ACUERDO

Asunto: 10 - Modificación de la Política de Seguridad de la Información del Cabildo Insular de Tenerife.

Visto el asunto de referencia y

ANTECEDENTES

RESULTANDO que las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una empresa u organización, garantizando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles.

RESULTANDO que el Cabildo Insular de Tenerife mediante Acuerdo número AC0000007924 adoptado por el Consejo de Gobierno Insular de fecha 26 de enero de 2021 aprobó su Política de Seguridad, como un documento que reflejaba las directrices que rigen la forma en la que el Cabildo debe gestionar y proteger la información y los servicios.

RESULTANDO que el Comité Técnico de Seguridad reunido el 20 de abril de 2022 en sesión ordinaria acordó, por unanimidad de los asistentes con derecho a voto, *"proponer al Comité de Dirección de Seguridad para su aprobación por el Consejo de Gobierno insular, la modificación del apartado séptimo de la Política de Seguridad, concerniente a la Organización de la Seguridad en el Cabildo, en el sentido que se propone quedando redactado de las siguiente forma:*

- El Comité de Dirección se reunirá con carácter ordinario, como mínimo, cada doce meses y extraordinariamente cuantas veces estime necesario su Presidencia

- El Comité Técnico se reunirá con carácter ordinario, como mínimo, cada doce meses y extraordinariamente cuantas veces estime necesario su Presidencia."

RESULTANDO que el Comité de Dirección de Seguridad reunido el 22 de abril de 2022, en sesión ordinaria acordó la revisión de la Política de Seguridad en los términos que se describen y su elevación al Consejo de Gobierno para su aprobación, "*la modificación del apartado séptimo de la Política de Seguridad, concerniente a la Organización de la Seguridad en el Cabildo, en el sentido que se propone quedando redactado de las siguiente forma:*

- El Comité de Dirección se reunirá con carácter ordinario, como mínimo, cada doce meses y extraordinariamente cuantas veces estime necesario su Presidencia.

- El Comité Técnico se reunirá con carácter ordinario, como mínimo, cada doce meses y extraordinariamente cuantas veces estime necesario su Presidencia."

CONSIDERANDO que la Política de Seguridad en su apartado 7.2.4 determina que el Comité de Dirección se reunirá con carácter ordinario, como mínimo, cada seis meses y extraordinariamente cuantas veces estime necesario su Presidencia y en su apartado 7.3.4 señala que el Comité Técnico se reunirá con carácter ordinario, como mínimo, cada tres meses

y extraordinariamente cuantas veces estime necesario su Presidencia.

CONSIDERANDO que conforme al apartado 7.2.5 de la Política de Seguridad, se levantará acta de las reuniones del Comité de Dirección, pudiéndose tratar en las mismas, entre otros, los siguientes temas:

- Revisión de la Política de Seguridad de la Información

Y puesto en relación con el apartado 25 de la Política de Seguridad que regula la Revisión de la Política de Seguridad de la Información, que señala que *"La revisión anual de esta PSI será misión del Comité de Dirección. La Política será aprobada por acuerdo de Consejo de Gobierno Insular del CIT.Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas"*

CONSIDERANDO que el expediente que se tramita no contempla obligaciones ni compromisos de carácter económico, no resultando preceptivo el Informe de la Intervención General. Y, en el mismo sentido, a tenor de lo previsto en el Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional, tampoco resulta preceptivo el informe de la Asesoría Jurídica.

En base a la documentación obrante en el expediente, los antecedentes y consideraciones expuestos, vistas las atribuciones que ostenta esta Consejería Insular del Área de Presidencia, Hacienda y Modernización en virtud de Decreto de la Presidencia 1825 de fecha 13 de septiembre de 2021 relativo a la modificación de la estructura y organización de esta Corporación Insular, y las atribuciones que ostenta la Dirección Insular de Modernización del Área de Presidencia, Hacienda y Modernización, en virtud de Acuerdo de "Nombramientos de órganos directivos de la Administración Insular" de fecha 6 de agosto de 2019, lo previsto en el Reglamento Orgánico corporativo, se eleva el presente informe a la Consejería Insular del Área de Presidencia, Hacienda y Modernización, por la presente, **EL CONSEJO DE GOBIERNO INSULAR ACUERDA**:

PRIMERO.- Modificar la Política de Seguridad del Cabildo Insular de Tenerife en el sentido que a continuación se detalla:

El apartado séptimo de la Política de Seguridad, concerniente a la Organización de la Seguridad en el Cabildo, queda redactado de la siguiente forma:

- El Comité de Dirección se reunirá con carácter ordinario, como mínimo, cada doce meses y extraordinariamente cuantas veces estime necesario su Presidencia.

