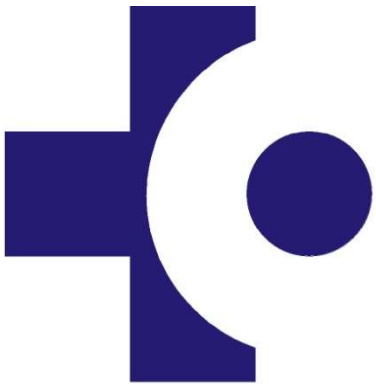

Osakidetza

ENS-PCN

Política de Seguridad de la Información

Versión: v3.0

Fecha: 28/11/2024

HOJA DE CONTROL

Título	ENS-PCN Política de Seguridad de la Información		
Nombre del Fichero	Política de Seguridad de la Información.docx		
Autor	Subdirección de informática y sistemas de información		
Organización de Servicios	Dirección General		
Versión/Edición	3.0	**Fecha Versión**	28/11/24
Aprobado por	Comisión de Seguridad de la Información y de Protección de Datos Personales	**Fecha Aprobación**	28/11/24
		Nº Total Páginas	29

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
1.0	Creación inicial del documento	RS	PyE	15/04/2015
1.4	Modificación del marco jurídico	RS	PyE	06/09/2016
2.0	Modificación	RS	Gobernanza	19/01/2023
3.0	Modificación	RS	Gobernanza	26/09/2024

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área	Nº Copias
Público			

CAMBIOS DESTACABLES (DESDE VERSIÓN ANTERIOR)

- Cambios que derivan de los requisitos del Esquema Nacional de Seguridad Real Decreto 311/2022.

ÍNDICE

1 INTRODUCCIÓN Y OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El objetivo del presente documento, es determinar el conjunto de directrices que rigen la forma en que Osakidetza gestiona y protege la información que trata y los servicios que presta.

Osakidetza estableció en su momento un marco de gestión de la seguridad de la información conforme al Real Decreto 3/2010, de 8 de enero, por el que se regulaba el Esquema Nacional de Seguridad. Con motivo de la evolución del marco regulatorio debido a la publicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), Osakidetza ha realizado la pertinente actualización y adecuación de su Política de seguridad de la información y de su sistema de gestión.

El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, para asegurar el acceso, la integridad, la disponibilidad, la autenticidad, la confidencialidad, la trazabilidad y la conservación de los datos, las informaciones y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

La misión de la implantación de este marco de referencia es la de asentar las bases sobre las cuales los trabajadores públicos y los ciudadanos puedan acceder a los servicios en un entorno de gestión seguro, anticipándonos a sus necesidades, y preservando sus derechos.

La Política de Seguridad de la Información protege a ésta de las diversas amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de Osakidetza.

La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales, jurídicos y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando y manteniendo la cultura de la seguridad en Osakidetza.

El marco de gestión de la seguridad de la información abarca igualmente la protección de los datos personales y tiene en cuenta lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, en adelante RGPD, así como lo contemplado en la legislación nacional y autonómica en dicha materia.

La gestión de la seguridad de la información ha de garantizar el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de los mismos.

Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

- Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y objetivos establecidos por Osakidetza.
- Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos personales y a la prestación de servicios a través de medios electrónicos.
- Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
- Proteger los recursos de información de Osakidetza y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad y legalidad de la información.

Esta Política de Seguridad asegura un compromiso manifiesto de las máximas autoridades de Osakidetza, para la difusión, consolidación y cumplimiento de la presente Política.

2 MARCO REGULATORIO

Está política de seguridad se sitúa dentro del marco regulatorio definido, entre otros, por las normas siguientes:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Decreto 21/2012, de 21 de febrero, de Administración Electrónica del Gobierno Vasco.
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Ley 37/2007, de 16 de noviembre, sobre la reutilización de la información del sector público.
- Reglamento UE 910/2014 (eIDAS), del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- ITS de conformidad con el Esquema Nacional de Seguridad.
- ITS de Informe del Estado de la Seguridad.
- ITS de auditoría de la seguridad de los sistemas de información.
- ITS de notificación de incidentes de seguridad.

