EUSKO JAURLARITZA
GOBIERNO VASCO

GureSeK

Sistema de Gestión

de la Seguridad de la Información

de la Administración Pública Vasca

Política de Seguridad y Privacidad de la Información

Honek onartua *Aprobado por*	Comité de Seguridad Corporativa	***Erreferentzia*** *Referencia*	Política de seguridad y privacidad de la información
Data *Fecha*	17-11-2020	***Jasotzaileak*** *Distribución*	A todo el personal

SEGURTASUN SAILKAPENA / CLASIFICACIÓN DE SEGURIDAD									
Erabilgarritasuna Disponibilidad	BAJA	**Osotasuna** Integridad	BAJA	**Konfidentzialtasuna** Confidencialidad	BAJA	**Benetakotasuna** Autenticidad	BAJA	**Trazabilitatea** Trazabilidad	BAJA

Contenido

1. Introducción

El Esquema Nacional de Seguridad (ENS) en su artículo 11 y en la medida org.1 del Anexo II, dice que «***se debe disponer formalmente de una política de seguridad***»; establece la necesidad de que obtenga la aprobación por parte de la persona titular del órgano superior competente, y que debe contener:

- Los objetivos o misión de la organización
- El marco legal y regulatorio en el que se desarrollarán las actividades
- Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación
- La estructura de los comités de seguridad para la gestión y coordinación de la seguridad y la privacidad, detallando su ámbito de responsabilidad, cada miembro y la relación con otros elementos de la organización
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso

Como referencia para la Administración Pública de la Comunidad Autónoma de Euskadi en materia de Seguridad de la Información, la Norma UNE-ISO/IEC 27001, en su apartado 5.2, también indica que se debe disponer de una política de seguridad.

Una política de seguridad de la información identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

La política de seguridad y privacidad de la información es el instrumento en que se apoya la Administración Pública de la CAE para alcanzar sus objetivos, utilizando de forma segura los sistemas de información y las comunicaciones. **La seguridad**, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales 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 la cultura de la seguridad en la Administración Pública Vasca.

1.1 *Desarrollo de un cuerpo normativo de seguridad y privacidad*

El cuerpo normativo sobre seguridad y privacidad de la información es de obligado cumplimiento y se desarrollará en niveles, según el ámbito de aplicación y el nivel de detalle técnico, de manera que cada norma se fundamente en las normas de nivel superior. Dichos niveles de desarrollo son los siguientes:

#	Nivel	Descripción
1	**Política** de seguridad y privacidad de la información	Está constituida por el presente documento y es de obligado cumplimiento.
2	**Normas** de seguridad y privacidad: instrucciones, planes de acción y actuaciones estratégicas en materia de seguridad y privacidad de la información	Documentos que sirven para indicar cómo se debe actuar, tanto de manera adecuada como en caso de que una cierta circunstancia no esté recogida en un procedimiento explícito. Es el conjunto de regulaciones que desarrollan la política de seguridad y privacidad y tratan de su aplicación. Cada norma deberá: a) Centrarse en los objetivos que se desean alcanzar, antes que en la forma de lograrlo. Las normas ayudan a tomar la decisión correcta en caso de duda b) Describir lo que se considera uso correcto, así como lo que se considera uso incorrecto c) Indicar la forma de localizar los procedimientos de seguridad y privacidad que se han desarrollado en la materia tratada d) Ser concisa, motivada y descriptiva, y definir puntos de contacto para su interpretación correcta e) Explicar cómo actuar ante situaciones anómalas y no previstas f) Describir la responsabilidad del personal con respecto al cumplimiento o violación de la norma: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente
3	**Procedimientos** de seguridad y privacidad	Conjunto de documentos que describen explícitamente y paso a paso como realizar una cierta actividad, según las directrices de carácter técnico o procedimental que se deben observar. Cada procedimiento debe detallar: a) En qué condiciones debe aplicarse b) Quiénes son las personas que deben llevarlo a cabo c) Qué es lo que hay que hacer en cada momento, incluyendo, en su caso, el registro de la actividad realizada d) Cómo se miden y evalúan sus resultados e) Cómo se reportan posibles mejoras y deficiencias en los procedimientos
4	Otros documentos	Además de los documentos citados, la documentación de seguridad y privacidad podrá contar con otros adicionales, como son: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

2. Principios de seguridad y privacidad

La Política de seguridad y privacidad de la información de la Administración Pública de la CAE se desarrollará, con carácter general, de acuerdo con los siguientes principios:

