ORDEN DE 23 DE ENERO DE 2019, DE LA CONSEJERA DE SEGURIDAD, POR LA QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁMBITO DE LAS REDES Y SERVICIOS DE INFORMACIÓN GESTIONADOS POR EL DEPARTAMENTO DE SEGURIDAD.

El Departamento de Seguridad es responsable de la planificación y mantenimiento de redes de comunicación y sistemas de la información en el ámbito de la seguridad pública, de conformidad con los arts. 14 y 17 de la Ley 15/2012, de 28 de junio, de Ordenación del Sistema de Seguridad Pública de Euskadi; el Decreto 24/2016, de 26 de noviembre, del Lehendakari, de creación, supresión y modificación de los Departamentos de la Administración de la Comunidad Autónoma del País Vasco y de determinación de funciones y áreas de actuación de los mismos y el propio Decreto 83/2017, de 11 de abril, por el que se establece la estructura orgánica y funcional del Departamento de Seguridad.

Tales redes de comunicación y sistemas de la información resultan críticos para la salvaguarda de la seguridad pública, de forma que debe asegurarse su protección y la continuidad de su prestación, tanto en lo que atañe al funcionamiento de las agencias implicadas e interconexionadas para la prestación de sus servicios, como en lo que atañe propiamente a las relaciones con la ciudadanía en el ámbito propio de la administración electrónica.

La protección de la seguridad de la información ha sido regulada desde diferentes normas en los últimos años. Por un lado existe el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por Real Decreto 951/2015, de 23 de octubre; y por otro, la novedosa normativa de protección de datos, constituida por el Reglamento General de Protección de datos y su transposición por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Pero, además, hay que tener en cuenta el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, además, del impacto de la normativa sobre protección de infraestructuras críticas en los casos que fuera aplicable.

Todas estas normas, atendiendo a diferentes bienes jurídicos a proteger, confluyen en imponer medidas de seguridad a las redes y sistemas de información que deben entenderse como complementarias, tal y como estipula la disposición adicional primera de la citada Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El Gobierno Vasco ha adoptado un Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco tomando por referente el esquema nacional de seguridad y atendiendo a lo dispuesto en el Decreto 21/2012, de 21 de febrero de Administración Electrónica y a la Orden 26 de febrero aprobando el Manual

de Seguridad para el mantenimiento de la seguridad de la información de la Administración General de la Comunidad Autónoma y sus Organismos Autónomos, así como 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. Debe atenderse igualmente al Acuerdo del Consejo de Gobierno de 19 de junio de 2018, 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.

El ámbito propio de dicha política de seguridad de la información, al igual que el esquema nacional de seguridad que toma por referencia, no abarca a todas las redes y sistemas de información que son el basamento del funcionamiento de la Administración de Seguridad, sino exclusivamente a los servicios propios de la Administración electrónica.

Sin embargo gran parte de la actividad de la Administración de Seguridad se manifiesta en actos materiales no procedimentalizados que cuentan como soporte el empleo de soluciones tecnológicas que precisan, dada su criticidad, de medidas de seguridad que exceden de los estándares comunes a cualquier otra rama de la Administración.

Por otra parte, los tratamientos de datos por las autoridades de seguridad pública para la prevención, investigación, detección o enjuiciamiento de ilícitos penales, se excluyen de la normativa común de protección de datos y se sujetan a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, aún pendiente de transposición.

Tales singularidades no impiden que las medidas que en tal ámbito se adopten no sean coherentes y tomen por referencia a las configuradas para el conjunto de la Administración. Si bien con salvaguarda de las especificidades existentes y de las acciones para salvaguardar la seguridad pública, incluidas las dirigidas a proteger la información clasificada o cuya revelación fuere contraria al interés general, o las que tengan como propósito el mantenimiento del orden público, la detección, investigación y persecución de los delitos, y el enjuiciamiento de sus autores.