Asimismo, resultarán de aplicación cuantas otras normas regulen la actividad de Osakidetza en el ámbito de sus competencias y aquellas otras dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos gestionados por el Ente igualmente en el ejercicio de sus competencias.

Asimismo, se deberán tener en cuenta las posibles modificaciones normativas y avances técnicos que puedan afectar al ámbito de esta Política de Seguridad.

3 OBJETIVO DE OSAKIDETZA

El objetivo prioritario de Osakidetza es garantizar a todas las personas un sistema sanitario público, universal y de calidad. La misión de Osakidetza es trabajar por la salud de todas las personas, que constituyen el eje central de todas las acciones. El derecho a la protección de la salud se entiende por lo tanto como un derecho incuestionable y constituye uno de los principios que sustentan el sistema sanitario público vasco.

Para llevar a cabo sus funciones y en la evolución que ha tenido la tecnología en el sistema sanitario, Osakidetza, apoya su actividad en los sistemas de información (SSII), que deben ser administrados con diligencia tomando las medidas de seguridad adecuadas para protegerlos frente a los daños accidentales o deliberados y las amenazas de rápida evolución y con potencial para incidir o afectar a las garantías de disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.

De una forma estrechamente relacionada con el cumplimiento de esto último, es importante resaltar la necesidad de una infraestructura de tecnologías de la información y las comunicaciones —en adelante, TIC— que prime y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio a la persona usuaria, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales. En este sentido, las TIC se constituyen como un instrumento de alto valor estratégico, debido a su potencial para impulsar la modernización de Osakidetza.

4 ALCANCE Y ÁMBITO DE APLICACIÓN

4.1 Alcance

La presente Política de Seguridad de la Información se aplicará a los servicios electrónicos prestados por Osakidetza, siendo de aplicación a todos los sistemas de información sobre los que se desarrollen dichos servicios.

4.2 Ámbito de aplicación

La presente Política de Seguridad de la Información se aplicará a todo el personal interviniente en la prestación de los servicios electrónicos que ofrece Osakidetza, tanto directa como indirectamente, independientemente de que sean personal de Osakidetza o personal externo a la organización.

Esta política se aplica a todas aquellas personas, instituciones, entidades o unidades y servicios, sean internos o externos, que participen en la prestación de los servicios y hagan uso de los recursos TIC de Osakidetza, sea mediante conexión directa o indirecta con los mismos, conexión remota o a través de equipos ajenos a la misma, incluyendo expresamente los servicios prestados a través de Internet. En adelante se considerará a todos ellos "usuarios".

Además, será de aplicación a los sistemas de información, y a todas las actividades de tratamiento de datos personales de las que es responsable Osakidetza.

5 PRINCIPIOS BÁSICOS DE SEGURIDAD

La presente Política de Seguridad de la Información se fundamenta en los siguientes principios básicos de protección que forman los pilares sobre los que se sustentan y sustentarán todas las actuaciones en materia de seguridad de la información que realice Osakidetza en su actividad.

5.1 La seguridad como proceso integral

La seguridad de la información es el resultado de un proceso integral que depende de todos y cada uno de los elementos humanos, técnicos, materiales, jurídicos y organizativos que intervienen en su tratamiento, evitando las actuaciones puntuales o tratamientos separados.

La política contará con el compromiso de todos los niveles directivos de modo que la seguridad de la información esté integrada y coordinada con las decisiones estratégicas de la organización.

Se contemplarán los aspectos de seguridad en todas las fases del ciclo de vida de los servicios, garantizando su seguridad por defecto. La seguridad se considerará como parte de la operativa habitual, estando presente y aplicando desde el diseño inicial de los sistemas de información.