#	Principio	Descripción
1	**Seguridad integral**	La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema, excluyendo cualquier actuación puntual o tratamiento coyuntural. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas sean fuentes de riesgo para la seguridad ni para la privacidad. Los requerimientos de la seguridad y la privacidad de la información se atenderán durante todo el ciclo de vida de los activos, desde su planificación hasta su retirada.
2	**Gestión del riesgo**	Gestionar la seguridad y privacidad de la información consiste en analizar los riesgos, establecer medidas de seguridad adecuadas, eficaces y proporcionadas, e incluir la corrección y mejora continuas que lleven a que la organización sea, cada vez, más preventiva que reactiva frente a los incidentes de seguridad, permitiendo el mantenimiento de un entorno controlado. Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y privacidad, y deberá mantenerse permanentemente actualizado.
3	**Disponibilidad, continuidad y conservación**	Se debe procurar que los activos estén disponibles cuando lo requieran las personas autorizadas para acceder a ellos. Para ello, se garantizará la prestación continuada de los servicios y la rápida recuperación ante posibles contingencias, mediante medidas de continuidad orientadas a la restauración de los servicios y de la información asociada a ellos. Así mismo se garantizará la conservación de los datos e informaciones en soporte electrónico. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.
4	**Integridad**	Se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.
5	**Confidencialidad**	Se deberá garantizar que los activos sean accesibles únicamente para aquellas personas expresamente autorizadas para ello.
6	**Autenticidad**	Se deberá garantizar que la información proceda y se intercambie con las personas idóneas para la interlocución y que los servicios se acrediten correctamente.

#	Principio	Descripción
7	**Trazabilidad**	Se deberá garantizar el seguimiento de las operaciones efectuadas sobre la información y los servicios que lo requieran.
8	**Prevención, reacción y recuperación**	Se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad o la privacidad. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen o, de producirse, no afecten gravemente a la información que maneja o a los servicios que se prestan. Las medidas de prevención deben eliminar, o al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema, contemplando, entre otras, la disuasión y la reducción a la exposición. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad o privacidad inhabilite los medios habituales.
9	**Escalonamiento**	Los sistemas han de disponer de una estrategia de protección en líneas de defensa, constituida por múltiples capas de seguridad dispuestas de forma que cuando una de las capas falle, permita: a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto c) Minimizar el impacto final sobre el mismo Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.
10	**Mejora continua y reevaluación periódica**	Se revisará de manera recurrente el grado de eficacia de los controles de seguridad y privacidad implantados en la organización para aumentar la capacidad de adaptación a la constante evolución de los riesgos y del entorno tecnológico. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.
11	**Proporcionalidad en coste**	La implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.
12	**Concienciación y formación**	Se articularán programas de formación, sensibilización y concienciación para las personas usuarias en materia de seguridad y privacidad de la información, debidamente apoyados en las políticas corporativas y con un acomodado proceso de seguimiento y actualización.

#	Principio	Descripción
13	**Función diferenciada**	Conforme a la exigencia legal de considerar la seguridad como una función diferenciada en la Administración, la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios. La política de seguridad y privacidad detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.
14	**Cumplimiento normativo**	Todos los sistemas de información, así como cualquier proceso relacionado, se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad y privacidad de la información, en especial aquella relacionada con la intimidad y la protección de datos de carácter personal y con la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de la tecnología.

3. Directrices

La Política de seguridad y privacidad de la información de la Administración Pública de la Comunidad Autónoma de Euskadi es la desarrollada en los apartados siguientes.

3.1 *Objetivo del Gobierno Vasco*

La misión del Gobierno Vasco es construir una **Administración innovadora y abierta** que ofrezca a la sociedad servicios de **calidad, eficientes, eficaces y seguros**, en colaboración con su entorno y con la **participación activa** de la ciudadanía, contando con las **personas como protagonistas del cambio**, y todo ello basado en los nuevos **valores de gobernanza**: apertura, orientación a resultados, transparencia e innovación.

Para conseguir este objetivo 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 que pued en afectar a las garantías de disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.

De forma estrechamente relacionada con el cumplimiento de esta misión, 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 nivel estratégico, debido a su potencial para impulsar la modernización de la Administración Pública de la Comunidad Autónoma de Euskadi, así como a su capacidad para estimular y sustentar el desarrollo social y económico de Euskadi. Por tanto, es imprescindible que los sistemas TIC sean administrados con diligencia, y también tomar las medidas adecuadas para protegerlos de amenazas de rápida evolución y con potencial para incidir en las garantías o dimensiones anteriormente citadas.