- El Comité Técnico se reunirá con carácter ordinario, como mínimo, cada doce meses y extraordinariamente cuantas veces estime necesario su Presidencia.

SEGUNDO.- En consecuencia, la Política de Seguridad del Cabildo Insular de Tenerife quedará redactada conforme al siguiente contenido:

Política de Seguridad de la información

1 Aprobación y entrada en vigor

La Política de Seguridad de la Información, en adelante, PSI, será aprobada por acuerdo del Consejo de Gobierno Insular (en adelante, CGI) del Cabildo Insular de Tenerife (en adelante, CIT).

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

2 Introducción

Los sistemas de información constituyen elementos básicos para la gestión de las actividades encomendadas al **CIT**, por lo que deben ser objeto de una especial protección a fin de que cumplan los requisitos de **disponibilidad**, **integridad**, **confidencialidad, trazabilidad** y **autenticidad** precisos.

El objetivo de la seguridad de la información es garantizar la calidad de la misma y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. En este sentido, a fin de dar cumplimiento al objetivo anterior, el CIT aborda en esta política de manera conjunta y coordinada tanto los sistemas TIC como los sistemas de información que dependen directamente de la seguridad física de la corporación insular.

Por un lado, los **sistemas TIC** deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

La responsabilidad en la explotación de los servicios basados en las Tecnologías de Información y las Comunicaciones (TIC) en el CIT es responsabilidad de la Dirección Insular de Modernización.

Por otro lado, los **sistemas de información también deben estar protegidos desde la seguridad física** de la Corporación Insular entendiendo por ella todos aquellos mecanismos -generalmente de prevención y detección- destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina, lo cual dependerá de las condiciones físicas del entorno y también de los sistemas o medios de información a proteger.

La responsabilidad en la seguridad física de la información en el CIT dependerá de los servicios y unidades administrativas que designe la Dirección Insular de Recursos Humanos y Asesoría Jurídica y será responsabilidad directa de esta última.

Tanto los servicios, unidades organizativas técnicas y administrativas, responsables de la explotación de los servicios TIC como los designados por la Dirección Insular de Recursos Humanos en términos de seguridad física, deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, (ENS), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. El nivel de seguridad se establecerá según la categoría del sistema de información reflejado en el informe de categorización de los sistemas del CIT y en función de los riesgos a los que está expuesto, dentro del marco estableció en el Artículo 43 del ENS.

La seguridad TIC y física debe ser una parte integral de cada etapa del ciclo de vida de los sistemas de información y, especialmente, de los servicios TIC desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la elaboración de presupuestos y en la licitación para proyectos de TIC, por la Dirección y las unidades organizativas administrativas y técnicas asociadas.

Las unidades organizativas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del ENS.

3 Misión

Las competencias del CIT vienen recogidas en la Ley 8/2015, de 1 de abril, de Cabildos Insulares.

El CIT para la gestión de sus intereses y de las funciones y competencias que tiene encomendadas, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y expectativas de la población y de todos los grupos de interés.

El CIT desea potenciar el uso de las nuevas tecnologías tanto internamente como en sus relaciones con la ciudadanía.

Los principales objetivos que se persiguen son, entre otros, los siguientes:

- Mejorar la calidad de los servicios públicos
- Fomentar la relación electrónica de la ciudadanía con el CIT, creando la confianza necesaria entre ciudadano y el CIT en esa relación.
- Reducir los tiempos de tramitación.
- Reducir las cargas administrativas.
- Hacer transparente la actividad del Cabildo.
- Fomentar la participación y colaboración.

4 Ámbito de aplicación

Esta política aplica a todos los sistemas de información, especialmente a los TIC del CIT.

Además, aplicará y será de obligado cumplimiento para los organismos autónomos dependientes, entidades públicas empresariales dependientes y consorcios del CIT en relación con todos los sistemas de información que éste les preste.

Todas estas entidades (organismos autónomos, entidades públicas empresariales y consorcios) deberán articular los roles de seguridad descritos en esta política y participar en los comités a través de sus representantes.

Esta política de seguridad es de obligado cumplimiento para todo el personal que acceda a los sistemas de información TIC, así como a la propia información gestionada por los diferentes organismos en cualquiera de sus formas y formatos. Aplica con independencia de cuál sea la relación o adscripción con el mismo.

Queda fuera del ámbito de esta política de seguridad todas aquellas actividades que realicen las entidades del SPI al margen de los servicios prestados por el CIT.

5 Marco normativo

Las actividades del CIT están reguladas por un marco normativo específico que recoge su composición, dependencia y funciones.

En materia de seguridad de la información, el Comité de Seguridad Corporativa se compromete a identificar y comunicar a su personal la legislación aplicable y a realizar las medidas de difusión, concienciación y control necesarias.