Por tal razón, se considera conveniente aprobar dentro del Departamento de Seguridad su propia política de seguridad de las redes y sistemas de la información de gestión propia. Tal política de seguridad está alineada con la política de seguridad de la información establecida para el conjunto de la Administración General del Gobierno Vasco y sus organismos autónomos en lo que atañe a al ámbito de las relaciones electrónicas con la ciudadanía, pero con salvaguarda de las especificidades del ámbito de la seguridad pública en el resto de redes y sistemas de la información.

Por todo lo cual,

RESUELVO:

Primero.- Aprobar la Política de Seguridad de la Información (en adelante, PSI) en el Departamento de Seguridad del Gobierno Vasco, que figura como anexo.

Segundo.- La presente orden se publicará en la sede electrónica del Gobierno Vasco y en la página web del departamento de seguridad, así como en las intranets departamentales existentes.

En Vitoria- Gasteiz, (firmado digitalmente).

ESTEFANIA BELTRÁN DE HEREDIA ARRONIZ
CONSEJERA DE SEGURIDAD

ANEXO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEPARTAMENTO DE SEGURIDAD DEL GOBIERNO VASCO

1. Objeto y ámbito de aplicación.

1.1. Es objeto del presente documento la definición de la Política de Seguridad de la Información (en adelante, PSI) en el Departamento de Seguridad del Gobierno Vasco y su organismo autónomo, así como el establecimiento del marco organizativo y tecnológico de la misma.

1.2. La presente PSI será de aplicación a las redes y sistemas de información del Departamento de Seguridad y será de obligado cumplimiento para todos los órganos y unidades del Departamento y su organismo autónomo, así como para todo el personal con acceso a los sistemas de información de este Departamento, con independencia de cuál sea su destino, adscripción o relación con el mismo.

1.3. En lo que atañe al ámbito de la administración electrónica definido por lo dispuesto en el Decreto 21/2012, de 21 de febrero de Administración Electrónica, se atenderá a lo dispuesto por el Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco.

1.4.- En lo que atañe al resto de redes y sistemas de la información gestionados por el Departamento de Seguridad, se atenderá a lo definido en el presente documento y sus desarrollos e implementaciones.

No obstante, se tendrán como referentes las directrices y medidas de seguridad contempladas por el Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco para la administración electrónica, sin perjuicio de las medidas precisas para salvaguardar la seguridad pública, incluyéndose las dirigidas a proteger la información clasificada o cuya revelación fuere contraria a los intereses esenciales, o las que tengan como propósito el mantenimiento del orden público, la detección, investigación y persecución de los delitos, y el enjuiciamiento de sus autores.

2. Principios de seguridad.

La presente PSI se desarrollará, con carácter general, de acuerdo con los siguientes principios:

a) 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.

Los requerimientos de la seguridad de la información se atenderán durante todo el ciclo de vida de los activos, desde su planificación hasta su retirada.

b) Gestión del riesgo:

Gestionar la seguridad 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.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

c) 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.

d) 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.

e) Confidencialidad:

Se deberá garantizar que los activos sean accesibles únicamente para aquellas personas expresamente autorizadas para ello.

f) Autenticidad:

Se deberá garantizar que la información proceda y se intercambie con los interlocutores idóneos y que los servicios se acrediten correctamente.

g) Trazabilidad:

Se deberá garantizar el seguimiento de las operaciones efectuadas sobre la información y los servicios que lo requieran.

h) Prevención, reacción y recuperación:

La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan. Se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad.

Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de 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 inhabilite los medios habituales.

i) Líneas de defensa y 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 ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse; reducir la probabilidad de que el sistema sea comprometido en su conjunto, y minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

j) Mejora continua y reevaluación periódica:

Se revisará de manera recurrente el grado de eficacia de los controles de seguridad 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.

k) 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.

l) Concienciación y formación:

Se articularán programas de formación, sensibilización y concienciación para las personas usuarias en materia de seguridad de la información, debidamente apoyados en las políticas corporativas y con un acomodado proceso de seguimiento y actualización.

m) Función diferenciada:

En los sistemas de información se diferenciará la responsabilidad de la seguridad de los sistemas de información de la responsabilidad sobre la prestación de los servicios, de conformidad con lo establecido en la atribución de roles contenida en la presente Orden, que delimita las atribuciones de cada responsable, así como los mecanismos de coordinación y resolución de conflictos.