3.2 *Marco normativo*

El marco normativo de las actividades de la Administración Pública de la Comunidad Autónoma de Euskadi en el ámbito de esta Política de Seguridad y Privacidad de la Información está integrado por las siguientes normas:

#	Norma	Fecha	Descripción	Finalidad
1	**Ley 15/1999**	13 de diciembre	de Protección de Datos de carácter personal. Derogada por la Ley 3/2018, salvo artículos 22, 23 y 24.	aporta criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger
2	**RD 1720/2007**	21 de diciembre	por el que se aprueba el Reglamento de desarrollo de la LOPD	Desarrolla y complementa el contenido de la Ley Orgánica 15/1999, de Protección de Datos de carácter personal.
3	**Ley 34/2002**	11 de julio	de servicios de la sociedad de la información y de comercio electrónico	regula determinados aspectos jurídicos de los servicios de la sociedad de la información, como pueden ser, el comercio electrónico, la contratación en línea, la información y publicidad y los servicios de intermediación
4	**Ley 59/2003**	19 de diciembre	de Firma Electrónica. Modificada por la Ley 39/2015.	regula la firma electrónica (que surge como respuesta a la necesidad de conferir seguridad a las comunicaciones por Internet), su eficacia jurídica y la prestación de servicios de certificación; deberá adaptarse a lo que dice el Reglamento UE 910/2014 (más conocido como eIDAS)
5	**Ley 11/2007**	22 de junio	de Acceso Electrónico de los Ciudadanos a los Servicios Públicos Derogada por la Ley 39/2015.	regula las bases de la Administración Electrónica, estableciendo los principios generales que rigen la prestación de servicios públicos mediante el uso de medios electrónicos, creando las condiciones de confianza en el uso de los medios electrónicos, y establece las medidas necesarias para la preservación de la integridad de los derechos fundamentales, en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos

#	Norma	Fecha	Descripción	Finalidad
6	**Ley 25/2007**	18 de octubre	de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones	estipula cómo conservar los datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones (transposición de la Directiva 2006/24/CE)
7	**Ley 37/2007**	16 de noviembre	sobre reutilización de la información del sector público	Establece un conjunto mínimo de normas que regulan la reutilización y los instrumentos prácticos para facilitar la reutilización de los documentos existentes conservados por organismos del sector público de los Estados miembros (transposición de la Directiva 2003/98/CE sobre la conservación y reutilización de la información del sector público).
8	**Decreto 232/2007**	18 de diciembre	por el que se regula la utilización de medios electrónicos, informáticos y telemáticos en los procedimientos administrativos	Garantiza a la ciudadanía el pleno ejercicio de los derechos reconocidos en las leyes, y posibilita a los órganos y personal de la Administración Pública el cumplimiento de las obligaciones que les vienen impuestas por el ordenamiento jurídico.
9	**Ley 56/2007**	28 de diciembre	de Medidas de Impulso de la Sociedad de la Información	Enmarca el conjunto de medidas que constituyeron el Plan Avanza 2006-2010 para el desarrollo de la Sociedad de la Información y de convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas, aprobado por el Gobierno en noviembre de 2005, continuado por el Plan Avanza 2 (2011-2015).
10	**RD 1671/2009**	6 de noviembre	por el que se desarrolla parcialmente la Ley 11/2007. Derogado en parte por las Leyes 39 y 40/2015.	Desarrollo parcial de la Ley 11/2007 en lo relativo a la transmisión de datos, sedes electrónicas y punto de acceso general, identificación y autenticación, registros electrónicos, comunicaciones y notificaciones, y documentos electrónicos y copias.

#	Norma	Fecha	Descripción	Finalidad
11	**RD 3/2010**	8 de enero	por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica	Crea las condiciones necesarias de confianza en el uso de los medios electrónicos, para lo cual establece los principios básicos y requisitos mínimos a cumplir en materia de seguridad, así como una serie de medidas de seguridad específicas que se deben aplicar.
12	**RD 4/2010**	8 de enero	por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica	Determina los criterios de seguridad, normalización (estandarización) y conservación de la información de los sistemas informáticos de la Administración Pública, con el objetivo de asegurar la interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios.
13	**Orden**	26 de febrero	aprobando el Manual de Seguridad para el mantenimiento de la seguridad de la información de la Administración General de la CAPV y sus Organismos Autónomos	Mantiene la seguridad de la información en el entorno de las aplicaciones informáticas que sirven de soporte a la tramitación telemática (Administración Electrónica).
14	**Decreto 21/2012**	21 de febrero	de Administración Electrónica	Regula los medios electrónicos necesarios para que las relaciones entre la ciudadanía y la Administración sean seguras, ágiles y con plenas garantías jurídicas.
15	**Ley 9/2014**	9 de mayo	General de Telecomunicaciones	Regula las telecomunicaciones, que comprenden la explotación de las redes, y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados.
16	**Reglamento UE 910/2014 (eIDAS)**	9 de julio	del Parlamento Europeo y del Consejo	Vela por la interoperabilidad respecto a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (deroga la Directiva 1999/93/CE).

