Osakidetza

ORGANIZACIÓN CENTRAL

Documento de Seguridad

Para la protección de los datos de carácter personal

Versión 6.01

Octubre 2015

Tabla de aprobación de la Versión Actual

Nombre	Organización	Cargo	Fecha
JON ETXEBERRIA CRUZ	OSAKIDETZA	Director General	15/10/2015
MARTÍN BEGOÑA OLEAGA	OSAKIDETZA	Responsable de Seguridad	15/10/2015

Versión Actual

Versión	06.01	F/Implantación	15/10/2015	F/Caducidad	14/10/2018

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Documento de Seguridad
02	20/06/2002	Documento de Seguridad
03	30/07/2002	Documento de Seguridad
04	30/04/2003	Documento de Seguridad
05	1/12/2004	Documento de Seguridad
06	17/06/2011	Documento de Seguridad

Cambios destacables (desde versión anterior)

- Actualización del Modelo Organizativo con la actual composición de la Comisión de Seguridad.
- Adecuación de las Funciones y Obligaciones del personal con acceso a DCP para referirlas no solo a personal interno sino también a posibles usuarios externos.
- Norma 10: Adecuar a la realidad actual de las medidas de seguridad en las comunicaciones
- Norma 40, Párrafo 2.7 sobre las preguntas para auto recuperar la contraseña por el propio usuario y Párrafo 3.1 sobre la TPE como medio de autenticación de identidad.
- Norma 50 se adapta el párrafo segundo a la redacción literal del artículo 103 RLOPD.
- Actualización de los Anexos finales.
- Procedimiento P010: autorrecuperación de contraseña; TPE; referencia a gestión de usuarios por el CAU; acceso remoto VPN.
- Procedimiento P030: enlace a política de copias de seguridad de SS.CC.
- Capítulo de Estándares de seguridad.

ÍNDICE

INTRODUCCIÓN

1. PROPÓSITO

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante LOPD), obliga al responsable del fichero, y, en su caso, al encargado del tratamiento, a adoptar 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, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana, del medio físico o natural. Añade que no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas; y remite a un Reglamento posterior el establecimiento de los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos protegidos (RLOPD 1720/2007).

El presente documento responde a la obligación establecida en el artículo 88 del Real Decreto 1720/2007 de 21 de diciembre en cuyo Título VIII se regulan las medidas de seguridad de los ficheros que contengan Datos de Carácter Personal. Por lo tanto en este documento se determinan los aspectos técnicos y organizativos que OSAKIDETZA debe cumplir en materia de seguridad de acuerdo al citado Real Decreto.

Asimismo la normativa también exige la estructuración de un equipo de personas articuladas orgánicamente que, de forma integrada y coordinada se responsabilicen, cada uno en su ámbito, de administrar, gestionar y controlar la seguridad de los ficheros que contengan Datos de Carácter Personal.

Además del presente capítulo de **Introducción**, el Documento de Seguridad está constituido por los siguientes contenidos:

- **Ámbito de Aplicación**, donde se describe cuál es el ámbito del documento, identificando y delimitando las instalaciones y sistemas de información a considerar. *(Se incluye en el presente texto).*
- **Directrices Generales de Seguridad,** donde se enumeran las directrices generales de seguridad que OSAKIDETZA debe considerar para regir sus actividades relacionadas con la seguridad de los ficheros con Datos de Carácter Personal. *(Se incluye en el presente texto).*
- **Organización de Seguridad y Funciones del Personal**, donde se estructura y define la organización que OSAKIDETZA precisa para garantizar la confidencialidad de todos los datos personales que maneja. *(Se incluye en el presente texto).*
- **Sistemas de Información y Estructura de Ficheros,** donde se identifican los Sistemas de Información que manejan Datos de Carácter Personal, inventariando los ficheros que contienen y el diseño de su estructura, e identificando y registrando la relación de perfiles de usuarios con permiso de acceso a su información. También se incluye la relación de ficheros notificados a la Agencia de Protección de Datos. *(No se incluye en el presente texto; la*

información sobre los sistemas de información y la estructura de los ficheros se mantiene registrada y actualizada en el sistema "Babeslebide").

- **Normativa**, donde se describe el contenido de las normas y medidas básicas diseñadas para dar cumplimiento a las exigencias legales e internas en cuanto se refiere a la seguridad de los Datos de Carácter Personal. *(Se incluye en el presente texto).*
- **Estándares,** donde se enumeran los artículos homologados en OSAKIDETZA al objeto de cumplir determinados aspectos contemplados por la legislación. *(Se incluye en el presente texto).*
- **Procedimientos**, donde se describen y definen los procesos básicos diseñados para dar cumplimiento a las exigencias legales e internas en cuanto se refiere a la seguridad de los Datos de Carácter Personal. *(No se incluye en el presente texto; los procedimientos están dispuestos en carpetas separadas, cada una de las cuales contiene la descripción, el esquema gráfico y los soportes documentales del procedimiento).*

2. DEFINICIONES Y GLOSARIO

CONCEPTOS BÁSICOS

Datos de Carácter Personal	Cualquier información (numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo) concerniente a personas físicas identificadas o identificables.
Persona identificable	Toda persona cuya identidad pueda determinarse directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.
Datos especialmente protegidos	Datos que se refieren a ideología, religión, creencias, afiliación sindical, origen racial, salud, vida sexual, datos recabados para fines policiales sin consentimiento de las personas afectadas y datos derivados de actos de violencia de género.
Fichero	Todo conjunto organizado de Datos de Carácter Personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.
Tratamiento de datos	Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
Persona afectada o interesada	Persona física a la que se refieren los datos que son objeto de tratamiento.
Procedimiento de disociación	Es un tratamiento de datos personales por el que se obtiene una información que no puede asociarse a una persona identificada o identificable.
Encargado del tratamiento	La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del Responsable del Fichero.
Consentimiento de la persona interesada	Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual, la persona interesada consiente el tratamiento de datos personales que le conciernen.
Cesión o comunicación de	Toda revelación de datos realizada a una persona distinta de la interesada.

datos

Persona destinataria o cesionaria	La persona física o jurídica, pública o privada, u órgano administrativo, al que se revelen los datos. En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará tercera a la persona o personas integrantes de los mismos.
Tercero	La persona física o jurídica, autoridad pública o privada, u órgano administrativo, distinta de la persona afectada o interesada, de la Responsable interna del Fichero, de la Encargada del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa de la persona Responsable del Fichero o de la Encargada del tratamiento. En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará tercera a la persona o personas integrantes de los mismos.
Fuentes accesibles al público	Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

CONCEPTOS RELACIONADOS CON LAS MEDIDAS DE SEGURIDAD

Sistema de información	Conjunto de ficheros, programas, soportes y equipos empleados para el almacenamiento y tratamiento de Datos de Carácter Personal.
Usuario/a	Persona o proceso autorizado para acceder a datos o recursos.
Recurso	Cualquier parte componente de un sistema de información.
Accesos autorizados	Autorizaciones concedidas a una persona usuaria para la utilización de los diversos recursos.
Identificación	Procedimiento de reconocimiento de la identidad de una persona usuaria.
Autenticación	Procedimiento de comprobación de la identidad de una persona usuaria.
Control de acceso	Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Contraseña	Información confidencial, frecuentemente constituida por una cadena de caracteres que puede ser usada en la autenticación de una persona usuaria.
Incidencia	Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
Bloqueo	La identificación y reserva de Datos de Carácter Personal con el fin de impedir su tratamiento excepto por parte de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades.
Borrado o supresión	La eliminación física de los Datos de Carácter Personal bloqueados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento de dichos datos.
Soporte automatizado	Aquel elemento físico que contenga información automatizada (por ejemplo, CDs, DVDs, cintas de backup, pendrives,…).
Soporte no automatizado	En relación a ficheros o tratamientos no automatizados, elementos contenedores de documentos en papel (por ejemplo, carpetas tipo A-Z, cajas,…)
Documentos en papel o documentación no automatizada	Aquellos, expedientes, escritos, o elementos similares que contengan datos y que están contenidos en soportes no automatizados

GLOSARIO DE TÉRMINOS

AEPD	Agencia Española de Protección de Datos
AVPD	Agencia Vasca de Protección de Datos
Babeslebide	Sistema de información mediante el que se gestionan los registros, documentos y procedimientos relacionados con el cumplimiento de la LOPD.
CPD	Centro de Proceso de Datos
DCP	Datos de Carácter Personal
DS	Documento de Seguridad
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal

Equipo informático	Terminales, ordenadores personales (tanto de sobremesa como portátiles), impresoras, etc. mediante los que se tratan los datos
ET	Encargado del Tratamiento
PC	Ordenador Personal (en inglés, *Personal Computer*)
OOSS	Organizaciones de Servicios
RLOPD	Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la LOPD
RS	Responsable de Seguridad
RSOS	Responsable de Seguridad de la Organización de Servicios
SO	Sistema Operativo
Soporte	Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos (discos duros, CD, disquetes, cintas, discos de los ordenadores portátiles, *pendrives* o memorias-*flash*, etc.)
SSII	Sistemas de Información
TPE	Tarjeta Profesional Electrónica

ÁMBITO DE APLICACIÓN

En este capítulo se indica el ámbito de aplicación del presente Documento, centrado en las instalaciones, Plataformas Tecnológicas, Sistemas de Información y Archivos de Documentación que almacenan y tratan datos de carácter personal.

La protección efectiva de los datos de carácter personal frente a tratamientos o accesos no autorizados, alteración o pérdida se deberá realizar mediante el control de todas las vías por las que se pueda tener acceso a dicha información.

Así, los recursos que sirven de medio directo o indirecto para acceder a los ficheros con DCP, y que, por tanto, deberán ser controlados por lo dispuesto en el Documento de Seguridad son:

- Las instalaciones o centros de tratamiento y locales donde se encuentran ubicados los ficheros y se almacenan los soportes que los contengan. Su descripción figura en el ANEXO 1.

- Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos, aparecen descritos en el ANEXO 2.

- Los servidores, y el entorno de sistema operativo y de comunicaciones tanto locales como externas en el que se encuentran ubicados los ficheros, se encuentran descritos en el ANEXO 3.

- Los archivos de documentación e información no automatizada, los cuales se encuentran descritos en el ANEXO 4.

- Los sistemas, ya sean automatizados, manuales o mixtos, establecidos para acceder a los datos.

DIRECTRICES GENERALES DE SEGURIDAD

Al objeto de implementar una solución que garantice la seguridad (confidencialidad, integridad y disponibilidad) de los Datos de Carácter Personal en OSAKIDETZA, este capítulo define las directrices básicas que se deben contemplar en lo que respecta a esta materia:

1. Constituir una Comisión de Seguridad que se establezca como máximo organismo consultivo y de apoyo en la toma de decisiones en materia de seguridad de la Información, para todos los centros de OSAKIDETZA.

2. Establecer una Organización de Seguridad que identifique, notifique (a la Agencia Vasca de Protección de Datos) y se responsabilice de los ficheros afectados por la LOPD. También se incluye dentro de su responsabilidad la definición, implementación y cumplimiento de los procedimientos de seguridad que precise OSAKIDETZA.

3. Elaborar y mantener actualizado el Documento de Seguridad adecuándolo a las necesidades de OSAKIDETZA y cumpliendo las medidas establecidas en la LOPD vigente e incluyendo las normas y procedimientos a aplicar.

4. Actualizar los Sistemas de Información y archivos de documentación para que adopten los estándares, medidas y procedimientos que se hayan definido en el presente Documento de Seguridad.

5. Difundir entre el personal de OSAKIDETZA que maneje Datos de Carácter Personal, las medidas de seguridad que deben observar para asegurar la integridad y confidencialidad de la información que tratan.

ORGANIZACIÓN DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

Este capítulo define la Organización de Seguridad implementada en OSAKIDETZA para garantizar la seguridad de los Datos de Carácter Personal soportados en ficheros automatizados y no automatizados.

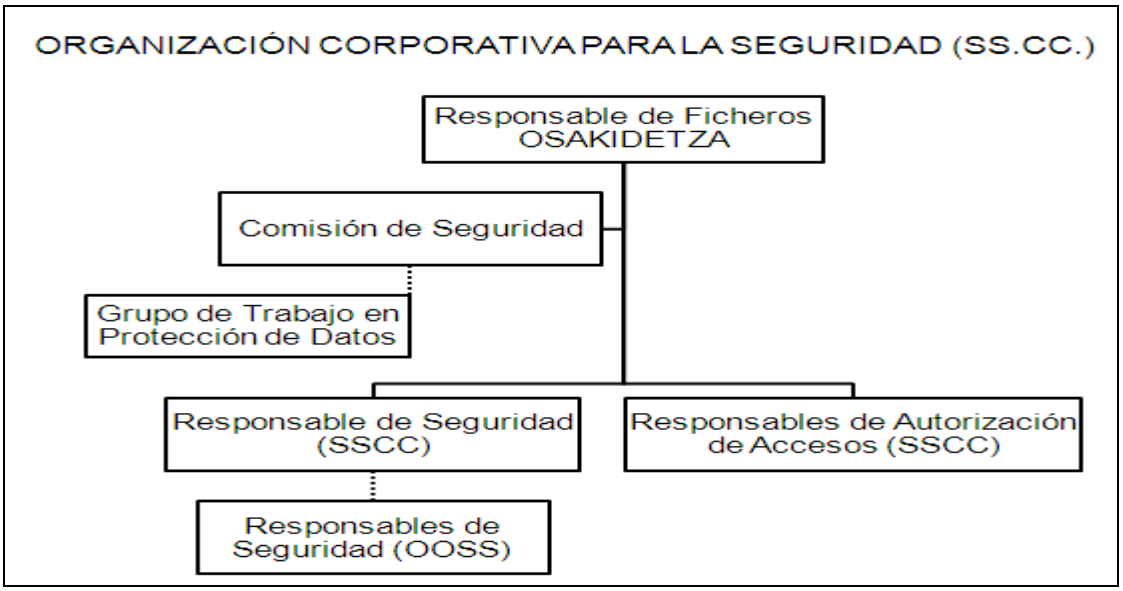
En un primer apartado, se representa el Modelo Organizativo de Seguridad, identificando y mostrando las unidades implicadas y la dependencia jerárquica o funcional existente entre ellas.

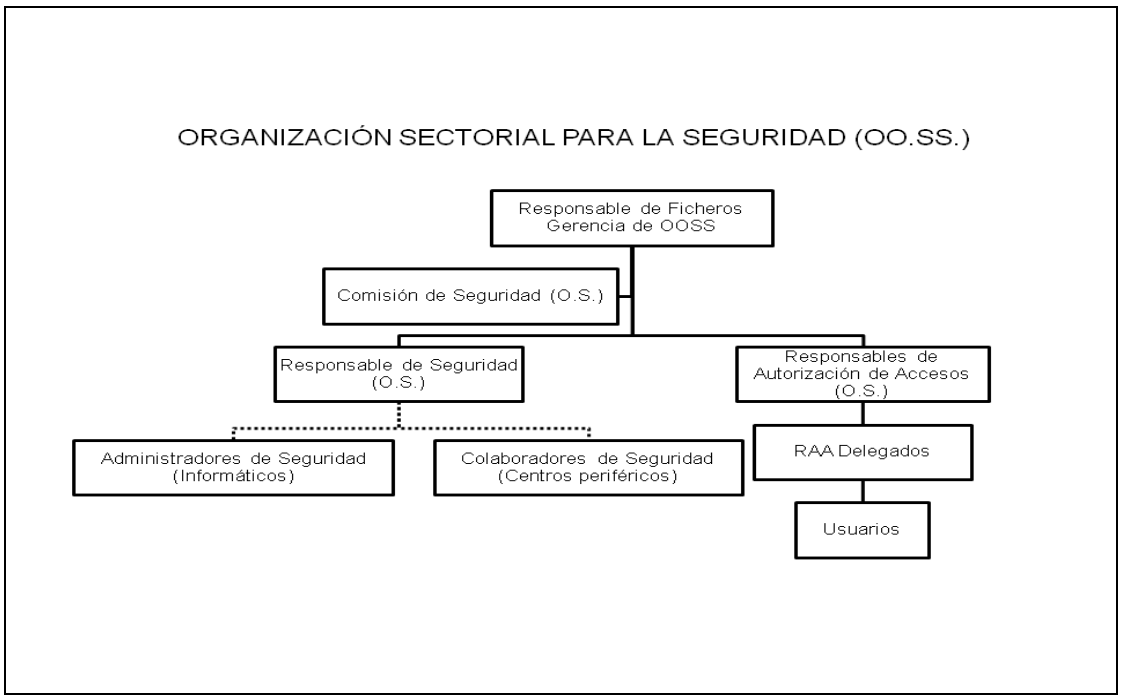
En un segundo apartado, se enumeran las funciones del personal adscrito a cada una de las unidades identificadas en el Modelo Organizativo.