El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

n) 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 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.- Estructura organizativa.

La presente PSI se instrumenta por medio de la siguiente estructura organizativa:

a) Responsable de la información.
b) Responsable del servicio.
c) Responsable de la seguridad.
d) Responsable del sistema.
e) Comité superior para la seguridad y privacidad de la información.
e) Comité técnico para la seguridad y privacidad de la información.

4.- Responsable de la información.

4.1. El responsable de la información es la persona u órgano corporativo que tiene la potestad de establecer los requisitos de la información en materia de seguridad o de determinar los niveles de seguridad de la información atendiendo a las directrices fijadas por el Comité para la seguridad de la información o, en su caso, el Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco.

4.2. De conformidad con el Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco en su ámbito son responsables de la información la persona titular de la Dirección de Servicios y el órgano unipersonal de gobierno correspondiente a cada Organismo Autónomo.

4.3. En el resto de redes y sistemas de la información departamentales vinculados a la seguridad pública es responsable de la información la persona titular de la Viceconsejería de Seguridad o persona o personas en quienes delegue, a las que corresponde:

a) Determinar los niveles de seguridad de la información tratada, previo informe del responsable de seguridad, valorando los impactos de los incidentes que afecten a la seguridad de la información.

b) Realizar, junto a los responsables de los servicios y con la participación del Responsable de la Seguridad, los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

c) Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.

d) Para la determinación de los niveles de seguridad de la información, el Responsable de la Información solicitará informe del Responsable de la Seguridad.

e) El responsable de la información será el responsable de las medidas de privacidad de conformidad con la normativa aplicable de protección de datos, a salvo que se establezca otra cosa en los documentos de desarrollo de esta PSI.

5.- Responsable del Servicio.

5.1. El responsable del Servicio es la persona u órgano corporativo que tiene la potestad de establecer los requisitos de los servicios prestados. Es el encargado de determinar los niveles de seguridad del servicio en cada dimensión de seguridad.

5.2. Los responsables del servicio son las personas titulares de los órganos del Departamento de Seguridad y de su organismo autónomo en relación a los servicios que tengan encomendados.

5.3.- Corresponde a los responsables de cada servicio:

a) Determinar los niveles de seguridad del servicio, valorando los impactos de los incidentes que afecten a la seguridad del servicio.

b) Realizar, junto al responsable de la información y contando con la participación del responsable de la seguridad, los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

c) Aceptar los riesgos residuales respecto de los servicios calculados en el análisis de riesgos.

d) Para la determinación de los niveles de seguridad del servicio, el responsable del servicio solicitará informe del responsable de la seguridad.

e) El responsable del servicio será el responsable de los tratamientos de datos que se realicen de conformidad con la normativa aplicable de protección de datos, a salvo que se establezca otra cosa en los documentos de desarrollo de esta PSI.

6.- Responsable de la Seguridad.

6.1. El responsable de la seguridad tiene la responsabilidad de establecer los estándares y requisitos de seguridad de las redes y sistemas de la información

que dan soporte a la actividad de la Administración de la Seguridad pública de Euskadi, determinando apropiadamente las medidas de seguridad a aplicar.

6.2. Dentro del Departamento de Seguridad asume el rol de responsable de la seguridad la persona titular de la Dirección de Gestión de Telecomunicaciones y Sistemas de Información, o persona en quien delegue, sin perjuicio de las atribuciones que correspondan a otros en el ámbito propio del Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco.