#	Norma	Fecha	Descripción	Finalidad
17	**Ley 39/2015**	1 de octubre	del Procedimiento Administrativo Común de las AAPP	Regula los requisitos de validez y eficacia de los actos administrativos, el PAC a todas las AAPP, incluyendo el sancionador y el de reclamación de responsabilidad de las AAPP, así como los principios a los que se ha de ajustar el ejercicio de la iniciativa legislativa y la potestad reglamentaria, estableciendo la obligación de cumplir con el Esquema Nacional de Seguridad.
18	**Ley 40/2015**	1 de octubre	de Régimen Jurídico del Sector Público	Establece y regula las bases del régimen jurídico de las AAPP, los principios del sistema de responsabilidad de las AAPP y de la potestad sancionadora, así como la organización y funcionamiento de la AGE y de su sector público institucional para el desarrollo de sus actividades, estableciendo la aplicación del Esquema Nacional de Seguridad en dichas actividades.
19	**RD 951/2015**	23 de octubre	de modificación del ENS	Actualiza el ENS, adoptando en cada momento los mecanismos que mejoren la respuesta en materia de seguridad de los sistemas tecnológicos utilizados en la Administración, en particular frente a las ciberamenazas, y reforzando los servicios de confianza y la protección para las transacciones electrónicas.
20	**Reglamento (UE) 2016/679**	de 27 de abril	Reglamento General de Protección de Datos	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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
21	**Ley 3/2018**	de 5 de diciembre	Protección de Datos Personales y Garantía de los Derechos Digitales	a) Adapta el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completa sus disposiciones. b) Garantiza los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución

#	Norma	Fecha	Descripción	Finalidad
22	**RD-Ley 14/2019**	de 31 de octubre	Por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones	Regula un marco normativo que comprende medidas urgentes relativas a la documentación nacional de identidad; a la identificación electrónica ante las Administraciones públicas; a los datos que obran en poder de las mismas; a la contratación pública; y al sector de las telecomunicaciones.

3.3 Organización de la seguridad

La organización de la seguridad se basa en el ***«Acuerdo por el que se aprueba la estructura organizativa y asignación de roles de seguridad para la administración electrónica del Gobierno Vasco»***, del Consejo de Gobierno de 30 de junio de 2015 y en el ***"Acuerdo por el que se aprueba la estructura organizativa y asignación de roles para la protección de los datos personales tratados por la administración pública de la Comunidad Autónoma de Euskadi"*** de 19 de junio de 2018.

El **ámbito de aplicación** afecta a la Administración Pública de la Comunidad Autónoma de Euskadi, y a la entidad responsable de explotación de las infraestructuras TIC sobre las que se sustenta la Administración Electrónica. Estos actores deben articular los **roles de seguridad y privacidad** que se describen a continuación, y participar en los comités de seguridad y privacidad establecidos.

Esta Política de seguridad y privacidad de la información hace referencia y es coherente con los documentos de seguridad de protección de datos de carácter personal que existen en el ámbito de la Administración Pública de la Comunidad Autónoma de Euskadi. Esto es, la articulación de los roles y responsabilidades definidos debe ser compatible y estar integrada, en la medida de lo posible, con el Reglamento (UE) 2016/679, así como con la Ley 3/2018, de 5 de diciembre.

Se denomina **GureSeK** (Gure Segurtasun Kudeaketa) al proceso de gestión de la seguridad y privacidad de la información encargado de gestionar la seguridad y privacidad de los servicios electrónicos prestados a la ciudadanía por la Administración Pública de la Comunidad Autónoma de Euskadi.

Se establecen una serie de obligaciones a cumplir por todo el personal, tanto perteneciente como subcontratado por la Administración Pública de la Comunidad Autónoma de Euskadi, a la hora de participar en la prestación de dichos servicios electrónicos, bien de forma directa o bien de manera indirecta, , tal y como se indica en el apartado «*3.8 - Obligaciones generales de las personas usuarias*».

Así mismo, se establecen unas directrices a cumplir desde el punto de vista de la seguridad y privacidad de la información a la hora de llevar a cabo la adquisición de productos o la contratación de servicios relacionados con la prestación de servicios electrónicos por parte de la Administración Pública de la Comunidad Autónoma de Euskadi.