5.2 Gestión de la seguridad basada en los riesgos

La gestión de la seguridad de la información está basada en la gestión de riesgos, cuyo objetivo debe ser mantener los niveles de riesgo dentro de unos niveles mínimos aceptables mediante el despliegue de las medidas de seguridad apropiadas y permanentemente actualizadas en todas las fases del ciclo de vida de las aplicaciones y servicios relacionados con el tratamiento de la información, estableciendo un equilibrio y proporcionalidad entre la naturaleza de los datos, los tratamientos realizados, los riesgos a los que estén expuestos y las medidas de seguridad aplicadas.

5.3 Prevención, detección, respuesta y conservación

La seguridad del sistema debe contemplar los aspectos de prevención, detección y respuesta para minimizar sus vulnerabilidades y conseguir que las amenazas sobre el mismo no se materialicen o que, en caso de hacerlo, no afecten gravemente a los datos que manejan los sistemas de información o los servicios que prestan.

Las medidas de prevención deberán eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse, reduciendo la superficie de exposición, mientras que las medidas de detección deberán permitir descubrir posibles ciberincidentes.

Las medidas de respuesta, gestionadas oportunamente, deberán permitir la restauración de la información y los servicios afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico y mantendrá disponibles los servicios durante todo el ciclo de vida de la información.

5.4 Existencia de líneas de defensa

Se establece una estrategia de protección constituida por múltiples capas de seguridad, compuestas por medidas de naturaleza organizativa, operativa, física y lógica, dispuestas de tal forma que, si una de ellas falla, el sistema no se vea comprometido en su conjunto, minimizando el impacto final sobre el mismo.

5.5 Vigilancia continua y reevaluación periódica

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

5.6 Diferenciación de responsabilidades, coordinación y colaboración

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos, siendo el Responsable de la Información quien determinará los requisitos de seguridad de la información tratada, el Responsable del Servicio quien determinará los requisitos de seguridad de los servicios prestados, el Responsable de Seguridad quien determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones, y el Responsable del

Sistema quien se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo.

Todos los implicados en el proceso de seguridad actuarán de manera coordinada en la aplicación y control de las medidas de seguridad, bajo la coordinación del Responsable de la Seguridad (definido más adelante). Esta coordinación se extenderá a todas las iniciativas y actuaciones de Osakidetza, en esta materia.

6 REQUISITOS MÍNIMOS DE LA SEGURIDAD

Los principios básicos de protección que forman los pilares sobre los que se sustentan y sustentarán todas las actuaciones en materia de seguridad de la información, se desarrollan aplicando los siguientes requisitos mínimos proporcionalmente a los riesgos identificados en cada sistema.

6.1 Organización e implantación del proceso de seguridad

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

La política deberá ser conocida por todas las personas que formen parte de la organización e identificar a los responsables de velar por su cumplimiento: responsable de la información, responsable del servicio, responsable de la seguridad y responsable del sistema.

6.2 Análisis y gestión de los riesgos

La organización realizará la gestión de riesgos mediante la elaboración del análisis y tratamiento de riesgos a los que está expuesto el sistema, empleando una metodología reconocida internacionalmente.

Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y existirá una proporcionalidad entre ellas y los riesgos.

6.3 Gestión de personal

El personal, propio o ajeno, estará formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que se supervisará para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la persona titular de la dirección general a propuesta de la Comisión de Seguridad de la Información y de Protección de Datos Personales.

6.4 Profesionalidad

La seguridad de los sistemas de información estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

La organización determinará los requisitos de formación y experiencia necesarias de este personal.

6.5 Autorización y control de los accesos

El acceso controlado a los sistemas de información deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

6.6 Protección de las instalaciones

Los sistemas de información y su infraestructura de comunicaciones deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

6.7 Adquisición de productos de seguridad y contratación de servicios de seguridad

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por Osakidetza se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, observando los requisitos y criterios que establezca el Centro Criptológico Nacional.