6.3. Serán funciones del Responsable de la Seguridad, dentro de su ámbito de actuación, las siguientes:

a) Desarrollar las directrices, estrategias y objetivos dictados por el Comité de Seguridad de la información y proveerle de asesoramiento y apoyo.

b) Elaborar la normativa de seguridad.

c) Aprobar los procedimientos operativos de seguridad.

d) Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información.

e) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

f) Realizar el seguimiento y control del estado de seguridad del sistema de información.

g) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

h) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

i) Elaborar informes periódicos de seguridad para el Comité de Seguridad de la información que incluyan los incidentes más relevantes de cada período.

j) Supervisar el registro de activos.

7.- Responsable de los sistemas.

7.1. El responsable de los sistemas es responsable de:

a) Definir la topología y sistema de gestión de dichos sistemas de información con las medidas de seguridad aplicables, estableciendo los criterios de uso y los servicios disponibles en el mismo.

b) Determinar apropiadamente sus características técnicas y los criterios de uso y establecer los servicios disponibles.

c) Desplegar y mantener los sistemas informáticos gestionados por el Departamento, sin perjuicio de los servicios convergentes comunes a todo el Gobierno Vasco.

d) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

e) Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

7.2. Dentro del Departamento de Seguridad asume el rol de responsable de los sistemas la persona titular de la Dirección de Gestión de Telecomunicaciones y Sistemas de Información, o persona en quien delegue, sin perjuicio de las atribuciones que correspondan a otros en el ámbito propio del Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco.

8.- Comité superior para la seguridad y privacidad de la información (CSSPI):

8.1. El Comité superior para la seguridad y privacidad de la información (CSSPI) tiene como misión construir la estructura de políticas, iniciativas y objetivos en materia de seguridad de un modo coordinado para racionalizar el gasto y disfunciones que permitan fallas de seguridad al ofrecer el Sistema puntos débiles donde pudieran ocurrir incidentes o se pudieran perpetrar ataques.

8.2. Sus funciones son las siguientes:

a) Aprobar las propuestas de modificación y actualización permanente de la PSI y velar por su cumplimiento.

b) Identificar requisitos, servicios y objetivos de seguridad, asignando recursos y priorizando las actuaciones.

d) Promover la mejora continua en la gestión de la seguridad de la información.

e) Impulsar la formación y concienciación.

f) Revisar el sistema de gestión de la seguridad de la información recabando informes regulares del estado del mismo.

g) Coordinar el contacto con los órganos del Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco para la administración electrónica y otras entidades para la elaboración de un perfil general del estado de seguridad de las redes y sistema de la información.

h) Impulsar el cumplimiento de la normativa de protección de datos, especialmente en la identificación y diseño de tratamientos, la asignación de niveles de criticidad; la implantación de medidas de seguridad o la realización de auditorías. En el ámbito propio del Centro de Elaboración de datos de carácter policial de Euskadi contará para ello con su cooperación.

f) Resolver los conflictos que puedan aparecer entre los diferentes responsables o áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

g) Articular la creación de grupos de trabajo para la realización de estudios, trabajos e informes que se consideren convenientes

8.3**.** El Comité para la seguridad y privacidad de la información está compuesto por las siguientes personas:

a) Presidencia: Titular de la Viceconsejería de Seguridad.

b) Vicepresidencia: Titular de la Viceconsejería de Administración y Servicios, que asumirá la presidencia en caso de ausencia de la titular de la presidencia.

c) Titulares de los siguientes órganos directivos:

- Dirección de Gestión de telecomunicaciones y sistemas de información, como responsable de sistemas, de seguridad y de la explotación.
- Dirección de Gestión Económica y Recursos Generales, como responsable de servicios comunes de gestión y mantenimiento de edificios, instalaciones e infraestructuras del Departamento de Seguridad.
- Dirección de Coordinación de Seguridad, como responsable en materia de sistemas de archivos policiales y del Centro de Elaboración de datos de carácter policial de Euskadi.
- Dirección de Régimen Jurídico, Servicios y Procesos Electorales, como responsable de la información dentro del ámbito del Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco.
- Dirección de la Ertzaintza.
- Academia Vasca de Policía y Emergencias.

d) La persona referente de protección de datos departamental y la persona que, caso de crearse la figura, asumiera las funciones de delegado o delegada de protección de datos del sistema de información policial.

e) Una persona con responsabilidad en seguridad en sistemas de la información de la Dirección de Gestión de Telecomunicaciones y Sistemas de

Información, que actuará como secretaria del Comité Sistemas de Información, que actuará con voz y voto, y será la garante de la ejecución directa o delegada de las decisiones del Comité superior para la seguridad de la información. Se encarga de preparar los temas a tratar en las reuniones, realizar la convocatoria y elaborar el acta de las mismas.

