARGADO.

Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

Derecho de información en el momento de la recogida de los datos.

6.2 Funciones de la Delegada de Protección de Datos

La delegada de protección de datos tendrá como mínimo las siguientes funciones (art 39 RGPD):

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud de Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del Reglamento;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del Reglamento, y realizar consultas, en su caso, sobre cualquier otro asunto.

Además:

1. Controlar y coordinar la implantación de las medidas de seguridad establecidas en el Manual.
2. Mantener el contenido del Manual de Seguridad debidamente actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la Entidad.
3. Supervisar la solicitud de creación o modificación de permisos y privilegios sobre el sistema y comunicar al Responsable de Informática las acciones que se deban realizar.
4. Mantener una relación actualizada de usuarios que tengas acceso a los Ficheros y restringir los accesos mediante un código de usuario y una contraseña.
5. Mantener un Registro de Incidencias de conformidad con lo dispuesto en el Manual de Seguridad y adoptar las medidas adecuadas para su resolución.
6. Analizar los Informes de Auditoría interna y elevar las conclusiones al Director General.
7. Dar cuentas de todos los temas relacionados con la LOPD al Director General.
8. Mantener actualizada la relación de empresas para las que somos Encargados del Tratamiento, junto con toda la documentación que se derive de esta circunstancia.
9. Mantener actualizados los Contratos de LOPD con todas las empresas para las que somos Encargados del Tratamiento del Fichero.
10. Elaborar y redactar los modelos de documentos, formatos o contratos que tiene que utilizar Osarten para dar cumplimiento a las obligaciones de LOPD.
11. Colaborar en la elaboración y redacción de los modelos de documentos, formatos o contratos que pueden servir de referencia para su uso por las empresas asociadas.
12. Colaborar en las auditorias del sistema de información según lo establecido por LOPD.

En Osarten existe un mail dpo@osarten.com cuya destinataria es, además de la Delegada de Protección de Datos, el Director General y el Responsable de Sistemas de Osarten.

6.3 Responsable de Sistemas Informáticos

1. Asesorar a la Delegada de Protección de Datos en todo lo relacionado con seguridad informática, copias de seguridad, control de accesos al sistema, sistemas de protección de la información, procedimientos de seguridad, etc., esto es, en todo lo relacionado con los Sistemas de Seguridad Informática.
2. Mantener actualizado en las aplicaciones informáticas de Osarten los procesos de control de acceso, registro y trazabilidad, de acuerdo con lo establecido en RGPD y LOPD
3. Mantener actualizado el Documento de Normas de Seguridad Informática de Osarten.
4. Supervisar el cumplimiento de las Normas de Seguridad Informática: controlar el cumplimiento de procedimientos, supervisar la operatoria seguida y los registros de seguridad, cumplimentar los formatos de registro de incidencias en el acceso a la información, etc.
5. Colaborar en las auditorías internas / externas del sistema de información según lo establecido por LOPD.
6. Realizar el informe de incidencia del Área de Sistemas de Información y comunicárselo la Delegada de Protección de Datos.
7. Velar por el cumplimiento de la LOPD en el ámbito de su área. Identificar desviaciones y proponer soluciones.

6.4 Funciones y obligaciones de los trabajadores en el cumplimiento LOPD.

Estas obligaciones afectan expresamente a los trabajadores que acceden a datos de carácter personal protegidos por el RGPD y LOPD

Todos los trabajadores expresamente autorizados para acceder a la información de los DATOS DE CARÁCTER PERSONAL y hacer uso de los sistemas de información, deberán cumplir con las funciones y obligaciones de seguridad que se implante en la empresa y que a tal efecto se le comuniquen por parte la Delegada de Protección de Datos. El INCUMPLIMIENTO de estas obligaciones podrá suponer sanciones disciplinarias de acuerdo con lo establecido en el Reglamento de Régimen Interno. Esta información se ha comunicado a todos los trabajadores a través del correo electrónico y también en alguna de las Charlas que la Dirección General dirige periódicamente a los trabajadores de Osarten Koop. E.

A continuación, se expone de forma resumida, las obligaciones que deben observarse:

EN EL PUESTO DE TRABAJO

- Los puestos de trabajo estarán bajo la responsabilidad del usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.
- Cuando se abandone un puesto de trabajo, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
- En el caso de las impresoras deberá asegurarse que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos.
- Cada trabajador será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

GESTIÓN DE SOPORTES DE INFORMACIÓN

- Observar y cumplir el procedimiento de gestión de soportes:
  - Los dispositivos de almacenamiento de datos (discos, pen-drives, listados en papel, etc.) deben estar correctamente identificados y permitir conocer el tipo de información que contienen.
  - Queda prohibida la salida de soportes magnéticos (pen-drives, discos,…) con datos de carácter personal fuera del edificio, salvo que ésta esté autorizada por la Delegada de Protección de Datos.
  - Todos los datos de carácter personal que se transmitan por correo electrónico deben estar encriptados.
- La pérdida o sustracción de cualquier dispositivo de almacenamiento de datos debe ser comunicada la Delegada de Protección de Datos. Esto incluye también datos en papel.
- Los soportes con información (papel, discos, CD/DVD,…) deberán ser custodiados para que no puedan ser manipulados por terceros.
- Los soportes de información, si procede su eliminación, deberán ser destruidos en la trituradora de materiales.