Finalmente, con carácter general, se definen las funciones y obligaciones del personal con acceso a los Datos de Carácter Personal.

1. MODELO ORGANIZATIVO DE SEGURIDAD

Los siguientes organigramas recogen la representación gráfica y simplificada de la estructura de seguridad para gestionar y controlar la seguridad de los Datos de Carácter Personal en OSAKIDETZA. En ellos se representan las unidades Responsables involucradas en la organización de seguridad y las relaciones jerárquicas o funcionales existentes entre las mismas.





El modelo organizativo, recogido en el presente Documento de Seguridad, se establece siguiendo los criterios de la Instrucción General nº 02 del año 2003, adaptándose a los nuevos requerimientos derivados del RLOPD.

Seguidamente, se define cada una de las unidades representadas en el modelo gráfico:

RESPONSABLE DE FICHEROS

OSAKIDETZA, entidad con personalidad jurídica propia, se erige como Responsable último de todos los ficheros que contengan Datos de Carácter Personal en sus instalaciones, de acuerdo con la definición legal del artículo 3 d) de la LOPD.

Cada fichero con datos de carácter personal de OSAKIDETZA, estará adscrito a:

1. un órgano con rango de Dirección de División, o al órgano de Dirección General, en caso de ser común a varias Divisiones, si su ámbito de funcionamiento fuese corporativo; o bien,

2. al órgano de Dirección-Gerencia de la Organización de Servicios que corresponda, si su ámbito de funcionamiento fuese sectorial (específico de la Organización de Servicios).

Esta adscripción de cada fichero al órganos directivo correspondiente se realizará considerando precisamente las funciones que dicho órgano tiene atribuidas y para cuyo mejor ejercicio se han recogido los datos que se contienen en el mismo.

El órgano directivo al que se adscriba cada fichero será el garante de la implementación práctica de las normas, procedimientos y medidas de seguridad concretas contenidas en este Documento.

La realización de las tareas operativas relacionadas con la seguridad de los datos de carácter personal que corresponden al Responsable de los Ficheros se delega en las siguientes figuras:

- Comisión de Seguridad de SS.CC.
- Grupo de Trabajo en Protección de Datos
- Responsable de Seguridad de SS.CC.
- Responsables de Autorización de Accesos de SS.CC.
- Comisiones de Seguridad de las OO.SS.
- Responsables de Seguridad de las OO.SS. (y sus Colaboradores en Centros periféricos)
- Responsables de Autorización de Accesos de las OO.SS. (y sus Delegados)

Esta delegación de actividades no supone en ningún caso una exoneración de las responsabilidades, que en materia de seguridad de Datos de Carácter Personal corresponden legalmente a OSAKIDETZA.

COMISIÓN DE SEGURIDAD DE SS.CC.

La Comisión de Seguridad de SS.CC. se establece en OSAKIDETZA como máximo órgano consultivo y de apoyo a las diversas direcciones y subdirecciones de la organización, en la toma de las decisiones referidas a la seguridad de la información y a la protección de datos.

En el ejercicio de sus competencias, esta Comisión actúa por delegación y con el respaldo manifiesto de la Dirección General, máxima representación del Ente Público en su calidad de Responsable de los Ficheros que contengan datos de carácter personal, así como de las diversas Direcciones a las que se adscriben dichos ficheros, en su calidad de órganos internos responsables de los mismos.

Realizará reuniones **con una periodicidad que como mínimo será semestral**, así como cada vez que sea necesario valorar una decisión importante en materia de seguridad. Como fechas orientativas para las reuniones ordinarias se considerarán: 15 de abril y 15 de octubre.

El organigrama de esta Comisión de Seguridad de SS.CC. se define, y se actualiza cuando sea necesario, mediante Acuerdo del Consejo de Administración de OSAKIDETZA. Consta de los siguientes miembros, con carácter permanente:

- Presidente: El Responsable de Seguridad de SS.CC.
- Secretario o Secretaria: Titular de la Subdirección de Asesoría Jurídica.
- Vocales:
    - Titulares de las Subdirecciones de la Organización Central.
    - Un o una profesional de la Subdirección de Sistemas de Información.
    - Un letrado o letrada de la Subdirección de Asesoría Jurídica.

Además, se podrán incorporar temporalmente otras personas para tratar temas de seguridad o protección de datos a requerimiento de la Comisión permanente.

Se incorporan(n) en Babeslebide la(s) Resolución(es) con los nombramientos correspondientes.

GRUPO DE TRABAJO EN PROTECCIÓN DE DATOS

Para facilitar el funcionamiento del Modelo Organizativo de Seguridad, se articula el **Grupo de Trabajo en Protección de Datos**, como un subconjunto delegado de la Comisión de Seguridad, el cual permanece activo, manteniendo al día el sistema de protección de datos, y que se conforma según se describe a continuación:

- Un técnico de la Subdirección de Asesoría Jurídica de SSCC.
- Un técnico de la Subdirección de Sistemas de Información de SSCC.
- Cuando resulte necesario, una empresa externa especializada en materia de Protección de Datos, que proveerá los servicios de consultoría y asesoría.
- Cuando resulte necesario, los Responsables de Seguridad de las Organizaciones de Servicios, agrupados por territorio histórico (Araba, Bizkaia y Gipuzkoa)

Se incorporan(n) en Babeslebide la(s) Resolución(es) con los nombramientos correspondientes.

COMISIONES DE SEGURIDAD DE LAS OO.SS.

La Comisión de Seguridad de la OO.SS. se establece en cada Organización de Servicios como máximo órgano consultivo y de apoyo a las diversas direcciones y subdirecciones de la misma, en la toma de las decisiones referidas a la seguridad de la información y a la protección de datos.

Realizará reuniones con la periodicidad que se establezca en cada Organización de Servicios, que como mínimo será semestral, así como cada vez que sea necesario valorar una decisión importante en materia de seguridad.

Estará formada, con carácter permanente, por todos los componentes del Equipo Directivo de la Organización de Servicios y el Responsable de Seguridad de dicha Organización de Servicios.

Además, se podrán incorporar temporalmente otras personas para tratar temas de seguridad o protección de datos a requerimiento de la Comisión permanente.

Las directrices, políticas y procedimientos de seguridad afectan a toda la organización y por ello conviene que cuente con el apoyo y las sugerencias de los diferentes niveles administrativos de la Organización de Servicios. Es aconsejable que esta Comisión de Seguridad tenga en cuenta las consideraciones de todos los usuarios con acceso a Datos de Carácter Personal, por lo que se recomienda articular mecanismos que posibiliten las sugerencias y comentarios de los usuarios respecto a la seguridad de los datos de carácter personal.

Se incorporan(n) en Babeslebide la(s) Resolución(es) con los nombramientos correspondientes.

RESPONSABLE DE SEGURIDAD DE SS.CC.

Esta unidad se erige como coordinadora única de las tareas y actividades que en materia de seguridad se realicen en OSAKIDETZA. Asimismo, se responsabiliza de la definición, implantación y supervisión de las normas y procedimientos que afecten a todos los ficheros que contengan Datos de Carácter Personal.

Para el desempeño de las funciones propias de esta unidad, OSAKIDETZA designa al titular de la Subdirección de Informática y Sistemas de Información como Responsable de Seguridad.

Contará, en el resto de las OO.SS. de OSAKIDETZA, con la colaboración de los Responsables de Seguridad de dichas OO.SS., los cuales actuarán bajo su supervisión y coordinación, en cuanto se refiera a la seguridad de la información.

En la Organización Central de OSAKIDETZA, para la implementación de la seguridad técnica, se apoyará en la Subdirección de Informática y SS.II.

Se incorporan(n) en Babeslebide la(s) Resolución(es) con los nombramientos correspondientes.

RESPONSABLES DE SEGURIDAD DE LAS OO.SS.

Personas designadas formalmente como Responsables de Seguridad de las OO.SS. por OSAKIDETZA en su calidad de Responsable de Ficheros, en consenso con el Gerente de cada Organización de Servicios.

Funcionalmente, actuarán coordinados por el Responsable de Seguridad de SS.CC. de OSAKIDETZA.

Esta figura se erige como coordinadora de las tareas y actividades que en materia de seguridad de la información se realicen en el ámbito de su Organización de Servicios.

Como Responsables de Seguridad de OO.SS. se dispone que lo sean las Subdirecciones / Responsables de Informática de las OO.SS.. En caso de que la Organización de Servicios carezca de estas figuras, el Responsable de Autorización de Accesos de mayor rango asumirá las funciones del Responsable de Seguridad.

Se incorporan(n) en Babeslebide la(s) Resolución(es) con los nombramientos correspondientes.

COLABORADORES DE SEGURIDAD EN CENTROS PERIFÉRICOS

La finalidad de esta figura es la de hacer más operativa y eficaz la función de los Responsables de Seguridad. En su funcionamiento, actuarán precisamente por delegación de estos últimos.

Considerando las dimensiones, localización geográfica y complejidad organizativa de cada caso concreto, las Gerencias y las Direcciones o Subdirecciones de las organizaciones, determinarán la necesidad de atribuir esta responsabilidad a la persona que designe la Gerencia de la Organización de Servicios.

Se incorporan(n) en Babeslebide la(s) Resolución(es) con los nombramientos correspondientes.

ENCARGADOS DE TRATAMIENTO

OSAKIDETZA puede tener encargados de tratamiento sobre sus ficheros propios, lo que ocurrirá siempre que terceras entidades prestadoras de servicios accedan a datos de carácter personal de los ficheros de OSAKIDETZA al objeto de prestarle dichos servicios. En estos casos, ambas entidades deben suscribir un contrato que contenga los requisitos contemplados en la LOPD.

RESPONSABLES DE AUTORIZACIONES DE ACCESOS (EN SS.CC. Y OO.SS.)

La figura de Responsable de Autorización de Accesos es la persona encargada de decidir en los aspectos operativos de los Sistemas de Información, desde el punto de vista funcional de los servicios.

Estas figuras actuarán por delegación de OSAKIDETZA, como Responsable de Ficheros.

En Servicios Centrales, las personas de OSAKIDETZA que desempeñan esta función son básicamente las personas Responsables de la gestión del servicio involucrado; para el resto de las Organizaciones de Servicios, esta responsabilidad recae en las Direcciones o Subdirecciones funcionales de cada una de ellas (Dirección Médica, Dirección de Enfermería, Dirección de RR.HH., Dirección Económico-Financiera, etc.) tanto en los Centros Hospitalarios, como en los Centros de Atención Primaria.

Los Gerentes de las OO.SS. como responsables y coordinadores últimos en el ámbito de su propio centro, deberán designar a los Responsables de Autorización de Accesos de las OO.SS.

De forma general, es válido que esta responsabilidad se atribuya a la Dirección o Subdirección “propietaria” del proceso en que se manejan los datos de carácter personal.

Se incorporan(n) en Babeslebide la(s) Resolución(es) con los nombramientos correspondientes.

DELEGADO DEL RESPONSABLE DE AUTORIZACIONES DE ACCESOS

La finalidad de esta figura es la de hacer más operativa y eficaz la función de los Responsables de Autorizaciones de Acceso. En su funcionamiento, actuarán precisamente por delegación de estos últimos.

Considerando las dimensiones, localización geográfica y complejidad organizativa de cada caso concreto, las Gerencias y las Direcciones o Subdirecciones de las organizaciones, determinarán la necesidad de atribuir esta responsabilidad a las Jefaturas de Servicios correspondientes.

Se incorporan(n) en Babeslebide la(s) Resolución(es) con los nombramientos correspondientes.

ADMINISTRADORES DE SEGURIDAD

El Administrador de Seguridad es la persona encargada de aplicar operativamente los procedimientos de control de acuerdo con el Responsable de Seguridad y el Responsable de Autorización de Accesos, para garantizar la integridad y la confidencialidad de los Datos de Carácter Personal.

Generalmente sus funciones son realizadas dentro de las Unidades Informáticas por los Administradores de Redes, de Bases de Datos, de Aplicaciones, etc.

En definitiva, se trata del personal que se ocupa de activar y desactivar los permisos de acceso a los datos, ejecutando las instrucciones dadas por los Responsables de Autorización de Accesos, con el visto bueno del Responsable de Seguridad.

Este personal está explícitamente relacionado, ya que debido a sus funciones puede utilizar herramientas de administración que permiten el acceso a los datos protegidos obviando los controles de acceso de las aplicaciones.

Se incorporan(n) en Babeslebide la(s) Resolución(es) con los nombramientos correspondientes.

DEPOSITARIOS DE LA INFORMACIÓN

Esta figura se responsabilizará de custodiar los datos y de garantizar su disponibilidad de acuerdo con las especificaciones establecidas.

Normalmente sus funciones son desempeñadas por las Unidades de Explotación de los Centros de Proceso de Datos.

USUARIOS

Personas que, en el desempeño de sus funciones, tratan o tienen acceso a los datos de carácter personal cuya responsabilidad corresponde a OSAKIDETZA.

Dichos usuarios están obligados a respetar las normas y procedimientos contenidos en el presente Documento.

2. FUNCIONES DE LAS UNIDADES DE LA ORGANIZACIÓN DE SEGURIDAD

Seguidamente se definen las funciones a desarrollar por cada una de las unidades de la organización de seguridad anteriormente descrita[1].

Si fuese necesario, el personal asignado a las unidades de Seguridad desempeñará las funciones enumeradas de forma complementaria y compartida con las tareas que conlleve el ejercicio habitual de su trabajo en OSAKIDETZA.

RESPONSABLE DE FICHEROS

Dado que la responsabilidad de esta unidad recae en una persona jurídica: OSAKIDETZA, las funciones operativas de la misma son asumidas y realizadas de forma delegada por las figuras de los Responsables de Seguridad, los Responsables de Autorización de Accesos y las Comisiones de Seguridad.

A continuación se describen las funciones de dichas unidades.

COMISIÓN DE SEGURIDAD DE SS.CC.

Su ámbito de actuación es corporativo, y sus funciones, en dicho ámbito son:

- Definición de Estrategias de Seguridad.
- Articulación de Normativas de Seguridad.
- Aprobación de los Documentos de Seguridad que se elaboren.
- Revisión de los informes de auditoría que en materia de seguridad se emitan periódicamente.
- Revisión de los informes de verificación del correcto cumplimiento de lo dispuesto en el Documento de Seguridad que periódicamente emita el Responsable de Seguridad.

[1] Las funciones de algunas de las unidades indicadas anteriormente no figuran en la relación subsiguiente (Responsables de Autorización de Accesos Delegados, Colaboradores de Seguridad en Centros Periféricos, Administradores de Seguridad, Depositarios de la Información y Usuarios) ya que se sobreentiende que actuarán por delegación de las otras figuras o bien siguiendo las instrucciones que éstas emitan.

- Análisis de los informes explicativos de aquellas incidencias que afecten de manera grave a los Sistemas de Información que emita el Responsable de Seguridad.
- Seguimiento de los diferentes Planes de Seguridad que se definan.
- Coordinación de acciones en materia de seguridad, con el Responsable de Seguridad, a quien se atribuye el control y supervisión de dichas actividades.
- Tratar cualquier otro tema que se considere de interés en materia de seguridad.
- Aprobación de los Informes de control elaborados por el Responsable de Seguridad.

COMISIONES DE SEGURIDAD DE LAS OO.SS.