8.4. El CSSPI se reunirá con carácter ordinario, al menos, semestralmente a instancias de la Presidencia. Por razones de urgencia podrá reunirse siempre que la Presidencia lo estime conveniente.

8.5. En las reuniones del CSSPI podrán participar cuantos asesores, internos o externos, se estime conveniente por parte de la Presidencia del mismo.

9.- Comité para la seguridad y privacidad del sistema de información policial (CSPIP).

9.1. En el ámbito propio del sistema de información policial (SIP) se crea el Comité para la seguridad y privacidad del sistema de información policial (CSPIP), dependiente del Comité superior para la seguridad y privacidad de la información.

9.2. El CSPIP asume la función de impulsar, proponer los desarrollos normativos de la política de seguridad de la información en el ámbito propio del sistema de información policial, así como desarrollar y ejecutar la política de seguridad de la información acordada por el Comité Superior en dicho ámbito. A tal efecto:

a) Propone los desarrollos normativos y la revisión y actualización de la PSI en el ámbito del sistema de información policial.

b) Adecúa los requisitos, servicios y objetivos de seguridad, asignando recursos y priorizando las actuaciones, e impulsa la implantación de medidas de seguridad en el sistema de información policial y, en particular, en el Centro de Elaboración de datos de carácter policial de Euskadi.

c) Vela por el cumplimiento de la política de seguridad de la información y revisa su funcionamiento por medio de informes regulares y auditorías.

9.3. En el cumplimiento de su misión tiene en consideración las singularidades derivadas de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y las normas que la traspongan, así como, cuando se trate de sistemas de información policial de la Unión Europea las medidas de seguridad específicas que se contemplen en las normas reguladoras de los mismos.

9.4.- El CSPIP cuenta con la siguiente composición:

a) Presidencia: Titular de la Dirección de Coordinación de Seguridad.
b) Vicepresidencia: Dirección de Gestión de telecomunicaciones y sistemas de información.
c) Vocales:

- Una persona responsable del Centro de Operaciones de Seguridad del sistema de información policial.
- Una persona designada al efecto por la Dirección de la Ertzaintza en función de las responsabilidades en el Centro de Elaboración de datos de carácter policial.
- La persona referente de protección de datos departamental
- La persona que asuma las funciones de delegado o delegada de protección de datos del sistema de información policial.
- Una persona con responsabilidad en seguridad en sistemas de la información de la Dirección de Gestión de Telecomunicaciones y Sistemas de Información, que actuará como secretaria del Comité con voz y voto.

9.4. El CSPIP se reunirá semestralmente al menos con carácter ordinario y siempre que concurran razones de urgencia. Sus reuniones podrán participar cuantos asesores, internos o externos, se estime conveniente

9.5. El Centro de Operaciones de Seguridad del Sistema de Información Policial (COSSIP), dependiente de la Dirección de Gestión de telecomunicaciones y sistemas de información garantiza el nivel de disponibilidad de sus servicios de comunicaciones evitando fallos ocasionales; efectúa un análisis dinámico de riesgos e incidentes y de conocimiento de la situación; supervisa incidentes;, difunde alertas a los grupos de usuarios y da respuesta a los incidentes.

Para ello canales de comunicación con el COSSIP estarán claramente especificados y serán bien conocidos de los grupos de usuarios.

para lo cual cuenta con medios diversos para que se les contactar y puedan contactar a otros en todo momento.