6.8 Mínimo privilegio

Los sistemas de información serán diseñados otorgando los mínimos privilegios posibles para su correcto desempeño, proporcionando la funcionalidad imprescindible para que Osakidetza alcance sus objetivos siendo las funciones de operación, administración y registro, las mínimas necesarias para ello y asegurando que sólo son desarrolladas por las personas autorizadas desde recursos asimismo autorizados.

Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, desactivando las funciones innecesarias o inadecuadas.

6.9 Integridad y actualización del sistema

Para la inclusión o modificación de cualquier elemento físico o lógico en el sistema, se requerirá autorización formal previa.

En todo momento se conocerá el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, las deficiencias de configuración, las vulnerabilidades y las actualizaciones que les afecten, así como la detección temprana de incidentes sobre aquellos, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

6.10 Protección de la información almacenada y en tránsito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros (equipos o dispositivos portátiles o móviles, periféricos, soportes, y redes abiertas, etc.). Se garantizará la conservación de los documentos electrónicos producidos por los sistemas. Toda la información en soporte no electrónico que sea causa o consecuencia directa de la información electrónica de los sistemas, también estará protegida al mismo nivel.

6.11 Prevención ante otros sistemas de información interconectados

Se protegerá el perímetro del sistema de información, especialmente, en el caso de conectarse a redes públicas, reforzándose las tareas de prevención, detección y respuesta ante incidentes de seguridad. Se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas y se controlará su punto de unión.

6.12 Registro de actividad y detección de código dañino

Con el propósito de satisfacer el objeto del ENS, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Se podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino, así como otros daños a las antedichas redes y sistemas de información.

Cada usuario que acceda al sistema de información estará identificado de forma única, al objeto de conocer en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

6.13 Incidentes de seguridad

Osakidetza dispondrá de procedimientos de gestión de incidentes de seguridad, incluyendo asimismo mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como cauces de comunicación con las partes interesadas y el registro de las actuaciones. Este registro se utilizará para la mejora continua de la seguridad del sistema.

6.14 Continuidad de la actividad

Se dispondrá de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

6.15 Mejora continua del proceso de seguridad

Se actualizará y mejorará el proceso integral de seguridad de una forma continua, aplicando para ello criterios y métodos reconocidos en materia de seguridad de las TIC.

7 ORGANIZACIÓN DE LA SEGURIDAD

Para garantizar que todas las etapas del ciclo de vida de protección de la información sean realizadas de manera apropiada y las responsabilidades para su ejecución sean asignadas adecuadamente, Osakidetza establece una estructura que permite promover la aplicación consistente de la presente política y acomodar efectivamente los frecuentes cambios tecnológicos y organizativos.

Para ello, según lo dispuesto por el ENS, se definen los siguientes comités y roles generales relacionados con su participación en la gestión y supervisión de la seguridad de la información:

- Responsables de la Información.
- Responsables de los Servicios.
- Responsable de la Seguridad de la Información.
- Responsables de los Sistemas de Información.
- Comité de Seguridad de la Información, denominado en Osakidetza: Comisión de Seguridad de la Información y de Protección de Datos Personales.

7.1 Responsables de la Información

Los Responsables de la Información establecerán los requisitos de seguridad aplicables a la información bajo su responsabilidad. Este rol lo desempeñan las personas titulares de la Dirección General y de las Direcciones de División o personas en las que deleguen, asumiendo las siguientes responsabilidades específicas:

- Definir para la información bajo su responsabilidad, las dimensiones de la seguridad relevantes (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente.
- Establecer los requisitos de la información en materia de seguridad que deban ser garantizados en el tratamiento de la información.
- Cualquier otra función que se entienda pertinente en el ámbito de las funciones generales que les corresponden, en materia de seguridad de la información.