3.4 Roles de seguridad y privacidad

Los roles funcionales son los siguientes:

#	Rol	Titular	Funciones
1	Responsables de la Información	Persona titular de la Dirección de Servicios del Departamento respectivo o del órgano unipersonal de gobierno correspondiente a cada Organismo Autónomo	Tienen potestad para establecer los requisitos de seguridad y privacidad de la información necesarios para proteger apropiadamente la información de las aplicaciones utilizadas en su Departamento u Organismo Autónomo, y concretar los intereses a salvaguardar, así como las necesidades a cubrir. Son responsables tanto del uso que se haga de la información que manejan las aplicaciones del respectivo Departamento u Organismo Autónomo como de su protección, por lo que responden de cualquier error o negligencia en el uso de dichas aplicaciones que afecte a la seguridad de la información. Participan en el Comité de Seguridad Corporativa y designan a la persona de su Dirección u Organismo Autónomo que forma parte del Comité Técnico de Seguridad.
2	Responsables de los Servicios Comunes	Persona titular de la Dirección que ostenta la competencia del Servicio Común respectivo: • Administración Electrónica • Función Pública y gestión de personal • Oficina de Control Económico y Finanzas • Planificación Territorial y Urbanismo • Sistema de Archivo y Documentación • Seguridad de las Instalaciones	Tienen potestad para establecer los requisitos de seguridad necesarios para proteger apropiadamente los servicios prestados por estas aplicaciones y plataformas tecnológicas, determinando los intereses y necesidades aplicables. Son responsables tanto del uso que se haga del servicio común como de su protección, por lo que responden de cualquier error o negligencia en el uso de dichos servicios que provoque un incidente de seguridad. Participan en el Comité de Seguridad Corporativa y designan a la persona de su Dirección que forma parte del Comité Técnico de Seguridad.

#	Rol	Titular	Funciones
3	Responsable de la Seguridad	Persona titular de la Dirección competente en Informática y Telecomunicaciones	Tiene potestad para establecer los requisitos de seguridad de los sistemas de información que soportan la Administración Electrónica, determinando apropiadamente las medidas de seguridad a aplicar. Tiene la responsabilidad de promover la formación y concienciación en materia de seguridad de la información en todos los Departamentos y Organismos Autónomos del Gobierno Vasco. En este sentido, la articulación del programa de formación en materia de seguridad de la información en los Departamentos y Organismos Autónomos del Gobierno Vasco se llevará a cabo a través del Instituto Vasco de Administración Pública (IVAP), y formará parte del programa de formación transversal de dicho Organismo Autónomo. Es responsable de la protección de los sistemas de información que soportan la Administración Electrónica, por lo que responde de cualquier error o negligencia que provoque un incidente de seguridad o afecte a la misma. La aplicación de las medidas de seguridad técnicas se llevará a cabo a través de su «encargo general» a la sociedad pública Eusko Jaurlaritzaren Informatika Elkartea / Sociedad Informática del Gobierno Vasco [en adelante, EJIE] Participa en el Comité de Seguridad Corporativa y designa a la persona de su Dirección que forma parte del Comité Técnico de Seguridad.

#	Rol	Titular	Funciones
4	Responsable de los Sistemas	Persona titular de la Dirección competente en Informática y Telecomunicaciones	Tiene potestad para establecer los requisitos de seguridad de los sistemas informáticos que sustentan la Administración Electrónica y de las plataformas tecnológicas que les dan soporte, determinando apropiadamente las medidas de seguridad a aplicar. Es responsable de desarrollar y mantener dichos sistemas, por lo que responde de cualquier error o negligencia que provoque un fallo en ellos. En virtud de las responsabilidades anteriores, tendrá la potestad de definir la topología de red y la sistemática de gestión de dichos sistemas de información, y de determinar los criterios de uso y establecer los servicios disponibles. La finalidad es que los sistemas de información cumplan con los requisitos establecidos para los servicios prestados a través de ellos y con las medidas de seguridad aplicables, determinando apropiadamente las características técnicas de los mismos.