Sus instalaciones y las de los sistemas de información de apoyo estarán situados en lugares seguros, disponen de sistemas redundantes y espacios de trabajo de reserva.

10.- Comité técnico para la seguridad y privacidad de la información:

10.1. Se conformará un Comité técnico para la seguridad y privacidad de la información que englobe a personal técnico de cada una de las áreas concernidas como responsables de información y de medidas de privacidad; responsables de servicios y de tratamientos y responsables de seguridad y de sistemas.

10.2. Dicho Comité técnico, elaborará el perfil general del estado de seguridad del Departamento y su organismo autónomo, integrando el estado de las principales variables de seguridad de cada órgano, asegurará la coherencia de las políticas de seguridad sectoriales que afecten al Departamento y colaborará en la investigación y resolución de incidentes de seguridad de la información, tanto en el ámbito interno como externo al Departamento.

10.3. El personal designado para tal grupo de trabajo se responsabilizará de cooperar con el responsable de seguridad en el ejercicio que éste tiene encomendadas.

11. Gestión de los riesgos.

11.1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

11.2. Los Responsables de la Información y de los servicios son los responsables de los riesgos sobre la información y sobre los servicios, respectivamente, y por tanto, de aceptar los riesgos residuales calculados en el análisis, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

11.3. La selección de las medidas de seguridad a aplicar será propuesta por el Responsable de Seguridad al Comité de Seguridad de la información.

11.4. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse cada año por parte del Responsable de Seguridad, que elevará un informe al Comité de Seguridad de la información

12. Desarrollo normativo de la PSI. Documentación de Seguridad.

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

a) Primer nivel normativo: Política de Seguridad de la Información y directrices y normas de seguridad generales para todo el Departamento de Seguridad.

b) Segundo nivel normativo: Normas Específicas de Seguridad de la Información y Normas de Seguridad TIC. Son Las mismas desarrollan y detallan la PSI, centrándose en un área o aspecto determinado de la seguridad de la información.

c) Tercer nivel normativo: procesos, procedimientos e Instrucciones Técnicas. Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la PSI.

12.2. Además, la documentación de seguridad del sistema podrá contar con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

12.3. La documentación de seguridad debe mantenerse actualizada y organizada.

13. Protección de datos de carácter personal.

Los datos de carácter de personal que sean objeto de tratamiento deberán protegerse mediante la implantación de las medidas de seguridad correspondientes, a tenor de lo dispuesto en la normativa de protección de datos aplicable en cada caso.

14. Terceras partes.

14.1. Cuando el Departamento de Seguridad utilice servicios o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos órganos de seguridad de la información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

14.2. Cuando el Departamento de Seguridad preste servicios o ceda información a terceros, se les hará partícipes de esta Política y de la Normativa de Seguridad que ataña a dichos servicios e información. Los mismos quedarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias y se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad.

14.3. Cuando algún aspecto de la PSI no pueda ser satisfecho por una tercera parte según se establece en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe habrá de ser aprobado por los responsables de la información y los servicios afectados.

15. Formación.

15.1. Todo el personal relacionado con la información, los servicios y los sistemas de información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad de la información.

15.2. Para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del Departamento de Seguridad, se articularán los mecanismos necesarios para llevar a la práctica la concienciación y la formación específica necesaria e imprescindible en todos los niveles de la organización.

16. Acciones de Responsabilidad

16.1. El incumplimiento de las obligaciones y medidas de seguridad por parte de los empleados públicos establecidas en el presente documento para el personal afectado, se sancionará conforme a las normas relativas al régimen disciplinario del personal funcionario y laboral que presta sus servicios en las Administraciones Públicas aplicable en cada caso.

16.2. Ante el incumplimiento por parte de proveedores de servicios, o personal externo contratado, se actuará conforme a lo establecido en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, sin perjuicio de las acciones reflejadas en los pliegos de contratación, o cualquier otra acción que se determine en base a la naturaleza y gravedad del hecho.