7.2 Responsables de los Servicios

Los Responsables de los Servicios establecerán los requisitos de seguridad aplicables a los servicios bajo su responsabilidad. Este rol lo desempeñan las

personas titulares de las Subdirecciones corporativas de Asesoría Jurídica, de la Dirección de Asistencia Sanitaria, de la Dirección Económico-Financiera, de la Dirección de Recursos Humanos y cuantas otras Subdirecciones de Organizaciones de Servicios pudieran tener competencia directa en materias que se prestasen como servicios públicos electrónicos, así como aquellas otras personas en las que las anteriores pudieran delegar, asumiendo las siguientes responsabilidades específicas:

- Definir para los servicios electrónicos bajo su responsabilidad, las dimensiones de la seguridad relevantes (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente.
- Determinar para los servicios electrónicos bajo su responsabilidad la evolución del impacto de una indisponibilidad en función del tiempo.
- Establecer los requisitos de los servicios en materia de seguridad que deban ser garantizados en el tratamiento de la información.
- Colaborar en el análisis de impacto de los incidentes que se puedan producir y plantear las estrategias y salvaguardas ante los mismos.
- Cualquier otra función que se entienda pertinente en el ámbito de las funciones generales que les corresponden, en materia de seguridad de la información.

7.3 Responsable de la Seguridad

El Responsable de la Seguridad tomará las decisiones necesarias para satisfacer los requisitos de seguridad establecidos por los Responsables de la Información y de los Servicios. Este rol lo desempeña la persona titular de la Subdirección de Informática y Sistemas de Información de Osakidetza, asumiendo las siguientes responsabilidades específicas:

- Determinar las medidas de seguridad necesarias para la protección de la información manejada y los servicios prestados y verificar que las establecidas son adecuadas en todo momento, aprobando formalmente la Declaración de Aplicabilidad.
- Determinar la categoría del sistema y las medidas de seguridad que deben aplicarse, en función de las valoraciones previamente realizadas por los responsables de los servicios y de la información.
- Coordinar las tareas periódicas derivadas de la revisión y mantenimiento del Análisis de Riesgos y del Análisis de Impacto.
- Reportar el estado de la seguridad a la Comisión de Seguridad de la Información y de Protección de Datos Personales.
- Impulsar o instar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.
- Llevar a cabo el seguimiento de la operativa de la Política de Seguridad.

- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar un informe periódico de seguridad, que incluya los incidentes más relevantes del periodo.
- Informar a la Comisión de Seguridad de la Información y de Protección de Datos Personales de los incidentes de seguridad de carácter grave.
- Proponer la modificación de aquellas normas, instrucciones y directrices técnicas que considere necesaria en materia de seguridad a la Comisión de Seguridad de la Información y de Protección de Datos Personales.
- Decidir la aprobación de los procedimientos de seguridad elaborados por los Responsables de los Sistemas, y procurar su implementación.
- Cualquier otra función que se entienda pertinente en materia de seguridad, no atribuida específicamente a cualquier otro órgano de los contemplados en el presente documento.

7.4 Responsables de los Sistemas

Serán los encargados de aplicar las medidas de seguridad de índole tecnológica determinadas por el Responsable de la Seguridad. Este rol lo desempeñan los responsables de los servicios de la Subdirección de Informática y Sistemas de Información de Osakidetza, asumiendo dentro de su ámbito de competencia, las siguientes responsabilidades específicas:

- Garantizar que las tareas propias de la administración de la seguridad de los sistemas bajo su responsabilidad se llevan a cabo de manera correcta.
- Garantizar que los sistemas de información de los que es responsable permanecen bajo control.
- Llevar a cabo los procesos de seguridad en el ámbito de su área.
- Implementar la seguridad dentro de su área, gestionando y manteniendo las medidas de seguridad aplicables a los sistemas de información conforme al ENS.
- Colaborar en las auditorias de seguridad y en la gestión de riesgos.
- Cualquier otra función que se entienda pertinente en el ámbito de las funciones generales que les corresponden, en materia de seguridad de la información.