Su ámbito de actuación es sectorial y específico de cada Organización de Servicios, y sus funciones, en dicho ámbito, siempre y cuando no entren en conflicto con las de la Comisión de Seguridad de SS.CC., son:

- Valoración de las decisiones a tomar, en materia de seguridad de la información y protección de datos, en su Organización de Servicios. En última instancia, la decisión es competencia de la Gerencia de dicha Organización.
- Aprobación del Documento de Seguridad que se elabore.
- Revisión de los informes de auditoría que en materia de seguridad se emitan periódicamente.
- Revisión de los informes de verificación del correcto cumplimiento de lo dispuesto en el Documento de Seguridad que periódicamente emita el Responsable de Seguridad.
- Análisis de los informes explicativos de aquellas incidencias que afecten de manera grave a los Sistemas de Información que emita el Responsable de Seguridad.
- Seguimiento de los diferentes Planes de Seguridad que se definan.
- Coordinación de acciones en materia de seguridad, con el Responsable de Seguridad, a quien se atribuye el control y supervisión de dichas actividades.
- Tratar cualquier otro tema que se considere de interés en materia de seguridad.
- Aprobación de los Informes de control elaborados por los Responsables de Seguridad.

RESPONSABLE DE SEGURIDAD DE SS.CC.

Su **ámbito de actuación es corporativo**, y sus funciones, en dicho ámbito son:

Como coordinador de tareas y actividades en materia de seguridad:

- Notificar para su inscripción en el registro de la Agencia Española de Protección de Datos (y, en su caso, la Agencia Vasca de Protección de Datos) la creación, modificación y cancelación de ficheros que contengan Datos de Carácter Personal.
- Elaborar e implantar el Documento de Seguridad de los ficheros afectados por la LOPD, así como mantenerlo actualizado.
- Analizar los informes de Auditoría que periódicamente se realicen y adoptar las medidas que sean necesarias para solventar las deficiencias detectadas.
- Definir y establecer las normas y procedimientos que en materia de seguridad afecten a los ficheros y/o tratamientos automatizados y no automatizados.
- Coordinar, controlar y supervisar las actividades relacionadas con los ficheros y tratamientos automatizados y no automatizados en materia de seguridad.

Como Responsable de Seguridad en el ámbito de actuación corporativo:

1. Funciones para **tratamientos automatizados y no automatizados**

- Supervisar y analizar de forma periódica las incidencias acaecidas en los centros, relacionadas con la seguridad de los ficheros automatizados y no automatizados.
- Elaborar un informe explicativo de aquellas incidencias que afecten de manera grave a los sistemas de seguridad de OSAKIDETZA.
- Establecer medidas cuya aplicación aminore y/o elimine las incidencias acaecidas.
- En colaboración con el Responsable de Autorización de Accesos, adoptar las medidas oportunas para que el personal usuario de OSAKIDETZA conozca las normas de seguridad que afectan al desarrollo de sus funciones y las consecuencias en que puede incurrir en caso de incumplimiento.
- Estar informado de los cambios que pudieran producirse en la normativa de protección de datos de carácter personal y proponer las medidas de adecuación a los mismos.

- Establecer mecanismos que eviten que un usuario pueda acceder a información o recursos con derechos distintos a los autorizados.

- Realizar los controles periódicos para la verificación de lo dispuesto en el Documento de Seguridad.

2. Funciones en relación con el **tratamiento automatizado** de datos de carácter personal

- Mantener actualizado el registro de usuarios con acceso autorizado a los Sistemas de Información que contengan Datos de Carácter Personal, en relación al tratamiento automatizado de datos.

- Revisar periódicamente la información de control registrada sobre los accesos de los usuarios a los Sistemas de Información y elaborar al menos una vez al mes, un informe de las revisiones realizadas y los problemas detectados.

- Verificar la definición y aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos.

3. Funciones en relación con el **tratamiento no automatizado** de datos de carácter personal

- Mantener actualizado el registro de usuarios con acceso autorizado a los Archivos que contengan Datos de Carácter Personal, en relación al tratamiento no automatizado de datos.

- Verificar que la información contenida en el Registro de Accesos al Archivo permita identificar los accesos realizados a la documentación no automatizada de nivel alto.

- Supervisar las medidas que se adoptan en el traslado de documentación no automatizada y, en particular, en el traslado de documentación no automatizada de nivel alto.

RESPONSABLES DE SEGURIDAD DE LAS OO.SS.

Las funciones realizadas por estas figuras podrán ser llevadas a cabo por una o varias personas, es decir, por una persona para el tratamiento automatizado de datos y por otra para el tratamiento no automatizado de datos.

Su **ámbito de actuación es sectorial**, es decir, se circunscribe a su OOSS y sus funciones son:

Como colaborador del Responsable de Seguridad de SSCC:

- Colaborar con el Responsable de Seguridad de SS.CC. en todas aquellas cuestiones que afecten a la seguridad de la información en el ámbito de su Organización de Servicios.
- Aplicar, divulgar, verificar y realizar el seguimiento de las directrices generales de seguridad de la información.
- Elaborar los informes periódicos de situación que se determinen.
- Solicitar la actualización del Documento de Seguridad cuando las circunstancias lo requieran.
- Colaborar en las auditorías de seguridad relacionadas con el Reglamento de Desarrollo de la LOPD (R.D. 1720/2007).

Como Responsable de Seguridad en el ámbito de actuación sectorial:

1. Funciones para **tratamientos automatizados y no automatizados**

- Supervisar y analizar de forma periódica las incidencias acaecidas en los centros, relacionadas con la seguridad de los ficheros y tratamientos automatizados y no automatizados.
- Elaborar un informe explicativo de aquellas incidencias que afecten de manera grave a los sistemas de seguridad de OSAKIDETZA.
- Establecer medidas cuya aplicación aminore y/o elimine las incidencias acaecidas.
- En colaboración con el Responsable de Autorización de Accesos, adoptar las medidas oportunas para que el personal usuario de OSAKIDETZA conozca las normas de seguridad que afectan al desarrollo de sus funciones y las consecuencias en que puede incurrir en caso de incumplimiento.
- Estar informado de los cambios que pudieran producirse en la normativa de protección de datos de carácter personal y proponer las medidas de adecuación a los mismos.
- Establecer mecanismos que eviten que un usuario pueda acceder a información o recursos con derechos distintos a los autorizados.
- Realizar los controles periódicos para la verificación de lo dispuesto en el Documento de Seguridad.

2. Funciones en relación con el **tratamiento automatizado** de datos de carácter personal

- Mantener actualizado el registro de usuarios con acceso autorizado a los Sistemas de Información que contengan Datos de Carácter Personal, en relación al tratamiento automatizado de datos.

- Revisar periódicamente la información de control registrada sobre los accesos de los usuarios a los Sistemas de Información y elaborar al menos una vez al mes, un informe de las revisiones realizadas y los problemas detectados.

- Verificar la definición y aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos.

3. Funciones en relación con el **tratamiento no automatizado** de datos de carácter personal

- Mantener actualizado el registro de usuarios con acceso autorizado a los Archivos que contengan Datos de Carácter Personal, en relación al tratamiento no automatizado de datos.

- Verificar que la información contenida en el Registro de Accesos al Archivo permita identificar los accesos realizados a la documentación no automatizada de nivel alto.

- Supervisar las medidas que se adoptan en el traslado de documentación no automatizada y, en particular, en el traslado de documentación no automatizada de nivel alto.

ENCARGADOS DE TRATAMIENTO

A los Encargados de Tratamiento se le encomiendan todas las funciones definidas y recogidas en los correspondientes contratos que les vinculen con OSAKIDETZA.

RESPONSABLES DE AUTORIZACIONES DE ACCESOS (EN SS.CC. Y OO.SS.)

En el ámbito de sus atribuciones:

- Conceder o denegar a los usuarios la autorización de acceso a los Sistemas de Información.

- Aprobar por escrito la recuperación de datos desde copias de respaldo que requiera la utilización de procesos específicos no planificados.

- Autorizar la salida de soportes informáticos que contengan Datos de Carácter Personal.
- En colaboración con el Responsable de Seguridad, adoptar las medidas oportunas para que el personal usuario de OSAKIDETZA conozca las normas de seguridad que afectan al desarrollo de sus funciones y las consecuencias en que pueden incurrir en caso de incumplimiento.

3. FUNCIONES Y OBLIGACIONES DEL PERSONAL CON ACCESO A DATOS DE CARÁCTER PERSONAL

El personal de OSAKIDETZA en el ejercicio de las funciones que tiene atribuidas y, en su caso cualquier usuario que acceda a Datos de Carácter Personal, deberá cumplir con las siguientes normas, en lo que respecta al manejo de Datos de Carácter Personal:

EQUIPO INFORMÁTICO DEL USUARIO

- Proteger, en la medida de sus posibilidades, la confidencialidad de los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o cualquier otra manipulación o uso indebido, cualquiera que sea el soporte en que se encuentren contenidos los datos.

- Garantizar que la información que se muestra en el mismo durante su utilización no pueda ser visible por personas no autorizadas, bien sea este uso permanente u ocasional. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al equipo informático del usuario deberán, de manera preferente y siempre que sea posible, estar físicamente ubicados en lugares que garanticen esa confidencialidad.

- Cuando el usuario abandone temporalmente el equipo informático, deberá dejarlo en un estado que impida la visión de los datos protegidos. En su caso, si el abandono del equipo se produjera debido a la finalización de su turno de trabajo, el usuario procederá al cierre completo de la sesión del sistema. En caso de no ser posible el apagado del equipo, por hallarse el mismo realizando algún proceso de larga duración, deberá dejarse en un estado que impida asimismo la visión de los datos protegidos.

- Evitar mantener ficheros con datos de carácter personal en los discos locales de los equipos informáticos. En su caso, se contactará con el Responsable de Seguridad de OSAKIDETZA pertinente, quien determinará en qué zona protegida del servidor serán ubicados dichos ficheros. Sólo en el caso de que fuese imprescindible, se permitirá mantener los ficheros con datos de carácter personal en los discos locales de los equipos informáticos, en cuyo caso se aplicarán las medidas de seguridad que reglamentariamente correspondan.

- Los ficheros individuales con datos de carácter personal en ficheros ofimáticos, ubicados en los ordenadores personales de los usuarios, deben someterse a las mismas medidas de seguridad que los ficheros corporativos. Asimismo, si procediere, deberán ser declarados a la AEPD (y/o a la AVPD) y registrados en el Documento de Seguridad. Estas acciones, en su caso, serán coordinadas con el Responsable de Seguridad de OSAKIDETZA pertinente.

- La protección y el uso de los ordenadores personales y los ordenadores portátiles son responsabilidad de las personas a las que se entreguen.

USO APROPIADO DE RECURSOS

Los recursos informáticos y de comunicaciones propios de Osakidetza, a los que el usuario tiene acceso, únicamente están disponibles para el cumplimiento de sus funciones en el desempeño de su trabajo.

Por este motivo, el usuario viene obligado a, en su caso:

- Utilizar los programas antivirus y sus actualizaciones, poniendo la diligencia necesaria para proteger los sistemas de información contra accesos y usos no autorizados y evitar la destrucción o cualquier otro perjuicio a la información que maneja.

- Utilizar únicamente las versiones de software facilitadas por OSAKIDETZA o proveedor debidamente autorizado, siempre siguiendo sus normas de utilización. En ningún caso podrán instalar copias ilegales o irregulares de programas, ni borrar ninguno de los programas instalados legalmente.

- Sólo se introducirán datos identificativos y direcciones de personas en las agendas de contactos de las herramientas ofimáticas (por ejemplo Outlook).

A tal fin quedan prohibidos:

- El uso de los recursos para actividades no relacionadas con las funciones propias de cada usuario.

- Las actividades, equipos o aplicaciones no autorizadas por OSAKIDETZA.

- Introducir en los sistemas de información o la red corporativa contenidos comprometedores para OSAKIDETZA. Estos son contenidos obscenos, amenazadores, inmorales u ofensivos, pero caben también otras posibilidades.

- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX, sniffers, crackeadores o cualquier otro dispositivo lógico o físico que cause o pueda causar cualquier alteración o daño a los SSII o robo de información.

- Intentar destruir, alterar o inutilizar de cualquier otra forma los recursos de OSAKIDETZA.

- Intentar distorsionar o falsear los registros de actividad (log) de los SSII.

RECURSOS DE RED

Los usuarios son responsables, con carácter general, de asegurar que los datos, las aplicaciones y demás recursos informáticos puestos a su disposición, sean usados únicamente para el desarrollo de la operativa propia para la que fueron creados e implantados.

Ninguna persona con acceso a los SSII debe:

- Conectar, a ninguno de los recursos informáticos, ningún tipo de equipo de comunicaciones que posibilite la conexión a la red corporativa, sin la oportuna autorización.

- Conectarse a la red corporativa a través de otros medios que no sean los definidos y administrados por OSAKIDETZA, sin perjuicio de lo dispuesto en la normativa que sea de aplicación.

- Intentar acceder a áreas restringidas de los sistemas de información propios o de terceros, ni otros accesos distintos a aquellos que les hayan sido asignados.

- Intentar descifrar claves, sistemas o algoritmos de cifrado o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar cualquiera de los recursos informáticos.

IDENTIFICACIÓN Y AUTENTICACIÓN

El usuario, en el acceso a los sistemas de información, deberá disponer de un acceso autorizado, por regla general, en virtud de identificador de usuario y contraseña, sobre el que deberá observar las siguientes normas de actuación:

- No deberá revelar, bajo ningún concepto, su acceso autorizado, por lo que evitará teclear la contraseña en presencia de terceros, así como mantenerla por escrito a la vista o al alcance de éstos. El usuario será responsable de toda actividad relacionada con el uso de su acceso autorizado.

- Cambiar la contraseña si se sospecha que alguien la puede conocer.

- La contraseña caducará periódicamente, debiendo el empleado asignar una nueva. Para mayor seguridad, dicha contraseña deberá seguir los parámetros establecidos en el Documento de Seguridad. No se podrá utilizar ningún acceso autorizado de otro usuario, aunque lo autorice su usuario propietario.

GESTIÓN DE INCIDENCIAS

- Notificar al Responsable de Seguridad de OSAKIDETZA pertinente, mediante los canales establecidos y de forma inmediata cualquier incidencia o anomalía que se detecte sobre la seguridad en los Sistemas de Información, de acuerdo con lo establecido en el Documento de Seguridad de OSAKIDETZA.

- A estos efectos, se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos. A los efectos de su registro, se distinguen los siguientes tipos de incidencias:
    - Accesos no autorizados a datos de carácter personal.
    - Sospecha de uso indebido del acceso restringido.
    - Pérdida de soportes informáticos con datos de carácter personal.
    - Accesos no autorizados a dependencias que contienen sistemas de información con datos de carácter personal.
    - Alteración directa de los datos de producción, convenientemente autorizada, ante posibles fallos de programa u otras situaciones anómalas.
    - Petición de recuperación de datos de carácter personal.
    - Información remitida a destinatario(s) incorrecto(s).
    - Extravío de documentos con información confidencial.
    - Identificación errónea de persona(s), con otras consecuencias.
    - Otras (que se identificarán convenientemente y se incorporarán a la presente tabla).

GESTIÓN DE SOPORTES

Únicamente los usuarios debidamente autorizados (según lo establecido por el documento de Seguridad) podrán obtener soportes que contengan datos de carácter personal. Los siguientes párrafos se refieren única y exclusivamente a estos usuarios debidamente autorizados.

- Los usuarios anteriormente citados están obligados a devolver los soportes que contienen datos de carácter personal inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

- Igualmente deberán guardar los soportes que contengan datos de carácter personal en lugar seguro y siempre bajo llave cuando no sean usados, especialmente fuera de la jornada laboral.

- Los soportes que contengan datos de carácter personal deberán estar claramente identificados con una etiqueta externa que indique (directa o indirectamente) de qué fichero se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación, de acuerdo con lo indicado en el Documento de Seguridad.

- Aquellos medios de soporte de información que sean reutilizables, y que hayan contenido copias de datos de carácter personal, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no puedan ser recuperados nuevamente.

- Los soportes que contengan datos de carácter personal deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso de esos datos.

- Cualquier salida de soportes con datos de carácter personal, sólo podrá ser realizada por usuarios autorizados.