#	Rol	Titular	Funciones
5	Responsable de Explotación de los Sistemas	Director/a General de la sociedad pública Eusko Jaurlaritzaren Informatika Elkartea / Sociedad Informática del Gobierno Vasco (EJIE) sociedad que se responsabilizará, por encargo de la Dirección competente en Informática y Telecomunicaciones, del despliegue y mantenimiento de los sistemas informáticos que integran la Red Corporativa Administrativa del Gobierno Vasco (RCAGV), así como de su seguridad.	En consonancia con sus Estatutos, EJIE tendrá la responsabilidad última de instalar, poner en producción y mantener los sistemas informáticos que soportan la Administración Electrónica y su seguridad, siendo la responsable última de cualquier fallo en su funcionamiento. En virtud de las responsabilidades anteriores, la Dirección competente en Informática y Telecomunicaciones tendrá la potestad de definir la arquitectura, las características tecnológicas y el modelo de gestión a aplicar por EJIE en torno a dichos sistemas informáticos y a su seguridad, con el fin de que cumplan con los requisitos funcionales y de seguridad establecidos desde los diferentes Departamentos y Organismos Autónomos del Gobierno Vasco con responsabilidades sobre ellos. EJIE deberá participar en el Comité de Seguridad Corporativa a través de su Director/a General, y en el Comité Técnico de Seguridad a través de su Responsable de Seguridad. EJIE deberá aplicar las medidas de seguridad técnicas definidas por la Dirección competente en Informática y Telecomunicaciones en concordancia con su capacidad económica, de acuerdo a lo que se establezca en el Comité de Seguridad Corporativa. EJIE deberá proponer al Comité de Seguridad Corporativa una valoración previa de los servicios de Administración Electrónica compatible con su capacidad económica, con el fin de que dicho Comité pueda establecer las modificaciones que considere oportunas.

3.5 *Estructura de los Órganos de coordinación de la seguridad y privacidad*

Para la coordinación de la seguridad se crean los organismos colegiados siguientes:

#	Organismo	Titulares	Funciones
1	Comité de Seguridad y Privacidad Corporativa	1. Persona Responsable de la Seguridad y de los Sistemas, que lo presidirá 2. Personas Responsables de los Servicios comunes 3. Personas Responsables de la Información y medidas de privacidad 4. Persona Responsable de la Explotación de los Sistemas 5. Delegada o Delegado de Protección de Datos	Dirigir y coordinar los intereses de todas las personas afectadas por la Administración Electrónica en materia de seguridad y privacidad: 1) Resolver los conflictos que puedan aparecer en torno a la seguridad entre los diferentes afectados por la Administración Electrónica (Departamentos, Organismos Autónomos y EJIE) 2) Revisar, corregir y aprobar los niveles de seguridad aplicables en función de los requisitos establecidos, las medidas de seguridad asociadas y su coste 3) Crear en cada momento los órganos de trabajo más apropiados para impulsar el desarrollo de la seguridad en la Administración Electrónica Se reunirá, como mínimo, una vez al año, así como en todas aquellas ocasiones en que su Presidente lo considere necesario.

#	Organismo	Titulares	Funciones
2	Comité de Protección de Datos	1. Delegada o Delegado de Protección de Datos 2. Las personas que ejerzan de Referentes de protección de datos de los distintos Departamentos, Organismos Autónomos o Entes Públicos de Derecho Privado	1) Coordinarse con el Delegado o Delegada de protección de datos en las políticas de protección de datos y su aplicación. 2) Comunicar las instrucciones del Delegado o Delegada de protección de datos para que las personas referentes puedan realizar sus actividades de manera coordinada eficaz y eficiente. 3) Exponer, ante las demás personas integrantes del Comité de protección de datos, cuestiones planteadas por las personas Responsables del tratamiento de cada Departamento, Organismo Autónomo o Ente Público de Derecho Privado, a los efectos de unificar doctrina, cuando sea solicitado por el Delegado o Delegada de protección de datos. 4) Analizar las informaciones relevantes que se hayan producido en materia de protección de datos. 5) Examinar los últimos avances y/o interpretaciones efectuadas por las instituciones de control y otras administraciones públicas en relación con la protección de datos personales

#	Organismo	Titulares	Funciones
3	Comité Técnico de Seguridad	1. Persona perteneciente a la Dirección competente en materia de Informática y Telecomunicaciones 2. Persona perteneciente a la Dirección competente en Administración Electrónica 3. Persona perteneciente a la Dirección competente en Gestión Documental 4. Persona perteneciente a la Dirección competente en Seguridad Patrimonial 5. Todas las personas responsables del área informática y/o Responsables de Seguridad de los Departamentos y Organismos Autónomos del Gobierno Vasco 6. Persona Responsable de Seguridad de EJIE	Coordinar la seguridad de la Administración Electrónica entre los diferentes órganos implicados: 1) Atender las necesidades de EJIE y los Departamentos y Organismos Autónomos del Gobierno Vasco en materia de seguridad en la Administración Electrónica. 2) Informar regularmente del estado de la seguridad al Comité de Seguridad Corporativa. 3) Promover la mejora continua del proceso de gestión de la seguridad del Gobierno Vasco. 4) Elaborar la estrategia de evolución de la seguridad en el Gobierno Vasco. 5) Coordinar los esfuerzos de todas las personas participantes e implicadas en la Administración Electrónica en materia de seguridad de la información, asegurando que los esfuerzos son consistentes, están unificados y están alineados con la estrategia definida. 6) Revisar periódicamente y promover la actualización de la Política de Seguridad y las Normativas de Seguridad definidas por la Administración Pública Vasca. 7) Definir de manera preliminar los requisitos de formación y cualificación de las personas administradoras, operadoras y usuarias de la Administración Electrónica desde el punto de vista de la seguridad. 8) Dirigir el análisis y gestión de riesgos de seguridad de la Administración Electrónica. 9) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones con respecto a ellos. 10) Promover la realización del programa de auditorías de seguridad del Gobierno Vasco. 11) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados. 12) Aplicar, a través de sus entidades miembro, las medidas de seguridad de carácter no técnico que se definan. 13) Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en producción y operación. 14) Tratar los conflictos que en materia de seguridad puedan aparecer entre diferentes responsables y/o entre diferentes Departamentos u Organismos Autónomos, elevando al Comité de Seguridad Corporativa aquellos casos en los que no tenga suficiente autoridad para decidir. Estará presidido por la persona Responsable de la Seguridad o por una persona integrante de su Dirección que aquella designe, y se reunirá dos veces al año.