7.5 Comité de Seguridad. La Comisión de Seguridad de la Información y de Protección de Datos Personales

El comité de seguridad es el órgano colegiado que dirige, gestiona, coordina, establece y aprueba las actuaciones en materia de seguridad.

Este comité será el órgano en el que se resolverán los conflictos que puedan surgir en la aplicación de esta política de seguridad o de las normas y procedimientos que la desarrollen.

El referido comité tendrá la concreta denominación de: "Comisión de Seguridad de la Información y de Protección de Datos Personales".

La composición y el régimen de funcionamiento de esta Comisión serán los que acuerde al respecto la Dirección General de Osakidetza, quedando adscritos a la misma sus vocales, secretario y presidente, automáticamente en virtud de sus cargos, conforme al vigente Acuerdo del Consejo de Administración del Ente por el que se establezca y/o modifique su composición.

La Comisión de Seguridad de la Información y de Protección de Datos Personales recabará información y auxilio de todas las áreas de Osakidetza cuando así lo considere necesario.

Todos los servicios y unidades de Osakidetza estarán obligados a informar y prestar apoyo a la Comisión de Seguridad de la Información y de Protección de Datos Personales cuando ésta así lo requiera en materias de su competencia.

La Comisión de Seguridad de la Información y de Protección de Datos Personales será informada de cuantos incidentes de seguridad relevantes hayan sido detectados en las diferentes Organizaciones de Servicios del Ente, sin que ello implique que la intervención de la Comisión sea preceptiva para promover, en su caso, la apertura de un período de Informaciones Previas y/o la instrucción de procedimientos disciplinarios, si se hubiera constatado algún incumplimiento de las medidas de seguridad aplicables.

Esta Comisión de Seguridad de la Información y de Protección de Datos Personales tiene las siguientes funciones y responsabilidades adicionales concretas:

- Divulgar esta Política de Seguridad y la documentación elaborada dentro del marco normativo de dicha política.
- Informar del estado de la seguridad a los órganos de gobierno de Osakidetza.
- Interpretar e instar la resolución de los conflictos de responsabilidad surgidos en materia de seguridad.

- Comunicar a los órganos competentes el incumplimiento de la Política de Seguridad y las normas derivadas, e instar, en su caso, la adopción de las medidas correctoras correspondientes.
- Promover la mejora continua de la seguridad.
- Elaborar, revisar y hacer el seguimiento regularmente de esta Política de Seguridad y demás normas generales, proponiendo a los órganos de gobierno de Osakidetza las modificaciones que considere pertinentes.
- Elaborar e impulsar la estrategia y nuevas líneas de trabajo en lo que respecta a la seguridad.
- Priorizar las actuaciones en materia de seguridad.
- Supervisar y llevar a cabo el seguimiento del proceso de seguridad.
- Supervisar los incidentes de seguridad que se hayan podido producir y las medidas aplicadas en cada caso.
- Supervisar los resultados de las auditorias.
- Supervisión y aprobación de las tareas de seguimiento del ENS.

Hay previstas anualmente 3 sesiones de la Comisión de Seguridad de la Información y de Protección de Datos Personales, y se podrían celebrar reuniones extraordinarias si así se requiriese.

Las sesiones de la Comisión quedaran conformadas mediante quórum de la mitad de sus miembros incluyendo al Presidente y Secretario, como mínimo.

La composición de la Comisión de Seguridad de la Información y de Protección de Datos Personales se recoge en el vigente Acuerdo del Consejo de Administración del Ente por el que se establezca y/o modifique su composición.

8 OBLIGACIONES ASOCIADAS

8.1 Obligaciones de los usuarios

Todos los usuarios de Osakidetza tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa e instrucciones de seguridad desarrolladas a partir de ella, siendo responsabilidad de la Comisión de Seguridad de la Información y de Protección de Datos Personales disponer los medios necesarios para que la información llegue a los afectados.