- Cuando se produzca una salida de soportes con datos de carácter personal de nivel alto, estos deberán ser cifrados o bien se deberá utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.

COMUNICACIONES Y CORREOS ELECTRÓNICOS

- En general, y en su caso, se prohíbe el envío de correos electrónicos y transferencias de ficheros por las redes de comunicaciones (siempre que contengan datos que permitan la identificación de las personas físicas a las que se refieran) a terceros distintos del titular de dichos datos personales fuera del ámbito estricto de OSAKIDETZA. En cualquier caso, si estos envíos de información hubieran de realizarse, deberán contar con el consentimiento expreso del interesado titular de los datos o con el amparo de una norma con rango de ley, a menos que se trate de urgencias médicas. Cualquier cesión de datos personales a terceros se pondrá en conocimiento del al Responsable de Seguridad de OSAKIDETZA pertinente, a través de los Responsables de Autorización de Accesos correspondientes. Especialmente, habrán de informarle sobre los envíos de información a terceros países.

- Cualquier salida de información a través de redes de comunicaciones con datos de carácter personal, sólo podrá ser realizada por usuarios autorizados.

- Cuando se produzca una salida de información a través de redes de comunicaciones con datos de carácter personal de nivel alto, estos deberán ser cifrados siguiendo las pautas indicadas en el Documento de Seguridad.

- Se deberán registrar los envíos realizados mediante correo electrónico o transferencia de datos por red, de forma que siempre se pueda identificar su origen, tipo de datos, formato, fecha y hora del envío y destinatario de los mismos.

CONFIDENCIALIDAD DE LA INFORMACIÓN

- Mantener el secreto profesional respecto a la información confidencial con la que se trata. Esta obligación persistirá por tiempo indefinido, aún después de finalizar sus relaciones con OSAKIDETZA.

- En el caso en que, el usuario entre en posesión de información confidencial contenida en cualquier tipo de soporte y a través de cualquier medio, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello otorgue derecho alguno de posesión, titularidad, copia o distribución sobre dicha información.

- Llevar a cabo un tratamiento adecuado de la información evitando cualquier manipulación que pueda producir modificación, alteración o destrucción de los datos almacenados, responsabilizándose de cualquier actuación contraria a la norma.

- Reducir el uso de información confidencial de OSAKIDETZA a lo estrictamente necesario adoptando las debidas precauciones y medidas para evitar el acceso a los mismos por cualquier persona no autorizada.

- Destruir la información confidencial una vez que haya dejado de ser útil para el objeto con el que se recabó.

SOLICITUD DE INFORMACIÓN A TERCEROS

- Solicitar únicamente la información de carácter personal estrictamente necesaria para el motivo por el que se recoge, teniendo en cuenta los principios legales de información y consentimiento del afectado cuando fuere preciso.

TRANSFERENCIA DE INFORMACIÓN A TERCEROS

- Queda prohibida la transferencia de información confidencial a terceros, por cualquier medio (en soporte papel, magnético, electrónico, etc.), excepto a las personas o entidades debidamente autorizadas.

EN RELACIÓN AL TRATAMIENTO NO AUTOMATIZADO DE DATOS

- Considerando que los documentos en soporte papel están igualmente sometidos a las exigencias de la normativa de protección de datos, en el caso del uso de impresoras, deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de carácter personal, los usuarios de cada equipo deberán retirar los documentos conforme vayan siendo impresos.

- En su caso, todos los documentos en papel se mantendrán almacenados en lugares que impidan su lectura por personas no autorizadas y se destruirán convenientemente cuando ya no sean necesarios.

- Custodiar toda aquella documentación no automatizada, con la que se esté trabajando con motivo de sus labores diarias, mientras no se encuentre archivada (bien, en su caso, en los archivos departamentales, bien, en su caso, en los archivos personales como cajoneras o armarios).

- En su caso, cerrar con llave los lugares de archivo personales de la documentación no automatizada (cajoneras y/o armarios), cuando se produzca una ausencia del puesto de trabajo y esta ausencia, provoque que no pueda controlar estos lugares de archivo. En especial, deberá cumplirse esta obligación, en las ausencias del puesto de trabajo al finalizar la jornada laboral.

- En su caso, archivar la documentación no automatizada, de acuerdo con los criterios dictados por OSAKIDETZA.

- Abstener de realizar copias de documentos no automatizados con datos considerados de nivel alto, sin contar con la debida autorización por parte del Responsable de Autorización de Accesos de OSAKIDETZA pertinente.

CONSECUENCIAS DEL INCUMPLIMIENTO DEL DEBER DE SECRETO

El incumplimiento del deber de secreto se configura en la Ley 2/2004 del Parlamento Vasco, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos (LVPD), en diversos artículos:

Es infracción **muy grave** la vulneración del deber de guardar secreto sobre datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas. (Artículo 22.4.h)

Es infracción **grave** la vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales o a Hacienda pública, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo. (Artículo 22.3.f)

Es infracción **leve** el incumplir el deber de secreto salvo que constituya infracción grave. (Artículo 22.2.e).

Según el Artículo 24 de la LVPD (Infracciones cometidas por las administraciones públicas, instituciones y corporaciones de Derecho público):

- Cuando, instruido el correspondiente procedimiento, se llegue a la conclusión de que se ha cometido alguna infracción, **el director de la Agencia Vasca de Protección de Datos** dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción.

- La **AVPD** notificará su resolución al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados, si los hubiera.

- **El director de la Agencia Vasca de Protección de Datos podrá proponer también la iniciación de actuaciones disciplinarias**. El procedimiento y las sanciones a aplicar serán los establecidos en la legislación reguladora del régimen disciplinario correspondiente.

NORMATIVAS

Norma Nº	10	1. MEDIDAS DE SEGURIDAD EN LAS COMUNICACIONES			
Versión :	02	F/Implantación:	15/10/2015	F/Caducidad :	
Sustituye a:	01	Fecha :	30/12/2000		
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Norma 10

Cambios destacables (desde versión anterior)

- Adecuar a la realidad actual de OSAKIDETZA las medidas de seguridad en las comunicaciones

Ámbito de aplicación :	FICHEROS DE NIVEL ALTO TRATAMIENTO AUTOMATIZADO DE DATOS
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS RESPONSABLE DE COMUNICACIONES

Descripción de la Norma :
Este apartado describe la normativa a aplicar para implementar una solución de seguridad en comunicaciones sobre los sistemas de información que manejan Datos de Carácter Personal de nivel Alto. 1. La red de área extendida (WAN) que intercomunica a todos los centros entre sí, mantendrá un sistema de seguridad en las comunicaciones para los Sistemas de Información de nivel alto. 2. El sistema de seguridad contemplará al menos los servicios de autenticación, confidencialidad e integridad de datos. 2.1. Servicio de Autenticación. Mediante este servicio se asegura la identificación de los extremos en las sesiones de diálogo entre un puesto PC y los servidores de aplicaciones a fin de evitar la pérdida de información por envío a destinos incorrectos, manteniendo la confidencialidad y evitando la suplantación de terceros. No aplica a DATOS. 2.2. Servicio de Confidencialidad. Este servicio asegura la confidencialidad de la información circulante a través de las distintas líneas (protección contra ataques pasivos). Este servicio evita la legibilidad a terceros de la información circulante, mediante la encriptación de los datos. 2.3. Servicio de Integridad. La implementación de este servicio asegura la integridad de la información circulante a través de las distintas líneas de la red de comunicaciones (protección contra ataques activos). Con este servicio se evita la inserción, borrado o modificación de la información original. 3. La implementación de los servicios mencionados anteriormente se realizará mediante la aplicación de tecnologías de cifrado de datos (p.ej. PGP, SSL). 4. Únicamente se utilizarán algoritmos estándar de cifrado cuya eficacia haya sido demostrada a través del escrutinio público obteniendo el reconocimiento de la comunidad científica internacional. Actualmente, el sistema de cifrado utilizado en la red WAN de Osakidetza es AES, con MD5 y claves precompartidas. 5. Si se utilizan criptosistemas simétricos, la longitud de las claves de cifrado será, como mínimo, de 128 bits. 6. Si se utilizan criptosistemas asimétricos, sus claves han de tener una longitud que proporcione una fortaleza equivalente a la anterior.

7. Se revisarán anualmente los requerimientos sobre las longitudes de las claves de cifrado y se actualizarán en la medida en que el estado de la tecnología lo permita.
8. En ningún caso se permite la utilización de algoritmos propietarios[2] de cifrado.
9. Se respetará la legislación que sobre la materia hayan aprobado los Estados en que se ubiquen los extremos de comunicaciones cifradas.
10. El uso de las claves de cifrado estará restringido al personal previamente autorizado que lo necesite por motivos de su trabajo.
11. Las autorizaciones del uso de las claves será aprobada por el Responsable de Autorización de Accesos sobre la información que se someterá al cifrado.
12. La gestión y distribución de las claves estarán restringidas al Responsable de Comunicaciones.
13. El mecanismo de distribución de claves debe asegurar que únicamente las recibe su destinatario.

[2] Aquéllos que no han sido sometidos al escrutinio público.

Norma Nº	**20**	**2. CLASIFICACION DE LOS DATOS PERSONALES**			
Versión :	02	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:	01	Fecha :	30/12/2000		
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Documento de Seguridad

Cambios destacables (desde versión anterior)

- Actualización de la clasificación de los DCP para incluir el tipo “violencia de género”

Ámbito de aplicación :	GENERAL
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS

Descripción de la Norma :
Sin la existencia de un proceso previo de clasificación se corre el riesgo de dar un tratamiento inadecuado a los diversos tipos de datos almacenados, transmitidos, procesados o tratados. No todos los datos tienen el mismo valor, y así lo entiende el "Reglamento de Desarrollo de la Ley Orgánica 15/1999", aprobado en Real Decreto 1720/2007, de 21 de diciembre por lo cual es imprescindible realizar una evaluación previa de la calidad de los mismos. Estas medidas son de aplicación en toda declaración de ficheros al Registro General de la Agencia Española de Protección de datos, en el mantenimiento y actualización del Documento del Seguridad y en la resolución de las comunicaciones realizadas por el personal de Osakidetza en materia de protección de datos. Siempre y cuando el Responsable de los ficheros sea Osakidetza. En toda situación en la que se deba realizar una clasificación de los datos personales el encargado de la misma será el Responsable de Autorización de Accesos. Los criterios que indiquen la pauta de tal clasificación deben ser los marcados por: • La normativa legalmente vigente en la materia. (Concretada en Directivas, leyes orgánicas, ordinarias, reglamentos y decretos de desarrollo). • Jurisprudencia dictada por los Jueces y Tribunales competentes en la materia. • Las Instrucciones de la Agencia Española de Protección de Datos y de la Agencia Vasca de Protección de Datos. • Las Memorias anuales publicadas por la Secretaría General de la Agencia Española de Protección de Datos y por la Agencia Vasca de Protección de Datos. En caso de conflicto normativo, deben seguirse los siguientes axiomas: • Norma posterior deroga a norma anterior. • Norma específica explicita a norma genérica. • Norma inferior en rango no modifica a superior, la detalla. Esta norma ha de considerarse en la aplicación del Procedimiento de Registro de Ficheros (P180).

Los baremos de clasificación establecidos en la presente normativa deben actualizarse permanentemente, con los criterios que dicten los órganos anteriormente indicados.

El Responsable de Seguridad mantendrá actualizada dicha lista, haciendo las modificaciones pertinentes en el Documento de Seguridad y en las declaraciones de Ficheros.

El uso de la doctrina especializada sólo informará tales criterios en los supuestos en que exista una laguna interpretativa o contradicción normativa.

Los datos de carácter personal se clasifican en :

NIVEL BÁSICO
Todo fichero que contenga datos de carácter personal
NIVEL MEDIO
Comisión de infracciones administrativas o penales
Hacienda Pública
Servicios Financieros
Prestación de servicios de Información sobre solvencia patrimonial y crédito
Conjunto de datos que permitan obtener una evaluación de personalidad
NIVEL ALTO
Ideología
Afiliación Sindical
Religión
Creencias
Origen Racial
Salud
Vida sexual
Recabados para fines policiales sin el consentimiento del afectado.
Datos derivados de Violencia de Género.

El Responsable de Autorización de Accesos que se enfrente a la clasificación de los datos personales debe adoptar las siguientes pautas que le sirvan de guía y fundamento en la toma de su decisión.

2.1 Dato de carácter personal

Se define como cualquier información concerniente a personas físicas identificadas o identificables.

(Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999, de 13 de diciembre)

"El objeto de la protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal".

(Fundamento sexto STC 292/200, de 30 de noviembre.)

2.2 Comisión de infracciones administrativas o penales

Los ficheros que contengan datos personales sobre infracciones administrativas o penales sólo podrán ser incluidos en los ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras. (Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999, de 13 de diciembre)

OSAKIDETZA considerando su faceta de Entidad Pública, podría disponer de este tipo de datos en sus ficheros, siempre y cuando exista una norma que lo regule.

2.3 Hacienda Pública

Dicha expresión se refiere exclusivamente a los ficheros cuya titularidad corresponda a la Hacienda Pública, debiendo entenderse como aplicable a aquellos ficheros cuyo responsable sea una Administración Pública que ostente potestades en materia tributaria; esto es aquellos ficheros cuyo responsable sea la Agencia Estatal de la Administración Tributaria, los que correspondan a las Comunidades Autónomas en materia de Tributos que les hayan sido cedidos o aquellos padrones fiscales, correspondientes a los tributos locales, de los que son responsables las Haciendas Locales.

(Memoria de la Agencia de Protección de datos. Año 1999. Página 413)

OSAKIDETZA no tiene habilitación para disponer de ésta clase de datos.

2.4 Servicios Financieros

Para delimitar el sentido de esta referencia deberá atenderse al ámbito que, en relación con dicho tipo de servicios, establece la normativa vigente que, en todo caso, excederá de lo que deba ser considerado, meramente, como servicio bancario o actividades

tradicionales llevadas a cabo por las entidades de crédito.

Como elemento delimitador, el Real Decreto 1560/1992, de 18 de diciembre, por el que aprueba la clasificación nacional de actividades económicas, considera actividades de intermediación financiera como una categoría específica, incorporada en el apartado "J" de la clasificación, estableciendo tres epígrafes separados:

- Para las actividades de intermediación financiera en sentido estricto
- Las relacionadas con seguros (excepto la Seguridad Social obligatoria)
- Las actividades auxiliares a las anteriores.

(Memoria de la Agencia de Protección de datos. Año 1999. Página 411)

2.5 Prestación de servicios de Información sobre solvencia patrimonial y crédito.

Son datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor. Los titulares de tales ficheros sólo pueden ser entidades que se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito. En todo caso estos datos se fundamentan en la existencia de una deuda previa, cierta, exigible y que haya resultado impagada.

(Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999, de 13 de diciembre e Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de datos).

2.6 Conjunto de datos que permitan obtener una evaluación de la personalidad.

Las personas tienen el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

Solamente puede realizarse la misma cuando:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguarda de su interés legítimo.

b) Esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

(Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de24 de octubre de 1995)

2.7 Ideología

Se define como una determinada posición intelectual ante la vida y cuanto le acontece y a representar o enjuiciar la realidad según personales convicciones.

La ideología debe poder expresarse con arreglo a las propias ideas sin sufrir por ello sanción o demérito ni padecer la compulsión o la injerencia de los poderes públicos.

(Sentencia del Tribunal Constitucional 120/1990)

2.8 Afiliación Sindical

Todo dato que revele la pertenencia a un Sindicato, ya que son formaciones con relevancia social, debe incluirse en esta definición, ya que responde a una opción ideológica protegida por el artículo 16 de la Constitución.