GESTIÓN DE INCIDENCIAS EN MATERIA DE LOPD

- Notificar a la Delegada de Protección de Datos cualquier incidencia en la que se tenga constancia o sospecha de que se vulnera la LOPD.
- Se entiende por **incidencia** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

USO DE PORTÁTILES Y DISPOSITIVOS DE ALMACENAMIENTO DE DATOS

- A todos los ordenadores portátiles se debe acceder con usuario y contraseña.
- La pérdida o sustracción de cualquier portátil debe ser comunicada a la Delegada de Protección de Datos

FICHEROS TEMPORALES

- **Ficheros temporales son** ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.
- Durante su uso, estos ficheros deben estar protegidos para que ningún tercero pueda acceder a los mismos.
- Con carácter general se eliminarán semanalmente los ficheros temporales que se produzcan en todos los equipos informáticos o, en casos excepcionales, una vez finalizado el motivo por el que se creó el fichero.
- El trabajador que creó el fichero es responsable de su eliminación.
- En ningún caso debemos tener datos de carácter personal que no pertenezcan a nuestra base de datos.

EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN ,SUPRESIÓN, LIMITACIÓN, OPOSICIÓN AL TRATAMIENTO, REVOCACIÓN DEL CONSENTIMIENTO O SOLICITUD DE PORTABILIDAD DE LOS DATOS

Cualquier persona puede ejercer sus derechos de acceso, rectificación, cancelación , supresión, limitación, oposición al tratamiento, revocación del consentimiento, solicitud de portabilidad de los datos.
Hay que cumplimentar el documento “Solicitud DERECHOS ” adjuntando siempre una fotocopia del DNI (o documento equivalente de identificación) y enviarlo a la Delegada de Protección de Datos para que proceda a su gestión (tal y como se detalla en el PROCEDIMIENTO de PROTECCION DE DATOS).

I. **Política de contraseñas implantada.**

- ✓ **Longitud mínima:** 8 caracteres, formado por mayúsculas, minúsculas y algún número.
- ✓ **Caducidad:** 3 meses (pedirá una nueva contraseña).
- ✓ **Histórico:** 8 contraseñas (no se podrán repetir las últimas 8).
- ✓ **Bloqueo del usuario:** al 5º intento de acceso erróneo.

7. NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

En este apartado del Manual de Seguridad se recogen los procedimientos establecidos en OSARTEN Koop. E. relativos a los siguientes aspectos:

- **Procedimientos requeridos por RGPD** que se recogen en el documento de "PROCEDIMIENTO LOPD", incluyendo en su contenido los siguientes procedimientos:
  - Control de automatizaciones para el alta de datos
  - Seguimiento de acciones de LOPD
  - Otras acciones de seguimiento en materia de LOPD.
  - Ejercicio de los derechos de acceso, rectificación, cancelación, supresión, limitación, oposición al tratamiento, revocación del consentimiento, solicitud de portabilidad de los datos.
  - Baja y/o finalización de contrato de servicio
  - Cesión de datos.
- **Procedimientos de Seguridad de Sistemas de Información relacionados con el objetivo.** Los procedimientos referenciados se encuentran recogidos en el manual de "Normas de Seguridad Informática".
- **Normas relacionadas con el objetivo.** Las normas referenciadas se encuentran en el manual de "Normas de Seguridad Informática".

8. REGISTRO DE INCIDENCIAS.

Una **Incidencia** es cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

El mantener un registro de las incidencias que comprometen la seguridad de los datos es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como la persecución de los responsables de los mismos.

A efectos orientativos, tendrán la consideración de incidencias los siguientes hechos:

- Modificaciones / accesos no autorizados de información.
- Pérdida de información.
- Copias indebidas de datos en los puestos de trabajo.
- Mal funcionamiento durante la realización de copias de seguridad.
- Errores del sistema / transacciones / base de datos.
- Accesos no autorizados a las salas donde se ubiquen los sistemas y soportes informáticos (CPD, oficina, caja de seguridad, etc.).
- Caída del sistema.
- Intento no autorizado de salida de soportes.
- Destrucción total / parcial de soportes físicos.
- Conocimiento por terceros del identificador de usuario y contraseña.
- Existencia de sistemas sin las debidas medidas de seguridad.
- Cambio de ubicación física de los datos.
- Otros.