Para la elaboración de esta normativa se han tenido en cuenta los siguientes documentos:

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Real Decreto 3/2010, de 8 de enero por el que se regula el ENS en el ámbito de la administración electrónica y su modificación por el Real Decreto 951/2015, de 23 de octubre.

- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

- La guía CCN-STIC 801 Esquema Nacional de Seguridad. Responsabilidades y funciones

- 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 y por el que se deroga la Directiva 95/46/CE (RGPD, en adelante)

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD, en adelante).

- Ley 8/2015, de 1 de abril, de Cabildos Insulares.

6 Principios básicos de la seguridad de la información

Los principios básicos son directrices fundamentales de seguridad que han de tenerse presentes en cualquier actividad relacionada con el uso de los sistemas de información.

En el artículo 4 del ENS se establecen los siguientes:

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. 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

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

c) **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. Supondrá un deber de protección del patrimonio digital del Cabildo.

d) **Líneas de defensa**. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta 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, minimizar el impacto final sobre el mismo.

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

e) **Reevaluación periódica**. 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.

f) **Función diferenciada**. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad, fijando roles y responsabilidades.

De igual modo se establecen los siguientes principios de protección de datos:

g) **Los datos son tratados de manera lícita, leal y transparente** en relación con el interesado («licitud, lealtad y transparencia»).

h) **Los datos son recogidos con fines determinados, explícitos y legítimos,** y no serán tratados ulteriormente de manera incompatible con dichos fines; («limitación de la finalidad»).

i) **Los datos son adecuados, pertinentes y limitados** a lo necesario en relación con los fines para los que son tratados («minimización de datos»).

j) **Los datos son exactos y, si fuera necesario, actualizados;** se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»).

k) Los datos son mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales («limitación del plazo de conservación»).

l) Los datos son tratados de tal manera que se garantice una seguridad adecuada de los datos personales, 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 («integridad y confidencialidad»).

Además, en el CIT se añaden los siguientes:

m) **Alcance estratégico**: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas y conformar un todo coherente y eficaz.

n) **Proporcionalidad**: el establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

o) **Mejora continua**: las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

p) **Seguridad desde el diseño y por defecto**: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

7 Organización de la seguridad

Conforme al principio básico de seguridad de función diferenciada y tal como indica el artículo 12 del ENS, la seguridad deberá comprometer a todos los miembros de la organización.

Se establecen los siguientes roles y comités en la organización relacionados con la Seguridad de la Información, que se detallan en los siguientes apartados:

- Roles y responsabilidades.
- Comités:
  - Comité de Dirección (CD, en adelante)
  - Comité Técnico (CT, en adelante)

Figura 1. Roles y comités en el CIT relacionados con la Seguridad de la Información

7.1 Roles y Responsabilidades

Rol	Responsabilidades
Responsable Interno (RI) Se unifican las figuras de Responsable de la Información, Responsable del Tratamiento y Responsable del Servicio, de la normativa ENS, en la figura del Responsable Interno (RI), rol que será desempeñado con carácter general por el Jefe/a de Servicio con responsabilidad sobre el servicio e información asociada al sistema de información a excepción de los servicios considerados corporativos comunes en el CIT.	El RI tiene la responsabilidad última del uso que se haga de la información de los servicios, por tanto, de su protección, así como de cualquier incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información). Es el responsable de establecer los requisitos de la información y del servicio en materia de seguridad, determinando los niveles de seguridad en cada dimensión, pudiendo, para ello, recabar una propuesta al RST y escuchar la opinión del RSIS. Los criterios de valoración estarán alineados con esta PSI, de acuerdo a lo establecido en el ENS en el Anexo I del Esquema Nacional de Seguridad, sin perjuicio de que puedan darse criterios particulares en casos singulares. Además, como responsable interno del tratamiento de datos debe colaborar en la determinación de los fines y medios del tratamiento. Ha de velar por el cumplimento en materia de protección de datos y seguridad de la información debiendo ser reportado por los usuarios sobre estos asuntos. Deberá colaborar en la demostración del cumplimiento en protección de datos.
Responsable Interno de Servicios Corporativos Comunes (RISCC) Se unifican las figuras de Responsable de la Información, Responsable del Tratamiento y Responsable del Servicio, de la normativa ENS, en la figura del Responsable Interno (RISCC) para aquellos servicios corporativos comunes.	a) Las responsabilidades del RISCC son idénticas al RI y en exclusivo para los servicios corporativos del CIT b) El RISCC podrá asignar a los Jefes/as de Servicio aquellas funciones que considere necesarias para agilizar la prestación del mismo, siendo el responsable de velar por las medidas de seguridad que se apliquen.