(Sentencia del Tribunal Constitucional 94/1998 y Memoria de la Agencia de Protección de datos, año 1999)

2.9 Religión

El concepto de libertad religiosa y de culto garantizada por la Constitución, comprende, con la consiguiente inmunidad de ecuación, el derecho de toda persona a:

a) Profesar las creencias religiosas que libremente elija o no profesar ninguna; cambiar de confesión o abandonar la que tenía; manifestar libremente sus propias creencias o la ausencia de las mismas o abstenerse a declarar sobre las mismas.

b) Practicar los actos de culto y recibir asistencia religiosa de su propia confesión; conmemorar sus festividades; celebrar sus ritos matrimoniales, recibir sepultura digna sin discriminación por motivos religiosos y no ser obligado a practicar actos de culto o a recibir asistencia religiosa contraria a sus convicciones personales.

c) Recibir e impartir enseñanza e información religiosa de toda índole, ya sea oralmente, por escrito o por cualquier otro procedimiento, elegir para si y para los menores no emancipados e incapacitados, bajo su dependencia, dentro y fuera del ámbito escolar la educación religiosa y moral que esté de acuerdo con sus propias convicciones.

d) Reunirse o manifestarse públicamente con fines religiosos y asociarse para desarrollar comunitariamente sus actividades religiosas de conformidad con el ordenamiento jurídico general y lo establecido en la presente ley orgánica.

(Ley orgánica 7/1980, de 5 de julio, de libertad religiosa)

2.10 Creencias

Las creencias se manifiestan por el derecho que asiste al creyente de creer y conducirse personalmente conforme a sus convicciones, no estando sometido a más límites que los que le imponen el respeto a los derechos fundamentales ajenos y otros bienes jurídicos protegidos constitucionalmente: el derecho a manifestar sus creencias frente a terceros mediante su profesión pública, y el proselitismo de las mismas, suma a los primeros los límites indispensables para mantener el orden público protegido por la ley.

(Sentencia del Tribunal Constitucional 141/2000, de 29 de mayo de 2000)

2.11 Origen Racial

Datos que indiquen la casta o calidad del origen o linaje.

(Diccionario RAE, edición 2001)

2.12 Salud

Los datos de salud se dividen en datos médicos y datos genéticos. Los primeros son los que hacen referencia a todos los datos de carácter personal relativos a la salud de una persona. También afecta a los datos manifiesta y estrechamente relacionados a la salud y las informaciones genéticas. Por los segundos, entiende los datos de cualquier tipo, relacionados con los caracteres hereditarios de un individuo o que, vinculados a los mismos, compongan el patrimonio de un grupo de individuos emparentados. También afecta a todos los datos relativos a intercambios de información genética (genes) de un individuo o línea genética, con relación a cualquier aspecto de la salud o de una enfermedad, constituya o no un carácter identificable.

(Recomendación número R (97) 5, del Consejo de Europa)

2.13 Vida sexual

Ideas, actitudes y conductas personales relacionadas con la sexualidad humana. Datos sobre orientación, tendencias, actividad, comportamiento, etc. sexuales.

Sin embargo, conviene aclarar que cuando este tipo de datos se refiere a determinadas enfermedades, como por ejemplo las de transmisión sexual, se deben consignar como datos relativos a la salud del afectado y no como datos referentes a su vida sexual.

2.14 Recabados para fines policiales sin el consentimiento del afectado

Se definen como aquellos datos de carácter personal recogidos y tratados únicamente por las Fuerzas y Cuerpos de Seguridad limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en

función de su grado de fiabilidad.

(Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999, de 13 de diciembre)

OSAKIDETZA no tiene habilitación para disponer de ésta clase de datos.

2.15 Datos derivados de Violencia de Género

Violencia (todo acto de violencia física y psicológica, incluidas las agresiones a la libertad sexual, las amenazas, las coacciones o la privación arbitraria de libertad) que, como manifestación de la discriminación, la situación de desigualdad y las relaciones de poder de los hombres sobre las mujeres, se ejerce sobre éstas por parte de quienes sean o hayan sido sus cónyuges o de quienes estén o hayan estado ligados a ellas por relaciones similares de afectividad, aun sin convivencia.

Se incluyen en esta categoría tanto los datos de las víctimas como los de los agresores y terceras personas que pudieran verse afectadas por las circunstancias concretas de cada caso.

(Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género).

Norma Nº	**30**	**3. COMUNICACIÓN AL RESPONSABLE DE SEGURIDAD DE LA EXISTENCIA DE FICHEROS**			
Versión :	02	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:	01	Fecha :	30/12/2000		
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Documento de Seguridad

Cambios destacables (desde versión anterior)

- Referencia al procedimiento que desarrolla la norma.

Ámbito de aplicación :	GENERAL
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS

Descripción de la Norma :
Este apartado define la normativa a aplicar para el tratamiento de ficheros en uso que traten datos de carácter personal no declarados, o ficheros de nueva creación, ambos contenidos en los sistemas de información de OSAKIDETZA. 1. Todo fichero con datos de carácter personal tratado por los usuarios que no esté incluido aún en el Documento de Seguridad, debe ser comunicado sin dilación al Responsable de Autorización de Accesos competente que, a su vez, informará al Responsable de Seguridad en la Organización de Servicio afectada. 2. Todos los usuarios deben informar al Responsable de Autorización de Accesos competente, previamente a la creación de nuevos ficheros que contengan datos de carácter personal, sobre la finalidad, contenido y ubicación de los potenciales ficheros. El Responsable de Autorización de Accesos, a su vez, informará al Responsable de Seguridad en la Organización de Servicio afectada. Se exceptuarán de estas obligaciones los ficheros cuyos datos no permitan la identificación de los titulares de dichos datos, por encontrarse disociados. Esta norma ha de considerarse en la aplicación del Procedimiento de Registro de Ficheros (P180).

Norma Nº	40	4. ADMINISTRACIÓN DE USUARIOS			
Versión :	03	F/Implantación:	15/10/2015	F/Caducidad :	
Sustituye a:	02	Fecha :	17/06/2011		
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Documento de Seguridad
02	17/06/2011	Norma 40

Cambios destacables (desde versión anterior)

- Párrafo 2.7 sobre las preguntas para auto recuperar la contraseña por el propio usuario y Párrafo 3.1 sobre la TPE como medio de autenticación de identidad. Actualización de la política de contraseñas.

Ámbito de aplicación :	GENERAL
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS

Descripción de la Norma :

Este apartado describe la normativa a aplicar para la administración de usuarios con acceso a los Sistemas de Información, **tanto automatizados como no automatizados**, de OSAKIDETZA, con objeto de establecer mecanismos que eviten el acceso incontrolado a los recursos de información presentes en los sistemas.

1. Inventario de usuarios

1.1 El Responsable de Seguridad en colaboración con los Responsables de Autorización de Accesos a los Sistemas de Información definirá una colección de perfiles de usuarios donde se especifique las opciones de acceso permitidas y el tipo de acceso requerido (actualización o consulta.)

1.2. Los Responsables de Autorización de Accesos a los Sistemas de Información, en funciones de Responsables de Fichero, son los únicos con competencia para conceder, alterar o anular los accesos autorizados a los sistemas.

1.3. Todos los usuarios tendrán asignados perfiles con acceso autorizado exclusivamente a los recursos que precisan para desempeñar su función.

1.4 El Responsable de Seguridad mantendrá un registro de usuarios con acceso autorizado a los Sistemas de Información. El registro se mantendrá en todo momento actualizado, revisándose de forma periódica (ver Norma 70) para actualizar las altas, bajas y modificaciones de los usuarios, y teniendo especial cuidado en eliminar de forma inmediata las autorizaciones de acceso a los usuarios que causen baja en OSAKIDETZA, o cambien su trabajo a un puesto que no conlleve acceso alguno a los Sistemas de Información.

1.5 Este inventario deberá contemplar al menos la siguiente información:

- Sistema de Información.
- Nombre de usuario.
- Centro y cargo que desempeña en OSAKIDETZA
- Identificador de usuario (únicamente para el caso de tratamientos automatizados).
- Perfil de usuario.

1.6 En el caso de tratamientos automatizados, el mecanismo de registro identificará de manera unívoca cada usuario con acceso autorizado a los Sistemas de Información, e impedirá y/o detectará la alteración, modificación o eliminación de los datos de los registros realizados.

2. Accesos autorizados en sistemas de tratamientos automatizados

2.1 Todos los usuarios con acceso a un Sistema de Información, dispondrán de una única autorización de acceso compuesta de Identificador de usuario y Contraseña. El Identificador de usuario será personal y exclusivo para cada empleado y se configurará con su DNI (incluyendo la "letra de control").

2.2 Los Sistemas de Información deberán habilitar un mecanismo que exija cuatrimestralmente (cada 120 días) el cambio de la contraseña para cada autorización de acceso.

2.3 La política de contraseñas que se establece será la siguiente:.

- Las contraseñas deben de tener una longitud mínima de 8 caracteres y máxima de 15.
- El sistema comenzará a recordar al usuario que debe cambiar la contraseña desde 30 días antes de que caduque.
- La sintaxis de las contraseñas será la siguiente:
    - Deberá incluir caracteres de cada una de las siguientes categorías:
        - Mayúsculas (de la A a la Z)
        - Minúsculas (de la a a la z)
        - Números base decimal (del 0 a 9)
        - Caracteres no alfanuméricos (!()=@ +,.-%$#&/:;<>?)

2.4 Se aplicará el sistema de bloqueo que se indica a continuación:

- Cuando un usuario introduzca 5 veces seguidas una contraseña errónea, el acceso de ese usuario quedará bloqueado provisionalmente durante 30 minutos.
- Cuando un usuario no renueve su contraseña en los 120 días posteriores al último cambio, el acceso de ese usuario quedará bloqueado permanentemente hasta que el propio usuario o un administrador realice un proceso de recuperación/restauración de la contraseña.

.

2.5 El sistema almacenará mediante algoritmos de cifrado las contraseñas al objeto de garantizar la confidencialidad e integridad de las mismas.

2.6 Cuando el Administrador de Seguridad genere una nueva contraseña, ésta será temporal, de manera que se obligue al usuario a cambiarla en cuanto entre al sistema por primera vez, tras cada generación de la misma por el Administrador.

2.7 Para que el propio usuario, en caso de olvido, pueda recuperar su contraseña de acceso al sistema, previamente habrá tenido que registrar las respuestas a las

preguntas establecidas al efecto. Será necesario responder correctamente, al menos, a dos de las tres preguntas seleccionadas, para que el sistema recupere la contraseña del usuario.

3. Tarjeta Profesional Electrónica

3.1 Los usuarios que dispongan de su TPE con certificado podrán utilizarla como medio para autenticar su identidad ante los sistemas de información de Osakidetza.

Norma Nº	50	5. REGISTRO DE ACCESOS DE NIVEL ALTO			
Versión :	02	F/Implantación:	15/10/2015	F/Caducidad :	
Sustituye a:	01	Fecha :	30/12/2000		
Sustituida por:		Fecha :			

Ámbito de aplicación :	FICHEROS DE NIVEL ALTO TRATAMIENTO AUTOMATIZADO DE DATOS
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Norma 50

Cambios destacables (desde versión anterior)

- Adecuar el 2º párrafo de la Norma al literal del art. 103 RLOPD.
- Segregar las revisiones de logs según se trate de ficheros sectoriales o corporativos, respectivamente, a los RSOS y al RS-SSCC.

Descripción de la Norma :

Este apartado define la normativa a aplicar a todo Sistema de Información que contenga datos de carácter personal de nivel alto, cuya responsabilidad sea de OSAKIDETZA. Para los accesos a Datos de Carácter Personal de nivel alto se seguirá la presente Norma:

- Se realizarán trazas de auditoría en las que como mínimo se guardarán los siguientes datos:
  - Identificación del usuario que accede.
  - Fecha y hora en que realizó el acceso.
  - Fichero accedido.
  - Tipo de acceso: alta, baja, modificación y consulta.
  - Acceso autorizado o denegado.
  - Información que permita identificar los registros accedidos por el usuario, en caso de que el acceso se hubiera realizado con éxito.
- Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. En caso de que estos mecanismos debieran desactivarse, por motivos excepcionales, se recogerá este hecho en el Registro de Incidencias.
- El periodo de conservación de estos datos será de dos años.
- El Responsable de Seguridad de la OS se encargará de revisar periódicamente la información de control registrada correspondiente a los ficheros de su OS y elaborará un informe de las revisiones realizadas y los problemas detectados, al menos una vez al mes. El Responsable de Seguridad de la Organización Central hará lo propio con la información de control registrada correspondiente a los ficheros corporativos.
- El fichero de trazas de auditoría cumplirá con los siguientes criterios:
  - Debe existir un fichero por cada fichero físico que contenga DCP de nivel alto.
  - Incorporará las máximas medidas de seguridad en el acceso.
  - No requerirá funciones de trazabilidad (es decir, se evitará incorporar en el mismo DCP de nivel alto).
  - Será exclusivamente de lectura (exceptuando el propio proceso que lo alimente).
  - Estará ubicado en servidores de alta disponibilidad y con criterios de recuperación de máxima prioridad.
- Al fichero de auditoría sólo podrán acceder: el Auditor debidamente acreditado, el Responsable del Fichero de DCP, el Responsable de Seguridad de cuya OOSS sea el fichero de DCP, el Responsable de Seguridad de SSCC, la AEPD, la AVPD y el Órgano Judicial competente.

Norma Nº	**60**	**6. TRATAMIENTO DE FICHEROS TEMPORALES**			
Versión :	02	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:	01	Fecha :	30/12/2000		
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Documento de Seguridad

Cambios destacables (desde versión anterior)

- Actualización de la norma ampliando el ámbito al tratamiento de ficheros no automatizados.

Ámbito de aplicación :	GENERAL
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS

Descripción de la Norma :
Este apartado define la normativa a aplicar para el tratamiento de ficheros temporales, de forma que se asegure la privacidad y seguridad de los Datos de Carácter Personal contenidos en los Sistemas de Información de OSAKIDETZA Se deberá tener en cuenta que en la presente normativa, las funciones atribuidas al Responsable del Fichero son asumidas por los correspondientes Responsables de Autorización de Accesos. Asimismo se debe diferenciar la función del Responsable Informático del Sistema de Información y el Responsable Funcional del Sistema de Información, que en muchos casos coincidirá con el Responsable de Autorización de Accesos. 1. OSAKIDETZA permitirá la creación de ficheros temporales que contengan Datos de Carácter Personal siempre que cumplan con las medidas de seguridad del fichero original y sean destruidos al finalizar el objetivo para el cual fueron creados. Los ficheros temporales pueden ser creados en las siguientes situaciones: • Ficheros temporales creados por usuarios autorizados mediante el uso de herramientas ofimáticas. • Ficheros temporales generados por la Unidad de Explotación. • Ficheros temporales generados automáticamente en procesos internos de los Sistemas de Información. • Ficheros temporales obtenidos de copias físicas de documentos no automatizados o impresiones de ficheros automatizados. 2. Ficheros temporales generados mediante herramientas ofimáticas. • Este tipo de ficheros se generará únicamente por usuarios autorizados y para su uso en procesos específicos y perfectamente delimitados y precisándose de una password de red para acceder a este tipo de ficheros. Una vez hayan dejado de ser útiles para los fines que se crearon, este tipo de ficheros deberán ser borrados físicamente por el usuario. • Los ficheros temporales no podrán ser copiados en soportes externos, ni se permitirá su salida fuera de la unidad usuaria, salvo autorización expresa y por escrito del Responsable del Fichero y con copia al Responsable de Seguridad, quien la tramitará como una incidencia mediante el procedimiento habilitado para ello. 3. Ficheros temporales generados por la Unidad de Explotación. • Este tipo de ficheros se generan mediante procesos específicos ejecutados por la Unidad de Explotación, a petición de las áreas usuarias y con autorización del Responsable del Sistema de Información. • Estos ficheros son depositados en un directorio del servidor de red, en una carpeta de acceso restringido a un trabajador o grupo concreto de trabajadores de OSAKIDETZA.

- Al igual que los ficheros generados por los propios usuarios, una vez hayan dejado de ser útiles los ficheros generados por Explotación para los fines que se crearon, estos ficheros deberán ser borrados físicamente por el usuario.
- Estos ficheros temporales no podrán ser copiados en soportes externos, ni se permitirá su salida fuera de la unidad usuaria, salvo autorización expresa y por escrito del Responsable del Fichero y con copia al Responsable de Seguridad, quien la tramitará como una incidencia mediante el procedimiento habilitado para ello.