Todos los usuarios de Osakidetza deben ser conscientes de la necesidad de garantizar la seguridad de los sistemas de información, así como de que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad.

8.2 Responsabilidades de los usuarios en caso de incumplimiento

La Comisión de Seguridad de la Información y de Protección de Datos Personales podrá evaluar si por parte de alguno de los usuarios de Osakidetza ha podido existir algún tipo de incumplimiento en las obligaciones previstas en la Política de Seguridad de la Información o en su normativa e instrucciones de desarrollo.

En caso de que se aprecie un posible incumplimiento, se adoptarán medidas preventivas y correctoras encaminadas a salvaguardar y proteger los sistemas de información.

Igualmente, detectado un posible incumplimiento de la Política de Seguridad de la Información de Osakidetza, la Comisión de Seguridad de la Información y de Protección de Datos Personales podrá instar, a los órganos correspondientes, la instrucción de los procedimientos disciplinarios que se consideren convenientes.

El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario del personal al servicio de las Administraciones Publicas o de la propia Osakidetza.

8.3 Relación con terceros

Cuando Osakidetza preste servicios a otros organismos o maneje información de los mismos, el responsable de esa relación les hará partícipe de esta política de seguridad y de las normas e instrucciones derivadas. Se establecerán canales de comunicación y coordinación entre los Responsables de Seguridad

correspondientes, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Asimismo, cuando Osakidetza utilice servicios de terceros o ceda información a terceros, el responsable de esa relación les hará igualmente partícipes de esta política de seguridad y de la normativa e instrucciones de seguridad que ataña a dichos servicios o información.

Dichos terceros quedarán sujetos a las obligaciones y medidas de seguridad establecidas en las respectivas normas e instrucciones, debiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de prevención, detección, reporte y resolución de incidencias, siempre con el objetivo de que los terceros estén adecuadamente concienciados en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad.

En concreto, los terceros deberán garantizar el cumplimiento de políticas de seguridad basadas en estándares auditables y someterse a cuantos controles y revisiones se entiendan pertinentes para acreditar el cumplimiento de esta política.

Cuando algún aspecto de esta política de seguridad no pueda ser satisfecho por los terceros, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los Responsables de la Información y de los Servicios afectados antes de seguir adelante.

9 DESARROLLO Y DESPLIEGUE DE LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

La Comisión de Seguridad de la Información y de Protección de Datos Personales revisará la Política de seguridad de la información regularmente o cuando exista un cambio significativo que obligue a ello. La propuesta de revisión, en su caso, será aprobada y difundida para que la conozcan todas las partes afectadas.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

La entrada en vigor de la presente Política de Seguridad de la Información de Osakidetza supone la derogación de cualquier otra que pudiera existir a nivel de las diferentes organizaciones de servicios de Osakidetza.

Para su desarrollo Osakidetza establece un marco documental estructurado en diferentes niveles, de forma que las directrices marcadas por el presente documento tengan un desarrollo específico. En cualquier caso, las diferentes políticas, normas y regulaciones específicas que se desarrollen deberán estar alineadas con la presente política de seguridad y derivarse de la misma.

La composición del citado marco documental es la siguiente:

- *Primer nivel*: la propia POLÍTICA DE SEGURIDAD de la Información de los Servicios Electrónicos de Osakidetza.
- *Segundo nivel*: las NORMAS GENERALES de seguridad que emanan de la Política de Seguridad de la Información y soportan los diferentes ámbitos de la seguridad.
- *Tercer nivel*: los PROCEDIMIENTOS generales, como conjunto de documentos que describen las pautas específicas a seguir a la hora de realizar una determinada actividad relacionada con la seguridad de la información.
- *Cuarto nivel*:
  - GUIAS, documentos que describen pautas a seguir por personal de la subdirección de informática,
  - MANUALES, documentos que describen pautas a seguir por todos los usuarios de Osakidetza.