Responsable de Seguridad Técnica (RST) El RST determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, siendo el responsable de aplicación de las medidas técnicas de seguridad de los sistemas bajo su responsabilidad.	La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios: a) Mantener la seguridad de la información gestionada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con la PSI del CIT b) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. c) Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro. d) Elaboración de la memoria anual del estado de seguridad de los sistemas y presentación al comité. e) El RST podrá delegar, de forma documentada, algunas de sus funciones en otras partes del CIT. f) Además, las tareas definidas en el apartado “Tareas” de esta PSI. En caso de ocurrencia de incidentes de seguridad de la información: g) Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.

Responsable de Seguridad Física (RSF) El Responsable de seguridad física tendrá competencia y capacidad suficiente para decidir, implantar o ejecutar, hacer seguimiento, evaluación y corrección de medidas que afecten a la seguridad física, y cuantas otras propongan el CD en esta materia, además, este último velará por que se cumpla con todo lo anterior.	a) Establecer una estrategia integral de protección constituida por múltiples capas de seguridad predefinidas y establecidas en el CIT. b) Establecer medidas que protejan y aseguren la integridad e indemnidad de las instalaciones y dependencias del CIT. Especialmente, en las siguientes materias que se señalan con carácter enunciativo no limitativo: - Autorización y control de accesos a dependencias e instalaciones - Protección de las instalaciones - Protección de la información almacenada y en tránsito c) Implantar y ejecutar directamente las medidas de seguridad física que le competan. d) Implantar y ejecutar medidas propuestas y aprobadas previamente por el Comité de Dirección (CD). e) Asegurar la integridad, disponibilidad y confidencialidad de los elementos críticos del sistema de información en soporte físico. f) Informar al CD del grado de implantación de las medidas, su eficacia y los incidentes de seguridad física con carácter anual. En caso de ocurrencia de incidentes de seguridad física que afecte a la información del CIT: g) Planificar la implantación de medidas de salvaguardas de la información. h) Tomar decisiones a corto plazo si la información se ha visto comprometida y pudiera tener consecuencias graves i) Investigar el incidente: determinar el modo, los medios, los motivos y el origen del incidente y promover e implantar directamente las medidas que permitan evitar el mismo en el futuro.

Responsable de Seguridad Corporativa (RSC)	a) Encargada de velar por la armonización de la seguridad de información en sus diferentes vertientes: protección física, protección de los servicios y respecto de la privacidad. b) Recaba las inquietudes de los responsables de seguridad y lo traslada y debate en el Comité para su examen y acciones pertinentes. c) Debe de estar al tanto de cambios regulatorios y normativos que afecten al CIT. Debiendo informar de las consecuencias para las actividades del CIT, alertando al comité y responsables de seguridad dependiente, proponiendo las medidas oportunas de adecuación al nuevo marco. d) Es el responsable de la toma de decisiones cotidianas entre reuniones del comité y de informar de las mismas cuando estos se reúnan. e) Encargado de coordinar las actuaciones, en caso de incidencias que tengan repercusión fuera del CIT y en caso desastre.
Responsables del Sistema (RSIS)	a) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. b) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. c) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. d) Los RSIS puede proponer al CD 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 RIs y el RSC correspondiente antes de ser propuesta. En caso de ocurrencia de incidentes de seguridad de la información: e) Planificar la implantación de las salvaguardas en el sistema. f) Ejecutar el plan de mejora de la seguridad aprobado. g) Tomar decisiones a corto plazo si la información se ha visto comprometida y pudiera tener consecuencias graves h) Asegurar la integridad de los elementos críticos del sistema de información si se ha visto afectada la disponibilidad de estos. i) Mantener y recuperar la información almacenada por el sistema de información y sus servicios asociados. j) Investigar el incidente: determinar el modo, los medios, los motivos y el origen del incidente.

Delegado en Protección de Datos (DPD) El rol del Delegado en Protección de Datos es una figura requerida en la sección 4 del RGPD y en el capítulo III de la LOPDGDD.	a) Informar y asesorar al responsable y/o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de los datos personales de las obligaciones que les incumben en virtud del RGPD y otras disposiciones de protección de datos. b) Supervisar el cumplimiento de lo dispuesto en el RGPD, en otras disposiciones de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes. c) Ofrecer el asesoramiento que se le pida acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización. d) Cooperar y actuar de contacto con la autoridad de control, en este caso la Agencia de Protección de Datos para las cuestiones relacionadas con el tratamiento de datos personales incluidas la consulta previa, y consultar en su caso, sobre cualquier otro asunto. e) Ser oído en todos los aspectos relacionados con la seguridad de los datos personales y violaciones de seguridad de datos personales, entendiendo las mismas desde la perspectiva de la confidencialidad, integridad y disponibilidad. f) Participar en las reuniones del Comité de Dirección con voz, pero sin voto. g) Emitir su parecer en aquellos aspectos relacionados con la seguridad de los datos personales, promover, en su caso, revisiones de análisis de riesgos, elaboración de evaluaciones de impacto en protección de datos, elaboración o modificación de procedimientos o políticas de seguridad de datos personales, entre otros. h) Asesorar sobre la conveniencia o no de comunicar a la autoridad de control de protección de datos y. en su caso, a los interesados las violaciones de seguridad de datos personales. En caso afirmativo proceder a la notificación a la autoridad de control en representación del responsable del tratamiento i) Promover acciones de formación y concienciación en privacidad. j) Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos. k) Identificación de las bases jurídicas de los tratamientos. l) Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos. m) Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos. n) Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.