4. Ficheros temporales generados automáticamente en procesos internos de los Sistemas de Información.

   - Estos ficheros se generan automáticamente en procesos internos de los Sistemas de Información cuya ejecución puede estar programada periódicamente o con carácter esporádico. Tanto en un caso como en otro, los procesos deben estar diseñados para que los ficheros temporales creados durante su ejecución se eliminen a la finalización del mismo.
   - Si por causas accidentales el proceso falla durante su ejecución, los ficheros temporales permanecerán creados hasta que el Responsable Informático del Sistema de Información analice y conozca la causa que motivo el fallo. Posteriormente se procederá a borrar físicamente los ficheros temporales existentes mediante mecanismos complementarios habilitados.

5. Ficheros temporales obtenidos de copias físicas de documentos no automatizados o impresiones de ficheros automatizados.
   - Estos ficheros se obtienen a partir de fotocopias realizadas a documentación en formato papel, o bien al imprimir un extracto o la totalidad de un fichero automatizado.
   - Así como los demás ficheros temporales, una vez hayan dejado de ser útiles o hayan cumplido el fin por el cual ha sido creados, deberán destruirse siguiendo lo dispuesto en la Norma 13 “GESTIÓN Y CUSTODIA DE SOPORTES EN EL TRATAMIENTO NO AUTOMATIZADO DE DATOS”.
   - En ningún caso estos ficheros podrán salir de las dependencias físicas de la Organización de Servicios.
6. Los ficheros temporales tendrán aplicadas las mismas medidas de seguridad que correspondan a los ficheros de los cuales procede su información.

Norma Nº	70	7. REGULACION DE LOS CONTROLES PERIODICOS A REALIZAR PARA LA VERIFICACION DE LO DISPUESTO EN EL DOCUMENTO DE SEGURIDAD			
Versión :	02	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:	01	Fecha :	30/12/2000		
Sustituida por:		Fecha :			

Ámbito de aplicación :	GENERAL
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Documento de Seguridad

Cambios destacables (desde versión anterior)

- Modificación de la norma para mejorar la aplicación práctica de la misma.

Descripción de la Norma :

Mediante este apartado se define la normativa a aplicar con el fin de regular los controles periódicos a realizar para verificar que se cumplen las prácticas y medidas de seguridad especificadas en el presente Documento de Seguridad, dispuestas por el Título VIII del Reglamento de desarrollo de la LOPD. Los registros que afecten a los ficheros corporativos deberán ser revisados por el/los RS de SSCC, de la misma manera, los que afecten a los ficheros sectoriales deberán ser revisados por el/los RS de la OS.

1. La persona encargada de ejecutar estos controles periódicos es el Responsable de Seguridad, en su ámbito de actuación.

2. Los controles y la periodicidad mínima con la que estos se deben realizar se detallan a continuación:

A. MENSUALMENTE:

1) Se debe revisar el contenido de los siguientes registros:

- Registro de accesos a datos de nivel alto (log de trazabilidad).
- Registro de accesos al CPD (tratamientos automatizados)
- Registro de accesos al archivo (tratamientos no automatizados).

2) Se debe elaborar un informe acerca de las revisiones realizadas y los problemas detectados en relación con los registros indicados en el apartado (1).

3) El informe se ajustará al formato del *"Modelo de informe mensual de cumplimiento LOPD"*.

B. TRIMESTRALMENTE:

4) Se debe revisar el contenido de los siguientes registros:

- Inventario de usuarios con acceso autorizado a datos de carácter personal (tratamiento automatizado y no automatizado).
- Registro de incidencias relacionadas con la LOPD (tratamiento automatizado y no automatizado).
- Registro de entrada/salida de soportes (tratamiento automatizado y no automatizado).

- Inventario de soportes (tratamiento automatizado y no automatizado).

5) Se debe elaborar un informe acerca de las revisiones realizadas y los problemas detectados en relación con los registros indicados en el apartado (4).

6) El informe se ajustará al formato del *"Modelo de informe trimestral de cumplimiento LOPD"*.

C. SEMESTRALMENTE:

7) Se debe revisar el contenido de los siguientes registros:

- Verificación de la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

- Registro de versiones del Documento de Seguridad (tratamiento automatizado y no automatizado).

8) Se debe elaborar un informe acerca de las revisiones realizadas y los problemas detectados en relación con los registros indicados en el apartado (7).

9) El informe se ajustará al formato del "Modelo de informe semestral de cumplimiento LOPD".

3. Los informes correspondientes se presentarán a la Comisión de Seguridad para su aprobación. Se acompañarán de un Resumen de las anomalías y deficiencias que en materia de seguridad se hayan detectado y la relación de soluciones y mejoras propuestas.

En el caso de que los controles afecten a Datos de Carácter Personal de nivel **medio** o **alto** y se conservarán, al menos durante 2 años, para facilitar los trabajos de auditoría, así como las posibles inspecciones de la Agencia de Protección de Datos competente.

Norma Nº	**80**	**8. UTILIZACION DE DATOS REALES EN PRUEBAS**			
Versión :	02	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:	01	Fecha :	30/12/2000		
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Documento de Seguridad

Cambios destacables (desde versión anterior)

- Establecimiento de pautas más claras para la utilización de datos reales en pruebas.

Ámbito de aplicación :	DATOS DE NIVEL MEDIO Y ALTO TRATAMIENTOS AUTOMATIZADOS
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS

Descripción de la Norma :

Este apartado define la normativa a aplicar para la utilización de datos reales en pruebas, de forma que se asegure la confidencialidad y seguridad de los Datos de Carácter Personal contenidos en los Sistemas de Información de OSAKIDETZA.

Esta normativa será aplicable, al menos, a los Datos de Carácter Personal de nivel medio y alto.

OSAKIDETZA establece las siguientes pautas para la realización de pruebas con Datos de Carácter Personal reales en los entornos de Desarrollo y Pruebas:

- **Preferentemente**, los datos a utilizar deberán estar disociados de forma que no sea posible la identificación de los titulares de los mismos.
- En caso de que, justificadamente, no se disocien los datos, se aplicarán las medidas de seguridad correspondientes al nivel de seguridad de dichos datos.
- Las pruebas sólo podrán ser realizadas por usuarios autorizados expresamente por el Responsable de Autorización de Accesos.
- Se prohíbe en todo caso la cesión o entrega de datos personales para la realización de pruebas a terceras partes que mantengan las aplicaciones, sin la previa autorización expresa (por escrito) del Responsable de Autorización de Accesos (asesorado por el Responsable de Seguridad).
- La utilización de datos reales en pruebas, deberá anotarse en un Registro destinado a tal efecto. Este Registro deberá contener los siguientes datos:
    - Día o período en que se produce la prueba.
    - Entorno donde se produce.
    - Nivel de las medidas de seguridad implantadas (básico, medio o alto).
    - Motivo por el que se utilizan datos reales en las pruebas.

Norma Nº	**90**	**9. NORMATIVA PARA LA REALIZACION DE AUDITORIAS DE PROTECCION DE DATOS**			
Versión :	02	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:	01	Fecha :	30/12/2000		
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos
01	30/12/2000	Documento de Seguridad

Cambios destacables (desde versión anterior)

- Adecuación al R.D. 1720/2007

Ámbito de aplicación :	GENERAL
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS

Descripción de la Norma :

Este apartado define la normativa a aplicar para la realización de auditorías en OSAKIDETZA, con objeto de confirmar fehacientemente que las prácticas y medidas de seguridad aplicadas, son las adecuadas y que siguen las normas y procedimientos indicados en el Documento de Seguridad.

1. OSAKIDETZA realizará auditorías de seguridad sobre la LOPD con una periodicidad mínima bienal. Las auditorías se realizarán por personal propio de OSAKIDETZA o bien se delegará su realización a empresas consultoras externas.

2. También será obligatoria la realización de esta auditoría, siempre que se realicen modificaciones sustanciales en los sistemas de información, que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas. El cómputo de los dos años de plazo se debe calcular a partir de ese momento, en dichos casos.

3. Las auditorías deben contemplar al menos los siguientes puntos:

   - Adecuación de la normativa, procedimientos y controles contemplados en el Documento de Seguridad, a lo dispuesto en el Reglamento de Desarrollo de la LOPD (RLOPD) y a las disposiciones legales que en materia de Datos de Carácter Personal puedan establecer en el futuro las autoridades competentes.

   - Verificar para las instalaciones, Sistemas de Información y archivos con documentación que contienen Datos de Carácter Personal, el correcto cumplimiento de las medidas, procedimientos y normativas que en materia de seguridad se establezcan en el presente documento.

   - Identificación de las deficiencias que en materia de seguridad relacionadas con la LOPD se encuentren en las instalaciones, Sistemas de Información, archivos de documentación, normativas, procedimientos y prácticas de OSAKIDETZA.

   - Establecimiento de medidas y recomendaciones para solventar las deficiencias encontradas.

   - Inclusión de todos aquellos datos, hechos y observaciones en los que se basen los dictámenes, recomendaciones y propuestas emitidas.

4. El contenido de las auditorías (tanto si son internas como externas) será analizado por el Responsable de Seguridad, quien elaborará un documento resumen de conclusiones. Tanto la propia auditoría, como el documento resumen se entregará para su aprobación a la Comisión de Seguridad.

5. Los resultados de las auditorías, una vez aprobados por la Comisión de Seguridad, se remitirán al Director General, al objeto de que disponga la implementación de las

recomendaciones de mejora.

6. Las auditorías realizadas, conjuntamente con los informes de conclusiones, se depositarán y archivarán en OSAKIDETZA, manteniéndose los mismos a disposición de la Agencia Vasca de Protección de Datos.

Norma Nº	**100**	**10. ATRIBUCIÓN DE LAS FUNCIONES DEL MODELO ORGANIZATIVO AL PERSONAL DE OSAKIDETZA.**			
Versión :	01	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:		Fecha :			
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos

Cambios destacables (desde versión anterior)

- N/A

Ámbito de aplicación :	GENERAL
Responsable/s :	DIRECCIÓN GENERAL RESPONSABLE DE SEGURIDAD

Descripción de la Norma :

Conforme al artículo 89.2 del RLOPD, este apartado define la normativa a aplicar para realizar la difusión de normas, procedimientos, medidas de seguridad, marco organizativo y funciones y obligaciones del personal con acceso a DCP. Todo ello con objeto de garantizar la seguridad de los Datos de Carácter Personal en OSAKIDETZA.

1. El personal de OSAKIDETZA que tenga acceso a las aplicaciones, equipamiento, archivos, tratamientos, recursos o dependencias que contengan Datos de Carácter Personal, deberá conocer las funciones y obligaciones que le afectan en el desempeño diario y que se encuentran establecidas en el Modelo Organizativo para la protección de los datos de carácter personal[3]. También se informará al personal de las consecuencias en que pudiera incurrir en caso de incumplimiento.

    - La citada comunicación al personal con acceso a DCP se realizará mediante una copia, adaptada a las particularidades de la OOSS, del documento denominado: *"Comunicado de atribución de funciones del Modelo Organizativo de Osakidetza"*.

    - El Director Gerente emitirá el comunicado utilizando los medios adecuados:

        - Comunicado interno.
        - Correo electrónico, con acuse de recibo.
        - Manual de acogida del personal de la OOSS.
        - Intranet de la OOSS.
        - Otros medios apropiados.

2. El personal debe asumir los contenidos del Comunicado de atribución de funciones del Modelo Organizativo de OSAKIDETZA.

3. El Responsable de Seguridad de la OOSS, con el apoyo de la Comisión de Seguridad, será la unidad encargada de resolver o canalizar la resolución de las dudas o cuestiones que puedan surgir en materia de protección de datos, en el ámbito de la actividad diaria del personal.

[3] Véase el correspondiente capítulo en el presente Documento de Seguridad.

Norma Nº	**110**	**11. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD**			
Versión :	01	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:		Fecha :			
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos

Cambios destacables (desde versión anterior)

- N/A

Ámbito de aplicación :	GENERAL
Responsable/s :	RESPONSABLE DE SEGURIDAD

Descripción de la Norma :

Mediante este apartado se define la normativa a aplicar con el fin de regular los cambios en el Documento de Seguridad en el ámbito corporativo y en el ámbito sectorial.

1. En caso de que se produzca un cambio de titularidad en la Gerencia o Cuadro Directivo de la OOSS, o de la Organización Central, **no será necesario** volver a aprobar el Documento de Seguridad completo, en este caso, se deberán actualizar los anexos correspondientes con los nuevos nombramientos una vez aprobados formalmente.

2. De acuerdo con la Instrucción General nº 02 del año 2003 los nombramientos deberán ser comunicados al Responsable de Seguridad de OSAKIDETZA.

3. Capítulos del Documento de Seguridad **que pueden ser modificados** por la Organización de Servicios, a nivel sectorial:

- Introducción, Sistemas de Información y Estructura de Ficheros (en lo referente a la OOSS) y Anexos.
    - Estos capítulos pueden ser modificados sin aplicar el "Procedimiento de actualización del Documento de Seguridad".

- Directrices generales de seguridad
    - Las pautas de seguridad establecidas en este apartado son de obligado cumplimiento para toda Osakidetza, por tanto, las Organizaciones de Servicios podrán **añadir nuevas** directrices de seguridad siempre y cuando no entren en conflicto con las ya establecidas a nivel corporativo.

- Organización de la seguridad
    - Las Organizaciones de Servicios podrán modificar el modelo organizativo para adaptarlo a su propia organización. Dentro del Modelo Organizativo se deben mantener como mínimo la figura de Responsable de Seguridad, Responsable de Autorización de Accesos y Comisión de Seguridad.
    - Se ha de observar el **principio de segregación de funciones** establecido en los estándares de seguridad generalmente aceptados. Según este principio, una misma persona no debe tener privilegios para autorizar algo y para ejecutar dicha autorización, por tanto se intentará evitar esta circunstancia. En caso de no resultar posible la segregación de funciones se hará constar en el Documento de Seguridad, donde corresponda, en el Modelo Organizativo.

- Procedimientos

    - Se podrá alterar exclusivamente los procedimientos afectados por las modificaciones permitidas en el apartado “Organización de la seguridad” con el objeto de adaptarlos a dichas particularidades.

4. Los restantes capítulos del Documento de Seguridad sólo podrán ser modificados a nivel corporativo desde la Organización Central (por ejemplo, las Normativas). Por lo tanto, las Organizaciones de Servicios solamente pueden proponer los cambios que consideren necesarios siguiendo el “Procedimiento de Actualización del Documento de Seguridad” establecido para ello.

Norma Nº	**120**	**12. REALIZACION DE UN PLAN DE FORMACIÓN EN LOPD**			
Versión :	01	F/Implantación:	17/06/2011	F/Caducidad :	31/01/2015
Sustituye a:		Fecha :			
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos

Cambios destacables (desde versión anterior)

- N/A

Ámbito de aplicación :	GENERAL
Responsable/s :	RESPONSABLE DE SEGURIDAD COMISION DE SEGURIDAD

Descripción de la Norma :
Este apartado define la normativa a aplicar para la realización de un plan formativo en materia de LOPD en OSAKIDETZA, con objeto de que todo el personal conozca tanto la legislación como las normas y procedimientos contenidos en el Documento de Seguridad. 1. Se realizarán actividades formativas sobre la protección de datos de carácter personal dirigidas al personal de OSAKIDETZA, en las que se impartirán conocimientos básicos, de manera comprensible, sobre la legislación en dicha materia (la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 y demás normativa vigente). 2. Así mismo, se formará al personal en cuanto al contenido del Documento de Seguridad, sus normas, procedimientos y demás instrucciones dadas por la Dirección, tanto de la Organización Central como de la propia Organización de Servicios. 3. En el caso de que se requieran herramientas informáticas para el desarrollo o ejecución de alguno de los procedimientos establecidos en el Documento de Seguridad, se deberá capacitar al personal involucrado en dicho procedimiento, en la utilización de la herramienta corporativa dispuesta al efecto. 4. Anualmente, se establecerán los Planes de Formación pertinentes, en los cuales deberá incluirse, como mínimo, al 25% de la plantilla, hasta cubrir la totalidad de la misma. Esto supone un horizonte temporal de 4 años, tras los cuales deberá establecerse un porcentaje de mantenimiento. 5. Cada año se evaluarán los resultados obtenidos a través del Plan de Formación y se adoptarán las medidas pertinentes en caso de no ser los idóneos. 6. De igual manera, las Organizaciones de Servicios pondrán a disposición del personal material de consulta y referencia respecto a las normativas legales y el Documento de Seguridad, con el fin de posibilitar la autoformación de dicho personal.