3.6 Gestión de riesgos

La gestión de riesgos es parte esencial del proceso de seguridad y debe realizarse de manera continua sobre los sistemas de información, con el objetivo de mantener los entornos controlados y de minimizar los riesgos hasta niveles aceptables. Será preceptiva para los sistemas de información incluidos dentro del marco establecido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración electrónica, y puede ser opcional para el resto de supuestos.

Las personas Responsables de la Información y de los Servicios responden de los riesgos sobre la información y los servicios, respectivamente, y asegurarán su seguimiento y control, sin perjuicio de la posibilidad de delegar estas tareas. Para ello, podrán contar en el proceso con la participación y asesoramiento de quienes sean Responsable de la Seguridad y Responsable de los Sistemas.

Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y, en especial, las Guías elaboradas por el Centro Criptológico Nacional (CCN). Esta evaluación de los riesgos se repetirá regularmente para los sistemas de información teniendo en cuenta las recomendaciones formuladas por dicho Centro.

Existe un compromiso por parte del Gobierno Vasco, y una obligación por parte de las personas Responsables de la Información, de realizar análisis de riesgos y atender a sus conclusiones. Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos los activos. Dicho análisis se repetirá:

- Regularmente, al menos una vez cada dos años
- Cuando cambie sustancialmente la información manejada o los servicios prestados
- Cuando ocurra un incidente grave de seguridad o se descubran y reporten vulnerabilidades graves

3.7 Proceso de revisión de la política de seguridad y privacidad

Se debe revisar y promover la actualización de la Política de seguridad y privacidad de la información y de la normativa de seguridad y privacidad definidas por el Gobierno Vasco.

El Comité de Seguridad y Privacidad Corporativa revisará la Política de seguridad y privacidad 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.

3.8 *Obligaciones generales de las personas usuarias*

Todo el personal con acceso a los sistemas de información tiene el deber de conocer y cumplir la Política de seguridad y privacidad de la información y la normativa de seguridad y privacidad derivada que se establezca. A tal efecto, la Política de seguridad y privacidad de la información será comunicada a todas las personas usuarias de los sistemas de información incluidos en el ámbito de la Administración Electrónica, de manera pertinente, accesible y comprensible. Su incumplimiento podrá ser sancionado de conformidad con la normativa disciplinaria correspondiente.

Asimismo, el personal perteneciente a empresas externas subcontratadas que tengan acceso a la documentación o información asociada a alguno de los servicios del Gobierno Vasco tiene la obligación de conocer y cumplir esta Política de seguridad y privacidad de la información.

Todo personal que emplee sistemas de tecnologías de la información y las comunicaciones recibirá formación para el manejo seguro de dichos sistemas. Se deberán establecer los procedimientos de control que garanticen el cumplimiento efectivo de esta Política, que serán efectuados por los Departamentos y los Organismos Autónomos.

3.9 *Concienciación y formación*

Corresponde al Comité de Seguridad y Privacidad Corporativa promover la formación y concienciación en materia de seguridad y privacidad de la información en el ámbito de la Administración Pública de la Comunidad Autónoma de Euskadi.

Se desarrollarán actividades específicas orientadas a la formación y concienciación de todo el personal en materia de seguridad y privacidad de la información, así como a la difusión de la Política de seguridad y privacidad de la información y de su desarrollo normativo, y estarán dirigidas en particular al personal de nueva incorporación. A estos efectos, los planes de formación incluirán actividades específicas sobre seguridad y privacidad de la información.