	o) Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados. p) Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
	q) Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia. r) Diseño e implantación de políticas de protección de datos. s) Auditoría de protección de datos. t) Establecimiento y gestión de los registros de actividades de tratamiento. u) Análisis de riesgo de los tratamientos realizados. v) Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos. w) Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos. x) Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados. y) Relaciones con las autoridades de supervisión z) Implantación de programas de formación y sensibilización del personal en materia de protección de datos

Encargado del Tratamiento (ET) El encargado de tratamiento trata datos personales por cuenta del Responsable del Tratamiento. Debe aportar garantías suficientes de cumplimiento con el RGPD y adoptar las medidas de seguridad del ENS que correspondan al responsable de tratamiento.	a) Adoptar las medidas de seguridad que correspondan al responsable del tratamiento b) Aportar garantías suficientes de cumplimiento con el RGPD. c) Tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional d) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria e) Tomar todas las medidas de seguridad necesarias f) En general, no recurrir a otro encargado del tratamiento g) Asistir al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados h) Ayudar al responsable a garantizar el cumplimiento sus obligaciones i) Seguir las indicaciones del responsable una vez finalice la prestación de los servicios de tratamiento (suprimirá o devolverá todos los datos personales, y suprimirá las copias existentes)
	j) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable. k) Informar inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos

Comité de Dirección (CD)

7.1.1 Finalidad

El Comité de Dirección (CD) coordinará las actividades y controles de seguridad, velando por el cumplimiento de la normativa vigente -interna y externa- en materia de protección de datos y seguridad. Asimismo, es el espacio en donde se deberán tomar las decisiones estratégicas.

7.1.2 Composición

El Comité de Dirección lo componen:

- Los miembros del CIT del Comité de Dirección del Plan de Modernización.
- Responsable de seguridad Corporativa
- Representante de los consorcios a los que aplique la política.

7.1.3 Funciones

Asume las siguientes funciones:

a) Elaborar la estrategia de evolución de la entidad en lo que respecta a la seguridad de la información.
b) Coordinar las funciones de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
c) Velar por el cumplimiento de la normativa de carácter legal, regulatoria y sectorial
d) Velar por el alineamiento de las actividades de seguridad y de los objetivos de la organización
e) Coordinar los planes de continuidad de las diferentes áreas para asegurar una actuación sin fisuras en el caso de que deban ser activados
f) Elaborar la Política de Seguridad de la Información (PSI), que será aprobada por acuerdo del Consejo de Gobierno Insular (CGI).
g) Coordinar y aprobar las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad.
h) Aprobar la dotación presupuestaria correspondiente a los planes de mejora de seguridad de la información de la entidad.

7.1.4 Organización y funcionamiento

El CD se reunirá con carácter ordinario, como mínimo, cada doce meses y extraordinariamente cuantas veces estime necesario su Presidencia. Se levantará acta de estas reuniones, pudiéndose en dichas reuniones tratar, entre otros, los siguientes temas:

- Revisión de la PSI
- Seguimiento de los objetivos del sistema de seguridad
- Seguimiento del cuadro de indicadores y métricas
- Seguimiento de los planes de formación y de concienciación

Cuando los asuntos a tratar incidan o puedan incidir en tratamientos de datos personales, se deberá convocar al Delegado de Protección de Datos de CIT quien asistirá a la reunión con voz, pero sin voto.

En el trabajo e intercomunicación de las personas que forman parte del Comité se utilizarán preferentemente métodos telemáticos de transmisión de la información.

7.2 Comité Técnico (CT)

7.2.1 Finalidad

El Comité de Técnico (CT) coordina la seguridad de la información en el CIT.

Este comité coordinará además las actividades y controles de seguridad, velando por el cumplimiento de la normativa vigente -interna y externa- en materia de protección de datos y seguridad. Asimismo, tendrá la naturaleza de grupo de trabajo, y es el espacio en donde se deberán tomar las decisiones técnicas.