Norma Nº	**130**	**13. GESTIÓN Y CUSTODIA DE SOPORTES EN EL TRATAMIENTO NO AUTOMATIZADO DE DATOS**			
Versión :	01	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:		Fecha :			
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos

Cambios destacables (desde versión anterior)

- N/A

Ámbito de aplicación :	TRATAMIENTOS NO AUTOMATIZADOS [Se excluye la documentación clínica hospitalaria y la documentación clínica en atención especializada ambulatoria y en atención primaria]
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPONSABLE DE AUTORIZACIÓN DE ACCESOS

Descripción de la Norma :
Las siguientes normas serán de aplicación para **todos** los tratamientos no automatizados de datos de carácter personal, **excluyéndose** la documentación clínica hospitalaria y la documentación clínica en atención especializada ambulatoria y en atención primaria, a las que les será de aplicación el Procedimiento de actuación de expurgo y conservación de la documentación clínica, de junio de 2004, de la Comisión de Valoración, Selección y Expurgo de Documentación Clínica. 1. Los soportes no automatizados que contengan documentos de un Fichero o de un tratamiento no automatizado de datos de carácter personal, deberán estar claramente identificados con una etiqueta externa que indique el texto "*LOPD*". 2. La documentación no automatizada que deba ser eliminada, deberá destruirse utilizando mecanismos de destrucción de papel (destructoras de papel). En estos casos se deberán seguir los criterios de expurgo de la Ley 7/1990, de 3 de julio, de Patrimonio Cultural Vasco y su normativa de desarrollo[4]. 3. Los soportes no automatizados deberán ser almacenados en lugares a los que únicamente tengan acceso las personas debidamente autorizadas. 4. La salida de soportes no automatizados, fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el Responsable de Autorización de Accesos competente. 5. Cuando exista un traslado de soportes no automatizados, se adoptarán medidas encaminadas a prevenir la sustracción o pérdida de la documentación en ellos contenida. En particular: • El traslado de la documentación no automatizada deberá realizarse en cajas normalizadas según los criterios recogidos en la Ley 7/1990, de 3 de julio, de Patrimonio Cultural Vasco y su normativa de desarrollo[5]. • Estas cajas deberán estar precintadas, de tal manera que no puedan ser abiertas por usuarios no autorizados sin destruir el precinto. • Las cajas precintadas deberán ser transportadas por personal debidamente autorizado.

[4] DECRETO 232/2000, de 21 de noviembre, por el que se aprueban el Reglamento de los Servicios de Archivo y las normas reguladoras del Patrimonio Documental del País Vasco, DECRETO 174/2003, de 22 de julio, de organización y funcionamiento del Sistema de Archivo de la Administración Pública de la Comunidad Autónoma de Euskadi y la ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

6. Además de las medidas mencionadas anteriormente, el traslado o transporte de documentación no automatizada que contenga datos personales de **nivel alto**, se realizará aplicando medidas para impedir el acceso o manipulación de la mencionada documentación. En particular:

    - Las cajas normalizadas donde se traslade la documentación, se introducirán en contenedores que dispondrán de un mecanismo de apertura mediante llave de seguridad o similar.

    - El personal que realice el traslado de la documentación deberá estar debidamente autorizado por el Responsable de Autorización de Accesos.

    - En todo momento la documentación no automatizada trasladada deberá estar custodiada por el personal al que se refiere el punto anterior.

7. Mientras la documentación no automatizada se encuentre en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre a cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por cualquier persona que no esté debidamente autorizada.

Norma Nº	**140**	**14. CRITERIOS DE ARCHIVO**			
Versión :	01	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:		Fecha :			
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos

Cambios destacables (desde versión anterior)

- N/A

Ámbito de aplicación :	TRATAMIENTOS NO AUTOMATIZADOS [Se excluye la documentación clínica hospitalaria y la documentación clínica en atención especializada ambulatoria y en atención primaria]
Responsable/s :	SERVICIOS DE ARCHIVO

Descripción de la Norma :
Las siguientes normas serán de aplicación para **todos** los tratamientos no automatizados de datos de carácter personal, **excluyéndose** la documentación clínica hospitalaria y la documentación clínica en atención especializada ambulatoria y en atención primaria, a las que les será de aplicación el Procedimiento de actuación de expurgo y conservación de la documentación clínica, de junio de 2004, de la Comisión de Valoración, Selección y Expurgo de Documentación Clínica. 1. El archivo de la documentación no automatizada deberá realizarse de tal manera que garantice la correcta conservación de los documentos, su localización y consulta, así como que posibilite el ejercicio de los derechos de acceso, rectificación, cancelación y/u oposición. 2. El archivo de la documentación se deberá realizar siguiendo lo dispuesto en la Ley 7/1990, de 3 de julio, de Patrimonio Cultural Vasco y su normativa de desarrollo[6] considerando, en particular, lo relacionado con: • El personal que lleve la gestión del archivo. • Las cuestiones relacionadas con las instalaciones y la conservación de la documentación. • Los Servicios de Archivo. • La gestión de documentos y archivos. • Los ingresos, transferencias, preparación, organización, identificación, valoración, selección, expurgo y salida de documentación. • Las consultas y servicios de la documentación. • La reprografía de fondos documentales. • El préstamo de la documentación.

[6] DECRETO 232/2000, de 21 de noviembre, por el que se aprueban el Reglamento de los Servicios de Archivo y las normas reguladoras del Patrimonio Documental del País Vasco, DECRETO 174/2003, de 22 de julio, de organización y funcionamiento del Sistema de Archivo de la Administración Pública de la Comunidad Autónoma de Euskadi y la ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Norma Nº	**150**	**15. DISPOSITIVOS DE ALMACENAMIENTO**			
Versión :	01	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:		Fecha :			
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos

Cambios destacables (desde versión anterior)

- N/A

Ámbito de aplicación :	TRATAMIENTOS NO AUTOMATIZADOS
Responsable/s :	RESPONSABLE DE SEGURIDAD SERVICIOS DE ARCHIVO USUARIOS

Descripción de la Norma :
1. Los dispositivos utilizados para el almacenamiento de documentación no automatizada, en cualquier fase de su tratamiento, tales como archivos, armarios, cajoneras, y otros de similares características, contarán con cerraduras que deberán permanecer bloqueadas siempre que el responsable de cada dispositivo de almacenamiento, no pueda custodiar el acceso al mismo, y así evitar intentos de acceso no autorizados. 2. En particular, se deberá observar lo dispuesto en el apartado anterior cuando finalice la jornada laboral, o se vaya a abandonar el puesto durante más de 1 hora. 3. Para el caso de tratamientos de documentación no automatizada que contenga datos personales de **nivel alto** (incluyendo la documentación clínica), los dispositivos de almacenamiento, se ubicarán en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave o mecanismo similar. Dichas áreas deberán permanecer cerradas cuando no se precise el acceso a los documentos que albergan.

Norma Nº	**160**		**16. ACCESO A LA DOCUMENTACION NO AUTOMATIZADA DE NIVEL ALTO**		
Versión :	01	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:		Fecha :			
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos

Cambios destacables (desde versión anterior)

- N/A

Ámbito de aplicación :	TRATAMIENTOS NO AUTOMATIZADOS DE NIVEL ALTO
Responsable/s :	RESPONSABLE DE SEGURIDAD RESPOSABLE DE AUTORIZACIÓN DE ACCESOS

Descripción de la Norma :

1. Únicamente podrá acceder a documentación no automatizada que contenga datos personales de **nivel alto** personal debidamente autorizado por el Responsable de Autorización de Accesos competente.

2. Además de lo señalado en la presente Norma y para el caso **la documentación clínica hospitalaria y la documentación clínica en atención especializada ambulatoria y en atención primaria** se deberá atender también a lo dispuesto en los siguientes documentos:

   - "*Documentación Clínica en Atención Primaria: Procedimiento de acceso para uso no asistencial*" realizado por la Comisión de Documentación Clínica Atención Primaria en Julio de 2004.

   - Procedimiento de acceso a la documentación clínica hospitalaria de la Comisión de Documentación Clínica de Mayo de 2003

3. Se deberá disponer de un Registro de Accesos al Archivo, en el cual consten todos los accesos a la documentación no automatizada que contenga datos personales de **nivel alto** (incluyendo la documentación clínica). En dicho Registro se anotará, como mínimo, la siguiente información:

   - Número de referencia del documento o documentos obtenidos.

   - Fecha y hora del acceso a la documentación.

   - Fecha y hora de la devolución de la documentación (si procede).

   - Nombre, apellidos y firma de la persona que accedió a la documentación.

4. Únicamente el personal autorizado por el Responsable de Autorización de Accesos, podrá realizar labores de **copia y reproducción** de la documentación no automatizada que contenga datos personales de **nivel alto**.

5. El personal autorizado para la realización de dichas copias y/o reproducciones, generará única y exclusivamente los ejemplares estrictamente necesarios. Si, por cualquier motivo, se generasen más copias y/o reproducciones de la mencionada documentación, se procederá, de inmediato, a su destrucción de acuerdo con lo dispuesto en la norma 110 "GESTIÓN Y CUSTODIA DE SOPORTES EN EL TRATAMIENTO NO AUTOMATIZADO DE DATOS",

Norma Nº	170	17. REALIZACION DE AUDITORIAS PERIODICAS A LOS REGISTROS DE ACCESO A LAS HISTORIAS CLINICAS			
Versión :	01	F/Implantación:	17/06/2011	F/Caducidad :	
Sustituye a:		Fecha :			
Sustituida por:		Fecha :			

Histórico de Versiones

Versión	Fecha	Documentos sustituidos

Cambios destacables (desde versión anterior)

- N/A

Ámbito de aplicación :	GENERAL
Responsable/s :	COMITE DE AUDITORIA DE HISTORIAS CLINICAS RESPONSABLE DE SEGURIDAD

Descripción de la Norma :

Este apartado define la normativa a aplicar para la realización de auditorías de los registros de accesos a las historias clínicas en los centros de OSAKIDETZA, con objeto de confirmar el adecuado funcionamiento de los sistemas de control de accesos y trazabilidad así como la autorización y justificación de los accesos habidos.

1. OSAKIDETZA realizará auditorías periódicas de los registros de accesos a las Historias Clínicas, de los registros de accesos a las Historias Clínicas Resumidas (R.D. 1093/2010) y de los registros de accesos a las Historias Clínicas de Salud Laboral, se hallen dichas Historias en soporte automatizado, no automatizado o mixto e independientemente de que sean accedidas por personal de Osakidetza, por personal de servicios sanitarios de otras Comunidades Autónomas dentro del marco de interoperabilidad (Ley 11/2007) o por los propios titulares de aquéllas (pacientes) mediante internet.

2. Se establecen cinco grupos o categorías de historias clínicas cuyos registros de acceso han de ser objeto de auditoría:

   2.1. Personalidades (personas de relevancia social) atendidas en OSAKIDETZA.

   2.2. Personal de Osakidetza atendido en OSAKIDETZA.

   2.3. Historias Clínicas especialmente protegidas (adopciones, violencia de género, cambio de sexo, etc.).

   2.4. Resto de Historias Clínicas.

   2.5. Historias Clínicas de personas que solicitan participar en el muestreo.

3. Este proceso de auditoría se ofrecerá a la ciudadanía al objeto de que puedan solicitar la inclusión de su Historia Clínica en el mismo hasta cubrir el cupo previsto en el siguiente apartado. En caso de haber más solicitantes de los previstos por dicho cupo, se seleccionarán aleatoriamente. La solicitud deberá renovarse cada año.

4. Las auditorías se realizarán anualmente, obteniendo una muestra aleatoria de 10 Historias Clínicas de cada uno de los grupos, para verificar los registros de acceso a las mismas.

5. Se designará un Comité de Auditoría de Historias Clínicas.

6. Dicho Comité realizará el proceso de auditoría y extraerá los casos que, a su juicio, presentan alguna irregularidad relacionada con los accesos a la información, con el fin de solicitar una justificación de los mismos de acuerdo a lo establecido en el

procedimiento P190.

7. En todos los casos se realizará un informe con los resultados obtenidos de la auditoría del cual se entregará una copia a la Comisión de Seguridad de OSAKIDETZA y se almacenará otra copia en las dependencias de Asesoría Jurídica de OSAKIDETZA.

8. Asimismo, se entregará un informe con los casos no justificables a la Dirección General de OSAKIDETZA, quien adoptará las medidas previstas en la legislación vigente al objeto de que se pueda investigar y sancionar, llegado el caso, al infractor.

9. Por su parte, la Comisión de Seguridad de OSAKIDETZA analizará los informes de auditoría y establecerá las medidas a adoptar para asegurar que los accesos a las Historias Clínicas son adecuados y conformes con la legislación vigente en materia de protección de datos de carácter personal.

ESTÁNDARES

Este capítulo contiene la relación de productos, servicios, mecanismos, etc. cuyas especificaciones técnicas cumplen los estándares generalmente aceptados como garantía de cumplimiento de determinados aspectos en materia de protección de datos.

Únicamente los elementos incluidos en esta relación podrán ser implementados en los sistemas de información de OSAKIDETZA, con la finalidad indicada en cada caso.

Servicios de Acceso

Tipo de Acceso	Recursos Red Interna	Recursos Internet
Desde Redes LAN	PCs sobremesa: Conectados a la red de Osakidetza. Portatiles: Conectados a la red de Osakidetza.	PCs sobremesa: Conectados a la red de Osakidetza. Portatiles: Conectados a la red de Osakidetza.
Desde Redes WIFI Corporativas	Portátiles: Conectados a la Wifi de Osakidetza Otros dispositivos (electromedicina): Conectados a la Wifi de Osakidetza	Portátiles: Conectados a la Wifi de Osakidetza
Desde JASO	Equipos desconocidos	
Desde VPN	Equipos desconocidos	
Desde Internet		Equipos desconocidos

Seguridad de Accesos

Dispositivos de Red:

Servicios	Descripción	Producto/Tecnología
Firewall	Dispositivo de control de acceso entre diferentes segmentos de red	FW Externo – CheckPoint FW Interno – CheckPoint
Detección de Intrusos	Dispositivos que trata de detectar eventos de	Mcafee IDS (Interno)

(IDS/IPS)	seguridad en la red	Mcafee IPS (Externo)
VPN	Tecnología para securizar el acceso a redes.	VPN CheckPoint (cliente VPN)
WAF	Firewall a nivel de aplicación	ASM/F5
Antivirus	Tecnologías para prevenir los efectos del malware en los puestos de usuario final	Mcafee – Puesto de usuario y servidores Bluecoat – Navegación Web IronPort/Sophos/Mcafee - eMail

Autenticación y SSO

Servicio	Descripción	Producto/Tecnlogía
Autenticación	Identificación del usuario verificada	Usuario/Contraseña SmartCards (Certificados) Kerberos Microsoft Active Directory Norbide
SSO	Acceso a diferentes entornos a partir de un único login	eSSO (Oracle) Kerberos

Certificados, Firmas Digitales y Cifrado.

Servicio	Descripción	Producto/Tecnología
PKI Interna	CA Interna de Osakidetza	Microsoft CA
PKI TPE y Cert. Públicos	CA que emite certificados de TPE y públicos	Izenpe

	reconocidos	
Documentos Seguros	Intercambio seguro de documentos	SealPath-P22
Webs Seguras	Protocolos utilizados en web seguras (HTTPS)	SSL/TLS WS-Security
Algoritmos	Utilizados en criptografía	RSA, AES

Protección de Aplicaciones Web Públicas

- WAF
- HTTPS

Servicios de Transporte

Servicio	Descripción	Producto/Tecnlogía
Transporte	Protocolos de Transporte	L3, L4: TCP/IP, IPSec
Servicios	Estándares IETF	eMail (SMTP) SNMP LDAP DHCP DNS HTTP HTTPS/SSL/TLS

ANEXOS

1. EDIFICIOS Y OFICINAS

OOSS / Centro	Servicios Centrales		
Domicilio	ALAVA, 45		
Población	VITORIA-GASTEIZ	**C. Postal**	01006

2. DESCRIPCION DE LOS SISTEMAS DE INFORMACION

La descripción de los Sistemas de Información CORPORATIVOS que almacenan y tratan Datos de Carácter Personal en OSAKIDETZA – S.V.S. se tiene en el documento anexo referenciado como “Sistemas de Información CORPORATIVOS”.