La articulación del programa de formación en materia de seguridad y privacidad de la información en la Administración Pública de la CAE se llevará a cabo a través del Instituto Vasco de Administración Pública (IVAP), y formará parte del programa de formación transversal de dicho Organismo Autónomo. Será esta formación, también, función de la Delegada o Delegado de Protección de Datos.

3.10 *Terceras partes*

Cuando la Administración Pública de la CAE utilice servicios o maneje información de terceras partes, les hará partícipes de esta Política de seguridad y privacidad de la información. El Comité Técnico de Seguridad y Privacidad establecerá canales para reporte y coordinación, y establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Gobierno Vasco preste servicios a otros organismos, les hará partícipe de esta Política de seguridad y privacidad de la información y de las Instrucciones y Procedimientos que atañan a dichos servicios o información.

Cuando el Gobierno Vasco ceda información a terceras partes o encargue la prestación de servicios a otros organismos, les hará partícipe de esta Política de seguridad y privacidad de la información y de las Instrucciones y Procedimientos que atañan a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la normativa mencionada, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Asimismo, se exigirá que el personal de terceras partes esté adecuadamente concienciado en materia de seguridad y privacidad, al menos al mismo nivel que el establecido en esta Política.

4. Anexo: glosario de términos y abreviaturas

A continuación, se define una serie de términos que han sido empleados a lo largo de todo el documento y que facilitan el entendimiento del mismo.

#	Término	Definición
1	Activo	Componente, funcionalidad o recurso que tenga valor para la organización: información, datos, servicios, aplicaciones, equipos, comunicaciones, recursos administrativos, físicos y humanos…
2	Amenaza	Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización [UNE 71504:2008]. Las amenazas siempre están presentes, pero se puede intentar evitarlas o paliar los efectos de su materialización.
3	Análisis de Riesgos	Proceso para el análisis de las amenazas, vulnerabilidades, riesgos e impactos a los que está expuesto un sistema de información, teniendo en cuenta las medidas de seguridad ya presentes. Sirve como punto de partida para identificar las mejoras en las medidas de seguridad, tanto en lo que se refiere a su efectividad como a sus costes.
4	Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos [ENS].
5	Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados [ENS].
6	Cuerpo normativo	Conjunto de normas que desarrollan de forma más concreta la manera de alcanzar los objetivos de una política.
7	Dato de carácter personal	Cualquier información concerniente a personas físicas identificadas o identificables [LOPD].
8	Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a estos cuando lo requieren [ENS].
9	ENS	Esquema Nacional de Seguridad (RD 3/2010).
10	Gestión de la continuidad	Actividades que lleva a cabo una organización para asegurar que todos los procesos de negocio críticos estarán disponibles para sus personas usuarias, clientes, proveedores y otras entidades que deban utilizarlos.

#	Término	Definición
11	Gestión de incidentes o incidencias	Procesos orientados a recuperar el nivel habitual de funcionamiento del servicio y a minimizar en todo lo posible el impacto negativo de un fallo de seguridad en la organización, de forma que la calidad del servicio y la disponibilidad se mantengan.
12	Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respeto a los riesgos [ENS].
13	Incidente de seguridad	Suceso inesperado o no deseado con consecuencias negativas para la seguridad del sistema de información [ENS].
14	Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada [ENS].
15	LOPD	Ley Orgánica de Protección de Datos de Carácter Personal (LO 15/1999).
16	Medidas de seguridad	Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, disuasión, protección, detección y reacción, o bien de recuperación [ENS].
17	MSPLATEA	Manual de Seguridad de PLATEA.
18	PLATEA	Plataforma para la Administración Electrónica del Gobierno Vasco.
19	Política de seguridad y privacidad	Documento de alto nivel que especifica los objetivos en materia de seguridad y privacidad de una organización y refleja el compromiso de la dirección para alcanzarlos.
20	Proceso	Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y un fin delimitados, implica recursos y da lugar a un resultado [ENS].
21	RDLOPD	Reglamento de Desarrollo de la LOPD (RD 1720/2007).
22	Riesgo	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, con daños o perjuicios a la organización [ENS].
23	Riesgo residual	Riesgo remanente en el sistema tras la implantación de unas determinadas salvaguardas en el plan de tratamiento de riesgos.
24	Seguridad de la información	Protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas.

#	Término	Definición
25	Sistema de información	Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir [ENS].
26	Soporte	Medio físico de cualquier tipo (papel, USB, DVD, discos portátiles, etc.) utilizado para almacenar información.
27	Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad [ENS].
28	Vulnerabilidad	Una debilidad en un activo que puede ser aprovechada por una amenaza [ENS].