7.2.2 Composición

El Comité Técnico lo componen:

- Los miembros del Comité Técnico del Plan de Modernización.
- Responsable de seguridad Corporativa
- Responsable de seguridad Física
- Responsable de seguridad Técnica
- Delegado de protección de datos
- Responsables de seguridad de las entidades del SPI a los que aplique la política.

7.2.3 Funciones

Asume las siguientes funciones, además de las competencias establecidas por el Plan de Modernización:

a) Atender a las inquietudes del CIT, recabar respuestas y soluciones.
b) El RSC se encargará de llevar a cabo un control y presentación regular del progreso de los proyectos y anuncios de las posibles desviaciones.
c) Recabar de los RSF y RST informes regulares del estado de seguridad del CIT y de los posibles incidentes. Estos informes se consolidan y resumen para los órganos de gobierno.
d) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información. Tras analizar las propuestas y recomendaciones del DPO en violaciones de seguridad que afecten a datos personales, recomendar al RI su notificación o no a la autoridad de control y en su caso a los propios interesados
e) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
f) Aprobar planes de mejora de la seguridad de la información de la entidad. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
g) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
h) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
i) Monitorizar los principales riesgos residuales asumidos por la entidad y recomendar posibles actuaciones respecto de ellos.
j) Definir, dentro de la PSI, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes respecto a la segregación de funciones.
k) Definición de los objetivos de seguridad
l) Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
m) Aprobar la normativa de seguridad de la información.
n) Podrá constituir equipos de trabajo, con la composición que sea necesaria, para el estudio y presentación de informes relacionados con los objetivos del Plan de Mejora de la Seguridad:

    - Grupos de trabajo especializados internos, externos o mixtos.
    - Asesoría interna y/o externa.
    - Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

7.2.4 Organización y funcionamiento

El CT se reunirá con carácter ordinario, como mínimo, cada doce meses y extraordinariamente cuantas veces estime necesario su Presidencia. Se levantará acta de estas reuniones, pudiéndose en dichas reuniones tratar, entre otros, los siguientes temas:

- Seguimiento de los servicios prestados por terceros
- Seguimiento de los planes de actuación (planes de tratamiento de riesgos)
- Seguimiento de los proyectos de mejora en materia de seguridad de la información
- Seguimiento de la gestión de incidentes de seguridad
- Seguimiento de las pruebas de los planes de continuidad de negocio
- Revisión de contratos de servicios con terceros
- Revisión de la normativa aplicable
- Aprobación de la documentación del ENS

En el trabajo e intercomunicación de las personas que forman parte del Comité se utilizarán preferentemente métodos telemáticos de transmisión de la información.

7.3 Matriz RACI

La matriz de la asignación de responsabilidades (RACI por las iniciales, en inglés, de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera se logra asegurar que cada una de las tareas esté asignada a un individuo o a un equipo.

	ROL	DESCRIPCIÓN
R	**Responsable** *(Responsible)*	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RACI. Es quien debe ejecutar las tareas.
A	**Administrador** *(Accountable)*	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	**Consultado** *(Consulted)*	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	**Informado** *(Informed)*	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

TAREA	CD	CT	RI	RISCC	RSC	RST	RSF	DPD	RSIS
Niveles de seguridad requeridos por la información			AI	AI	I	R		C	C
Niveles de seguridad requeridos por el servicio			IA	IA	I	R		C	C
Determinación de la categoría del sistema			I	I	I	A/R	A/R	I	I
Establecimiento y gestión de los registros de actividades de tratamiento.								A/R	
Análisis de riesgos			I	I	I	A/R	A/R	R	C
Declaración de aplicabilidad			I	I	I	A/R		I	C
Medidas de seguridad adicionales			I	I	R	A/R	A/R	I	C
Configuración de seguridad			I	I	I	A	A	C	C/R
Aceptación del riesgo residual		R	A	A	R	R	R	I	I
Documentación de seguridad			IR	IR	A	A	A	C	C/I
Política de seguridad	A		I	I	R	R	R	I	C
Normativa de seguridad		A/R	I	I	A	A	A	I	C
Procedimientos de seguridad			IR	IR	C	C	CA	I	A
Implantación de las medidas de seguridad			I	I	R/I	C	R/I	I	A/R
Supervisión de las medidas de seguridad(1)			I	I	I	A	I	C	C
Estado de seguridad del Sistema	I		I	I	I	A	R/I	I	R
Planes de mejora de la seguridad	R		I	I	I	A	A	C	C
Planes de concienciación y formación	R		I	I	A	A	A	C	C

(1) Algunas tareas carecen de R porque no entra dentro del alcance de esta guía establecer quién se encarga de su realización. No obstante, se deberá determinar quién se encarga de cada tarea o cómo se subdivide hasta poder concretar.