El registro de incidencias es de obligado cumplimiento para todos los que trabajan en OSARTEN Koop. E. Afecta a la relación de Osarten con:

- Sus trabajadores.
- Las personas jurídicas (empresas) que demandan sus servicios.
- Las personas físicas (particulares) que demandan sus servicios.

Cuando un usuario detecta una incidencia, la comunica a la Delegada de Protección de Datos mediante el siguiente procedimiento:

Cualquier usuario que detecte una incidencia de seguridad en la protección de datos que haya puesto en peligro o haya dañado los ficheros de datos, se responsabiliza directa y personalmente de comunicarla sin demora a la Delegada de Protección de Datos, informando de aquellos datos que sean de su conocimiento. No comunicar una incidencia de la que se haya tenido conocimiento será considerado una falta contra la seguridad de los datos.

La Delegada de Protección de Datos, tomará las medidas oportunas para que, en el menor tiempo posible, se subsane la anomalía que haya generado la incidencia.

En caso de que se hayan visto afectados datos que hagan necesario llevar a cabo algún procedimiento de recuperación de datos, será imprescindible contar con la autorización del Responsable del tratamiento. Esta circunstancia se hará constar expresamente en el impreso de registro de incidencias.

La Delegada de Protección de Datos conservará debidamente cumplimentados y numerados correlativamente los registros de incidencias.
La Delegada de Protección de Datos informará de las incidencias de seguridad acaecidas en las reuniones con el Director General

9. COPIAS DE RESPALDO Y RECUPERACIÓN.

Con la finalidad de garantizar la integridad y la disponibilidad de los datos se realizan copias de respaldo y recuperación que, en caso de fallo del sistema informático, permitan recuperar y, en su caso reconstruir, los datos del fichero.

La política de salvaguardas es la siguiente:

Backups a cinta: se salva sobre el sistema de copias de Laboral Kutxa, para ello se utiliza una caché de discos y 2 librerías de cintas. El software utilizado es NetBackup.

Base de datos:

- Réplica en tiempo real sobre otra base de datos mediante Oracle data Guard. Mantiene actualizada la BD en un host remoto (Laboral Kutxa) para en caso de desastre poder switchear la producción a ese host.
- Backup de los LOGS de bbdd cada hora con retención 5 días
- Backup Full DIARIO de bbdd con retención 3 dias
- Backup Full SEMANAL de bbdd con retención 1 mes (4 semanas)
- Backup Full MENSUAL de bbdd con retención 3 meses
- Backup Full ANUAL de bbdd con retención indefinida, en Diciembre

Ficheros:

- Backup DIARIO, sólo ficheros modificados desde último Full, retención 1 semana
- Backup Full SEMANAL con retención 1 mes (4 semanas)
- Backup Full MENSUAL con retención 1 año
- Backup Full ANUAL con retención indefinida, en Diciembre

Exchange:

- Backup Full DIARIO con retención 1 semana
- Backup Full SEMANAL con retención 1 mes (4 semanas)
- Backup Full MENSUAL con retención 1 año
- Backup Full ANUAL con retención indefinida, en Diciembre

Servidores virtuales VMware:

- Backup DIARIO incremental, retención 1 semana
- Backup Full SEMANAL con retención 1 mes (4 semanas)
- Backup Full MENSUAL con retención 1 año
- Backup Full ANUAL con retención indefinida, en Diciembre

10. TELECOMUNICACIONES.

Como norma general, no se envían datos personales sensibles, mediante correo electrónico o cualquier otro medio de transmisión electrónica. No obstante, se autorizan los siguientes envíos:

- A los Servicios médicos de las empresas: datos de análisis clínicos, reconocimientos de ingreso, resultados de vigilancia de la salud u otros servicios de salud

- A Servicios de prevención ajenos: datos de análisis clínicos. Si, previamente, se dispone de la autorización del Responsable del tratamiento para el envío de dichos datos.

En los casos en los que está autorizado la transmisión de información sensible mediante correo electrónico o cualquier otro medio de transmisión electrónica, esta información se enviará siempre encriptada.

11. AUDITORÍA.

Anualmente se realizará una auditoría interna, que dictamine el correcto cumplimiento y la adecuación de las medidas del presente Manual de Seguridad o las exigencias del RGPD y la LOPD 2018, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán conocidos por la Delegada de Protección de Datos, quien propondrá al Responsable del Tratamiento las medidas correctoras correspondientes.