Dicho documento emana de la hoja Excel cuya responsabilidad corresponde al Servicio de Desarrollo y Mantenimiento de Aplicaciones, de la Subdirección de Informática y SS.II. corporativa.

3. EQUIPAMIENTO INFORMATICO

A continuación se describe el equipamiento informático mediante el que se realizan los tratamientos de datos de carácter personal.

La información referente al equipamiento informático es responsabilidad del Servicio de Infraestructuras, Operaciones y Comunicaciones, de la Subdirección de Informática y SS.II. corporativa.

3.1 RELACIÓN DE SERVIDORES

Esta información puede solicitarse al servicio responsable de la misma.

3.2 MODELO(S) CORPORATIVO(S) DE PUESTOS CLIENTES

Hardware:

- Microprocesador i3 de 3ª generación
- 2GB de memoria RAM

A partir de aquí no hay más requisitos, y en todo caso, los requeridos en el pliego de contratación vigente.

Software:

	Notas
Windows 7 32bits N Service pack 1	
Internet Explorer 8	*Versión de IE homologada por Osakidetza*
Servicio LPD	*Complemento para permitir la impresión de SAP / Osabide a través de impresoras locales*
Net Framework 1.1 SP1 KB867460-X86	*La plataforma .NET de Microsoft es un componente de software que puede ser añadido al sistema operativo Windows. Provee un extenso conjunto de soluciones predefinidas para necesidades generales de la programación de aplicaciones, y administra la ejecución de los programas escritos específicamente con la plataforma.*
Net Framework 2.0 y 3.5 (por defecto en S.O.)	
Net Framework 4.0 (4.0.30319)	
Java 6 u23	*Versión de Java homologada por Osakidetza*
Office 2010 Professional Plus Service pack 2 (14.0.7015.1000) - KB2687455	*Es posible que cambie a otro tipo de licencias (Office 2010 Standard). Se sigue manteniendo en equipos con versiones de maqueta anteriores(2.1 a 2.6)*

Office 2010 Standard	*(A partir de versión de maqueta 2.7)*
LIP 1.0 (2010/03/31) Windows y Office (interface en euskera) **SP2**	*Interface para Windows y Office en Euskera*
Adobe Reader XI (11.0.10)	*Visor básico de documentos PDF*
PDF Creator 2.0.2	*Impresora virtual para crear ficheros PDF*
Cliente Oracle 11.202	*Cliente Oracle que incluye ODP 10 y ODP 11*
Centura y Cristal Reports	
Citrix Receiver 3.1	*Agente Citrix que distribuye el Cliente en los equipos objetivo*
Agfa Impax Result viewer Active X	*Visor web ligero de radiología. Se está a la espera de sustituir por un software nuevo de Agfa (Xero)*
Izarc 4.1.9	*Compresor / Descompresor de ficheros. Sustitución. Se sigue manteniendo en equipos con versiones de maqueta anteriores(2.1 a 2.6)*
7ZIP	*Compresor / Descompresor de ficheros. Antes: Izarc.(A partir de versión de maqueta 2.7)*
Visor tiff (office 2007)	
Adobe Shockwave 12.1.6.156 (15/01/2015)	
Adobe Flash Player 16.0.0.305	*Versión de Flash Player homologada por Osakidetza.*
DNIe Librerías CAPICOM TC-FNMT 4.0.0 (21-noviembre-2013) (FNMT).	Librerías CAPICOM SDK 2.1.02 (FNMT)
Omega 3000/PSM. Actualizada DLL	
Middleware Universal de Izenpe 4.0.0.0	*Inlcuye Card Manager 1.8.3.0*

Usbdlm 4.7.1.0	*Gestión de letras USB*
DLL SQLORA de CENTURA	*Team Developer. En maqueta 2.1 a 2.6 - versión 5.2.2.21679*
DLLs de Cruces - Pedidos electrónicos - VFP6RESN.DLL y VFP6R.DLL	*VFP6RESN.DLL: Librería de idiomas para Visual Foxpro.* *VFP6R.DLL: Librería runtime de Visual Foxpro*
ActiveX de Eginbide	
ActiveX de CAPICOM	
Utilidad N2K	*Outlook. Utilidad recuperar libreta direcciones (Caché)*
Windows Media Feature Pack	
Infomega (Roche)	
Plug-in archivado	*Enterprise Vault de Symantec*
Norbide (C:\)	** Norbide (OIM)* ** Actualmente en C:\Norbide solamente se guarda el fichero **idCheck.jar** , que se mete por políticas*
Iconos (C:\soft\iconos)	*Iconos para las aplicaciones*
Visor Dicom Philips R3 (C:\program files)	*Visor Philips*
Calitel (C:\)	
Cliente APPV (C:\soft)	*Última versión (APPV-4.6 SP3)*
Epson M2000 (3.20.3) 20 Nov 2012 Epson M2400 (3.28.3.f) 10 Dic 2012 HP 3000 5.6.0.14430 (15 dic 2012) PCL 6 Universal M300, M200, M400 ¿M4000? Epson Net Config 4.1 CX3800N/6200 E Net Cg v3.7 y Zebra, Epson TM Lexmark C740, MS415DN,	*Drivers de impresoras*

MS510DN	
Impresoras de Roche (HP 3000, HP 4000-4050, HP 2000-2015)	
Driver teclado HP (071)	*Driver 'problemático' de teclado HP Part Number 071 antiguo (cuadrado)*
OMEGA p/ROCHE (DLL) 15/01/14	*Librería crpl32.dll*
IPV6 Habilitar (cambio por registro)	
Dejar C:\Temp control total y hidden	
Script IDE > AHCI	*Script de Bull*
Modificar Script de impresora predeterminada	
Se registran las librerías de Roche (.bat)	
Fuente Aller Cruces	
BGINFO v 4.16	*Programa para visualizar datos PC, servidor, maqueta en el escritorio*
Actualizaciones Windows	*Estamos implementando un sistema de actualizaciones mensuales en todo el parque de equipos*
BackgroundDefault.jpg	*Fondo de escritorio donde incluye el teléfono del CAU*
EPO McAfee	
Antivirus McAfee 8.7	
Cliente SCCM	
Owncloud (cliente ligero) Osabox	*Tiene que estar con la versión 32 de Firefox.* *Hay despliegue de esta aplicación virtualizada (firefox)*
ESSO	

DNIe minidriver	
Powershell	

Distribuciones por SCCM, APPv y AXIS.

No se recomienda ActiveX embebido para aplicaciones web.

RESTRICCIONES

Restricciones más importantes del usuario **estándar** con máquina **estándar** (se refiere a los usuarios que inician sesión con su DNI en una máquina normal):

- No puede explorar en la unidad C:

- No puede instalar aplicaciones

- No puede modificar las opciones de seguridad de Internet Explorer

- No puede modificar los sitios de confianza de Internet Explorer

- No puede instalar ActiveX

- No puede añadir barras ni complementos al navegador

- No puede salvar datos en USB ni soporte óptico

- El acceso a las aplicaciones puede estar restringido, bien por el pintado de menú, o bien por una capa de acceso (Norbide), dependiendo de las OUs.

- Los accesos a máquinas externas deben habilitarse expresamente, bien de forma general o bien por IP concreta (esto puede incluir las aulas)

NOTA IMPORTANTE: el acceso a Internet, a sitios de Internet, restricciones o la ejecución o instalación de ciertas aplicaciones o complementos pueden ser diferentes en algunas OUs.

3.3 PLATAFORMAS TECNOLÓGICAS

Osakidetza dispone de múltiples aplicaciones desarrolladas en diversas tecnologías (principalmente Java y .Net), y albergadas en diferentes plataformas (principalmente Apache HTTP Server y Citrix XenApp como soluciones de presentación, Oracle WebLogic y Microsoft IIS como servidores de aplicación y Oracle RDBMS y Microsoft SQL Server como servidores de BBDD).

En conjunto, el entorno tecnológico de las aplicaciones actualmente en producción en Osakidetza, es:

- Plataformas de desarrollo:
    - .NET sobre Windows 2008R2
    - Java sobre Red Hat Enterprise Linux 6.6
- Sistemas Operativos:
    - Servidores: Windows 2008 R2 Enterprise (64bits), Red Hat Enterprise Linux 6.4 (64bits)
    - Puesto de trabajo: Windows 7 Enterprise N SP1 32 bits
- Almacenamiento SAN: EMC VCPLEX y NAS Hitachi HUS
- Plataforma de virtualización: VMWare vSphere 5.5
- Servidor Web: Apache Webserver 2.2.25, Web Dispatcher de SAP Netweaver 7.0
- Servidor de Aplicaciones: MS IIS 7.5, Tomcat 6.0.32, Weblogic 11g
- Sistemas de Gestión de Bases de Datos
    - Oracle 11.2.0.3 (Standby, RAC)
    - Microsoft SQL Server Enterprise 2008
- Gestión de contenidos: MS Share Point 2010 Enterprise
- Infraestructura SOA: Oracle Service Bus 11.1.1.7
- Plataforma de firma (PKI) :Izenpe
- Autenticación basada en Directorio Activo de MS

NOTA: A medio plazo Osakidetza evolucionará:

- S.O. Windows Server 2008 R2 a Windows Server 2012 R2
- Servidor de Aplicaciones Weblogic 11g a Oracle Weblogic Server 12c
- SGBD Oracle 11g a Oracle 12c y MS SQL Server 2008 a SQL Server 2012
- IIS 8.5
- OSB12c

3.4 ENTORNO DE COMUNICACIONES

Esta información puede solicitarse al servicio responsable de la misma.

4. RELACIÓN DE ARCHIVOS DE DOCUMENTACIÓN NO AUTOMATIZADA

Esta información puede solicitarse a los servicios responsables de la misma.

5. PERFILES Y USUARIOS CON ACCESO AUTORIZADO

Para obtener la relación de los usuarios con acceso a los Sistemas de Información que tratan datos de carácter personal, así como de los diferentes perfiles de usuario, es preciso dirigir una solicitud escrita y motivada al Responsable de Seguridad indicando la denominación del Sistema de Información del que se quiere obtener el inventario.

El Responsable de Seguridad sólo entregará tal listado con autorización expresa del Responsable de Fichero.

6. PLAN DE AUDITORÍAS REGLAMENTARIAS

Al objeto de facilitar el cumplimiento de la Normativa para la realización de auditorías periódicas, según exige el Artículo 96 del R.D. 1720/2007, se incluye a continuación la relación de ficheros que han de ser sometidos a estas auditorías y el periodo de las mismas.

FICHEROS CORPORATIVOS	NIVEL	PERIODO	F/ Ult. Audit.	F/ Sig. Audit.
R. ADMINISTRATIVAS Y D. JUDICIALES	A	2 AÑOS	30/06/2014	30/06/2016
REGISTRO DE CASOS DE SIDA Y NUEVAS	A	2 AÑOS	30/06/2014	30/06/2016
REGISTRO DE DONANTES	A	2 AÑOS	30/06/2014	30/06/2016
DETECCIÓN PRECOZ DEL CÁNCER DE MAMA	A	2 AÑOS	30/06/2014	30/06/2016
P. MANTENIMIENTO - P. OBJ. INTERMED	A	BAJA 7/7/2015	30/06/2014	
REGISTRO HOSPITALARIO DEL CANCER	A	2 AÑOS	30/06/2014	30/06/2016
REGISTRO DE RECEPTORES	A	2 AÑOS	30/06/2014	30/06/2016
SIST. DE CLASIFICACIÓN DE PACIENTES	A	2 AÑOS	30/06/2014	30/06/2016
PROGRAMA ATENCIÓN DENTAL INFANTIL	A	2 AÑOS	30/06/2014	30/06/2016
CITAS	A	2 AÑOS	30/06/2014	30/06/2016
HISTORIAL CLÍNICO	A	2 AÑOS	30/06/2014	30/06/2016
GESTIÓN DE LAS DEMORAS	A	2 AÑOS	30/06/2014	30/06/2016
REGISTRO DE TUBERCULOSIS	A	2 AÑOS	30/06/2014	30/06/2016
REGISTRO DETECCIÓN SORDERA INFANTIL	A	2 AÑOS	30/06/2014	30/06/2016
INOZ - INFECCIÓN NOSOCOMIAL	A	2 AÑOS	30/06/2014	30/06/2016
REGISTRO VIDEOGRABACIONES DOCENTES	A	2 AÑOS	30/06/2014	30/06/2016
PROGRAMA CANCER DE COLON	A	2 AÑOS	30/06/2014	30/06/2016
REGISTRO DE HIPERTENSION PULMONAR	A	2 AÑOS	30/06/2014	30/06/2016
REGISTRO DE BEBES	A	2 AÑOS	30/06/2014	30/06/2016

CLIENTES	A	2 AÑOS	30/06/2014	30/06/2016
REG. SALUD PERSONAL OSAKIDETZA-SVS	A	2 AÑOS	30/06/2014	30/06/2016
GESTIÓN INTEGRADA DE RR. HH.	A	2 AÑOS	30/06/2014	30/06/2016
SELE. Y PROV. DE PUESTOS DE TRABAJO	A	2 AÑOS	30/06/2014	30/06/2016

FICHEROS SECTORIALES DE SSCC	NIVEL	PERIODO	F/ Ult. Audit.	F/ Sig. Audit.
REGISTRO DE ENTRADAS Y SALIDAS	A	2 AÑOS	30/06/2014	30/06/2016
ALUMNOS DE LA ESCUELA DE ENFERMERÍA	A	BAJA 7/7/2015	30/06/2014	
ESTUDIOS DE INVESTIGACIÓN	A	2 AÑOS	30/06/2014	30/06/2016

En los Documentos de Seguridad de las OOSS se harán constar los ficheros cuya responsabilidad corresponde a las Gerencias de dichas OOSS y que son objeto de las auditorías reglamentarias.

7. DIAGRAMAS DE RESPONSABILIDAD LINEAL

En los Procedimientos que se describen en el Documento de Seguridad, las funciones y responsabilidades establecidas para cada actividad de un proceso se representan mediante *diagramas de responsabilidad lineal*.

Dichos diagramas consisten en una matriz de actividades, por un lado, y actores involucrados, por otro. Las actividades se contemplan en las columnas de la matriz, mientras que las filas recogen los actores involucrados.

Los actores involucrados pueden ser:

- RF Responsable de Fichero
- RS Responsable de Seguridad
- ET Encargado del Tratamiento
- Usuarios Personal autorizado a tratar DCP
- Otros Se especifica cada caso concreto

La intersección [fila (actor), columna (actividad / tarea)] identifica el grado de responsabilidad del actor para cada actividad o tarea. Los grados de responsabilidad son los siguientes:

R Responsable de que la actividad se lleve a buen término.

E Ejecuta o realiza la actividad.

C Será consultado obligatoriamente por R o por E para hacer el trabajo

I Suministra o puede suministrar información (opcionalmente)

Un *diagrama de responsabilidad lineal* tipo es como sigue:

	Actividades							
	A1	**A2**	**A3**	**...**				
Actor 1								
Actor 2								
...								

Estos diagramas se establecen de acuerdo con las siguientes reglas:

1. Los actores pueden adoptar diferentes grados de responsabilidad en cada actividad.
2. Toda actividad o tarea debe tener un R (responsable).
3. Toda actividad o tarea debe tener al menos una E (al menos, un ejecutor). R y E pueden ir juntas; esto es, un actor puede ser responsable y ejecutor a la vez.
4. No podrán coincidir en la misma persona o actor los grados de responsabilidad “C” e “I” con una “E” o “R”, ni ir juntos.