La Política de Seguridad de la Información será aprobada por el Consejo de Administración de Osakidetza a propuesta de la Comisión de Seguridad de la Información y de Protección de Datos Personales, mientras que las normas generales del segundo nivel serán aprobadas por la Comisión de Seguridad de la Información y de Protección de Datos Personales a propuesta del Responsable de Seguridad de la Información, y los procedimientos del tercer nivel lo serán por el Responsable de Seguridad de la Información, en colaboración, si fuese necesaria, con los

Responsables de los Servicios y de los de Sistemas. Las guías, manuales y demás documentación del cuarto nivel serán aprobados por el Responsable de sistemas.

Las normas generales de seguridad (segundo nivel) aprobadas por la Comisión de Seguridad de la Información y de Protección de Datos Personales deberán adoptarse por Resolución de la Dirección General de Osakidetza, cuyo incumplimiento podrá dar lugar a la correspondiente responsabilidad disciplinaria.

La presente Política de Seguridad de la Información, las normas generales y el resto de documentación específica que se apruebe deberán ser comunicadas a todos los responsables de los servicios afectados. La Política de Seguridad de la Información se publicará en la página web de Osakidetza; las normas generales y el resto de documentación específica han de quedar publicadas en la intranet de Osakidetza.

10 FORMACIÓN Y CONCIENCIACIÓN

Osakidetza desarrollará actividades orientadas a la formación y concienciación de todo el personal en materia de seguridad de la información y protección de datos personales, así como a la difusión de la Política de seguridad de la información y de su desarrollo normativo, particularmente dirigidas al personal de nueva incorporación, de modo que garantice que sus empleados conocen, entienden y cumplen las normas y las medidas de protección en materia de seguridad adoptadas, advirtiéndoles de los riesgos que puede suponer un mal uso de los dispositivos y soluciones tecnológicas a su alcance.

Todas las personas con responsabilidad en el uso, operación o administración de sistemas TIC deben estar capacitadas para el manejo seguro de los sistemas, por consiguiente, recibirán formación específica en la medida en que la necesiten para realizar su trabajo.

11 PROTECCIÓN DE DATOS PERSONALES

A los efectos de la protección de los datos personales será de aplicación lo contemplado en el Reglamento General de Protección de Datos y lo dispuesto en la legislación nacional y autonómica en dicha materia.

Cada área de Osakidetza se encargará de gestionar y mantener la seguridad referente a los datos personales incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad.

Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas, conforme a la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Todos los sistemas de información de Osakidetza se ajustarán a los requisitos de seguridad establecidos por dicha normativa.

12 CLASIFICACIÓN DE LA INFORMACIÓN

El Responsable de la Información clasificará e inventariará los activos de la información en virtud de su naturaleza, de acuerdo con lo establecido en la presente Política de Seguridad de la Información. El nivel de protección y las medidas a aplicar se basarán en el resultado de dicha clasificación.

La información que tratan los sistemas de información, estará calificada en una de las siguientes categorías por orden descendente de importancia:

- **Reservada**:
  - *Restringida*: Esta información está disponible para usuarios con acceso restringido y su pérdida, corrupción o publicación no autorizada causaría un daño grave o muy grave a la reputación de Osakidetza, a sus funciones, o produciría pérdidas financieras o consecuencias legales graves o muy graves.
  - *Confidencial*: Esta Información está disponible para usuarios autorizados, y su pérdida, corrupción o publicación no autorizada pueden causar alguna pérdida financiera o consecuencia legal a Osakidetza o a nivel individual.
  - *Uso interno*: Esta información está disponible para usuarios autorizados y su pérdida o corrupción no causaría más que alguna disfunción operativa cotidiana o cuya publicación no autorizada puede causar problemas de credibilidad o reputación personal.
- **Pública**:
  - Esta información está disponible y accesible para el público en general.