7.4 Procedimiento de designación.

Los distintos responsables del ENS serán designados por el CD. Se nombrarán y documentará en las actas de reunión de dicho comité.

8 Datos de carácter personal

El CIT trata datos de carácter personal. El Registro de Actividades del Tratamiento detalla los tratamientos afectados y los responsables correspondientes, así como las medidas de seguridad adoptadas derivadas de la evaluación de impacto y análisis de riesgo realizado sobre los tratamientos.

Las medidas de seguridad a aplicar a los datos de carácter personal se corresponden con las previstas en el ENS.

Todos los sistemas de información del CIT se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades de Tratamiento.

9 Gestión de riesgos

9.1 Justificación

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

9.2 Criterios de evaluación de riesgos

Para la armonización de los análisis de riesgos, el Comité de Dirección establecerá a propuesta del Comité Técnico una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Los criterios de evaluación de riesgos detallados se especifican en la metodología de evaluación de riesgos del CIT, basada en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

9.3 Directrices de tratamiento

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9.4 Proceso de aceptación del riesgo residual

Los riesgos residuales serán determinados por el Responsable Interno.

Los niveles de riesgo residuales esperados sobre cada Información y sobre cada servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su responsable interno.

Los niveles de riesgo residuales serán presentados por el Responsable Interno al Comité Técnico, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

9.5 Necesidad de realizar o actualizar las evaluaciones de riesgos

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

10 Gestión de incidentes de seguridad

El CIT debe estar preparado para prevenir en la medida de lo posible que la información o servicios se vean perjudicados por incidentes de seguridad. Se deben poder detectar anomalías monitorizando la operación continua de los servicios. Para responder de forma eficaz a los incidentes, se deben establecer los procedimientos necesarios.

El CIT debe también diseñar planes de continuidad de los servicios TIC.

11 Desarrollo de la política de seguridad de la información

La Política de Seguridad de la Información en el ámbito de la administración electrónica se deberá alinear con las políticas existentes en el CIT, complementándolas en aquellos aspectos específicos que sean requeridos. Estas políticas del CIT están documentadas y publicadas en los sistemas de información del Cabildo.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

12 Gestión del personal

12.1 Obligaciones del personal

Todos los miembros del CIT tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Dirección disponer los medios necesarios para que la información llegue a los afectados. Para ello, esta política estará disponible en el sitio web del CIT (intranet) y, al menos una vez al año, se recordará a todo el personal, ya sea de forma presencial u on-line, la necesidad de su conocimiento y cumplimiento y se notificará cualquier cambio que

se haya producido. Asimismo, se establecerá un programa de concienciación continua para atender a todos los miembros del CIT, en particular, a los de nueva incorporación.

Las personas con responsabilidades en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidad en el mismo.

12.2 Concienciación y formación

El personal del CIT recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del CIT.

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros del CIT y a todas las actividades, de acuerdo al principio de Seguridad Integral recogido en el artículo 5 del ENS, así como la articulación de todos los medios necesarios para que todas las personas que intervienen en proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Se difundirán todos aquellos documentos que aplican a cada nivel en los distintos puestos de trabajo.

13 Profesionalidad

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

Se hace necesario que, de manera objetiva y no discriminatoria, las organizaciones que presten servicios de seguridad del CIT cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

14 Terceras partes

Cuando el CIT utilice servicios de terceros o ceda información a terceros, se les hará participes de esta Política de Seguridad de la Información y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta 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. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en la política.

Cuando el CIT preste servicios a otros organismos 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 Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando algún aspecto de la Política no pueda ser satisfecho para una tercera parte según se requiere 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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

15 Autorización y control de los accesos

El acceso a los sistemas de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas. Dicha responsabilidad recaerá sobre el Responsable Interno (RI).

Los Responsables Internos deberán velar, en el ámbito de sus servicios y competencias por lo anterior y, a su vez, cumplir con las instrucciones de coordinación, medidas y estrategias que determine el Responsable de Seguridad Física.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad

16 Protección de las instalaciones

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Por ello, en primer lugar, se ha de establecer un perímetro físico de seguridad que proteja la información de la organización para prevenir incidencias, y garantizar el funcionamiento del resto de medidas.

El acceso a los locales, mediante vías de acceso autorizadas y controladas, barreras arquitectónicas como paredes o ventanas, elementos adicionales como áreas de descarga controladas, debe ser gestionado para proteger las zonas que contienen instalaciones informáticas o permiten el acceso a las mismas.