12. MEDIDAS DE SEGURIDAD APLICABLES A LOS TRATAMIENTOS NO AUTOMATIZADOS.

El acceso a la documentación con datos protegido se limita exclusivamente al personal autorizado.

Por regla general se evitara el archivo en formato papel, en USBs u otros dispositivos de almacenamiento, archivando todo documento en los directorios de red de cada Departamento. Una vez que se escaneen o copien en red los datos, estos deberán ser destruidos en las destructoras de papel habilitadas.

Aquella información que deba conservarse en soportes distintos de los de red u aplicaciones informáticas deberá almacenarse en armarios con llave y con acceso exclusivamente para la Delegada de Protección de Datos y el personal autorizado.

Documentos	Acceso	Lugar de almacenamiento
Consentimiento de particulares	Personal de laboratorio	Una vez escaneados se destruyen los originales
Consentimiento reconocimientos	Personal medicina	Una vez escaneados se destruyen los originales
Documentos de salud Radiografías	Médicos DUEs	Despachos médicos
Datos de trabajadores	Administrativo Dirección Administrativo SyS Asesoría Jurídica	Carpetas de Dirección bajo llave
Vídeos ergonomía	Técnicos de ergonomía	Se descargan en USB individuales. Cada Técnico la guarda bajo llave en sus armarios. Se trata de copias temporales.

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en lugar de acceso restringido (ver tabla) al que solo tendrán acceso las personas con autorización (ver tabla). La Delegada de Protección de Datos habilitará o retirará el permiso de acceso.

El archivo de los soportes o documentos se realizará garantizando la correcta conservación de los documentos, la localización y consulta de la información y posibilitarán el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

Los documentos incluidos en la Tabla anterior, se almacenarán de forma que se obstaculice su apertura. Cuando sus características físicas no permitan adoptar esta medida, el responsable adoptará medidas que impidan el acceso a la información de personas no autorizadas.

Los elementos de almacenamiento que dispongan de datos especialmente protegidos deberán encontrarse en lugares físicos que cuenten con acceso restringido (como llaves u otros dispositivos). Además estos

lugares permanecerán cerrados en tanto no sea preciso el acceso a los documentos. Si a la vista de las características de los locales no fuera posible cumplir lo anteriormente indicado, se adoptarán medidas alternativas tales como cajas de seguridad o armarios cerrados

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas.

Siempre que se proceda al traslado físico de la documentación con datos de protección de nivel alto, deberán adoptarse medidas orientadas a impedir el acceso o manipulación de la información cuando estos datos son trasladados. Únicamente están autorizados los traslados de información en ordenadores de Osarten, sujetos a la seguridad adecuada.

La realización de copias o reproducción de los documentos con datos personales sólo se podrán llevar a cabo bajo el control del siguiente personal autorizado: Médico y Directora de Laboratorio

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida. Para ello se utilizarán las destructoras de papel habilitadas o en el caso de que el volumen sea mayor se solicitará la destrucción a una empresa que garantice dicha destrucción.

13. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

13.1 Verificación

El Manual de Seguridad debe mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes, por ejemplo, en los sistemas de información o en la Entidad. Asimismo, el contenido del Manual de Seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

La Delegada de Protección de Datos y/o las personas designadas en las plantillas habilitadas al efecto, serán los encargados de velar por el correcto cumplimiento de los términos del presente Documento, así como los encargados de velar por la veracidad y exactitud de los términos y datos contenidos.

Por todo ello, se procederá a la realización de controles periódicos para comprobar el cumplimiento de los términos del presente Documento y, en su caso, poder detectar anomalías y proceder a su corrección.

Debe observarse cualquier cambio organizativo, procedimental y/o técnico en los Sistemas de Información de la Entidad, que pudiera afectar a la estructura y/o medidas de seguridad implementadas que se han definido en el presente documento.

13.2 Responsable de la actualización.

La Delegada de Protección de Datos es la encargada de coordinar y controlar las medidas definidas en el Documento de Seguridad.

13.3 Introducción de los cambios en el Documento de Seguridad.

El Manual de Seguridad se modificará siempre que se produzcan cambios significativos en:

- La propia la estructura de los tratamientos (cambio de finalidad, accesos por terceros, creación de nuevos ficheros, cambios significativos en los sistemas de información y en las aplicaciones, etc.).

- Las medidas de obligado cumplimiento del RGPD y LOPD
- Los cambios de organización (cambios departamentales, personal responsable, etc.).

13.4 Aprobación del Responsable del tratamiento.

La realización de una nueva versión actualizada del Documento de Seguridad, requerirá la aprobación del Responsable del tratamiento. Para ello, la Delegada de Protección de Datos le informará sobre los cambios en la organización, procedimentales y/o técnicos que afectarán a los datos y a los tratamientos, así como la forma en que se ha visto afectada el presente documento.