Dentro del perímetro de seguridad, se deben identificar las ubicaciones que almacenan soportes que puedan contener datos confidenciales o especialmente protegidos, estas ubicaciones dispondrán de una identificación personal de los usuarios que permita validar sí disponen de autorización para su acceso.

Se deben validar las medidas de seguridad físicas de acceso al perímetro de seguridad, compuestas por puertas, cerraduras, alarmas, vigilancia y formalizarlas en instrucciones de acceso a los locales, que deberán ser comunicadas a todo el personal.

Los Responsables Internos deberán velar, en el ámbito de sus servicios y competencias por lo anterior y, a su vez, cumplir con las instrucciones de coordinación, medidas y estrategias que determine el Responsable de Seguridad Física.

17 Adquisición de productos de seguridad

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones, así como, de seguridad física, que vayan a ser utilizados por el CIT se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, y se velará por que se contemple en los pliegos contractuales,

La certificación indicada deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

18 Seguridad por defecto

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

19 Integridad y actualización del sistema

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

20 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. Tendrán la consideración de entornos inseguros los siguientes dispositivos: equipos portátiles, tabletas, dispositivos periféricos, soportes de información (pendrive, disco duro) y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por el CIT en el ámbito de sus competencias.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de estos.

21 Prevención ante otros sistemas de información interconectados

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados

de la interconexión del sistema, o a través de redes, con otros sistemas, y se controlará su punto de unión.

22 Continuidad de la actividad

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

23 Mejora continua del proceso de seguridad

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

24 Cuerpo normativo

La estructura jerárquica de la documentación de seguridad será la siguiente:

Documento	Detalle	Ubicación
Política	• Define las metas y expectativas de seguridad. • Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos.	• Disponible . pdf en la intranet: https://www.tenerife.int/intranet • Disponible .doc en la herramienta de gestión del ENS
Normativa	• Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. • Es de carácter obligatorio.	• Disponible pdf en la intranet: https://www.tenerife.int/intranet • Disponible .doc en la herramienta de gestión del

Documento	Detalle	Ubicación
		ENS
Procedimiento	• Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución. • Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar. • Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad.	• Disponible .pdf en la intranet los de Uso interno y externo: https://www.tenerife.int/intranet • Disponible .doc en la herramienta de gestión del ENS • Disponible en la herramienta de uso interno de gestión documental
Instrucciones técnicas	• Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.). • Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. • Una instrucción técnica debe ser clara y sencilla de interpretar. • Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de la misma. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución.	• Disponible en la herramienta de uso interno de gestión documental
Guías	• Tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo "*Guía de actuación RGPD con respecto al DPO*". • Las guías ayudan a prevenir que se pasen por alto aspectos	• Disponible .pdf en la intranet: https://www.tenerife.int/intranet • Disponible en el portal de informática

Documento	Detalle	Ubicación
	importantes de seguridad que pueden materializarse de varias formas.	
Registros	• Registro de actividad de la aplicación de los documentos anteriores que muestran la evidencia de su implantación y desarrollo en la organización	• Disponible los registros manuales en la herramienta de gestión del ENS • Disponibles en las herramientas de gestión de los sistemas automatizados

25 Revisión de la Política de Seguridad de la Información

La revisión anual de esta PSI será misión del Comité de Dirección.

La Política será aprobada por acuerdo de Consejo de Gobierno Insular del CIT.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas. Anexo I. Glosario de términos

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables.
Gestión de incidentes

Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.
Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
Incidente de seguridad

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.
Información

Caso concreto de un cierto tipo de información.
Política de seguridad

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.
Principios básicos de seguridad

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.
Responsable de la seguridad
El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que se encarga de la explotación del sistema de información.
Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.
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.

TERCERO.- Comunicar y difundir el contenido de la Política de Seguridad conforme se detalla:

Difusión externa:

- Publicación en el Portal de Transparencia y la Sede Electrónica del Cabildo Insular de Tenerife.

Difusión interna:

- Notificación a los entes del sector público insular incluidos en el ámbito subjetivo.
- Publicación en la Intranet Corporativo.
- Correo informativo a Cabildo Completo y todo su sector público.

Contra el presente acuerdo, que pone fin a la vía administrativa, se podrá interponer, potestativamente, **RECURSO POTESTATIVO DE REPOSICIÓN** ante el mismo órgano que ha dictado el acto impugnado, en el plazo de UN MES, contado a partir del día siguiente al de la recepción de su notificación o directamente **RECURSO CONTENCIOSO-ADMINISTRATIVO** ante los Juzgados de lo Contencioso-Administrativo de los de Santa Cruz de Tenerife, dentro del plazo de DOS MESES contados a partir del día siguiente al de la recepción de la notificación, sin perjuicio de la interposición de cualquier otro recurso que estime procedente**.**