HISTÓRICO DE REVISIONES

Edición	*Modificado Por*	*Fecha*	*Motivo de la REVISIÓN*
2.0	Pablo M.P.	28/03/2019	Versión actualizada tras auditoría AENOR febrero 2019
3.0	Pablo M.P.	22/12/2020	Versión aprobada por el Consejo de Administración de Metrotenerife
4.0	Pablo M.P.	07/02/2023	Adecuación a nuevo ENS según RD 311/2022. Versión aprobada por el Consejo de Administración de Metrotenerife
5.0	Comité de Seguridad de la Información	15/01/2025	Se añaden aspectos sobre los principios básicos del ENS, roles y responsabilidades, clasificación de la información y gestión de la documentación
6.0	Comité de Seguridad de la Información	01/04/2025	Versión actualizada tras auditoría AENOR marzo 2025
6.1	Comité de Seguridad de la Información	23/05/2025	Se añade fecha de actualización de última versión del documento en apartado 1

ELABORADO:	*CARGO:*	*FECHA:*	*FIRMA:*
Comité de Seguridad de la Información		01/04/2025	
REVISADO 1:	*CARGO:*	*FECHA:*	*FIRMA:*
REVISADO 2:	*CARGO:*	*FECHA:*	*FIRMA:*
Aprobado:	*CARGO:*	*Fecha:*	*Firma:*
D. Pedro Ribeiro	Dirección General		

índice

1 APROBACIÓN Y ENTRADA EN VIGOR

Esta política fue aprobada inicialmente el día 29 de Octubre de 2018, revisada posteriormente en varias ocasiones por la Dirección General de Metropolitano de Tenerife S.A., siendo la última de éstas revisiones la de fecha 23 de Mayo de 2025, y siendo efectiva desde esta fecha y hasta que sea reemplazada por una nueva.

La Dirección General de Metropolitano de Tenerife, S.A. se compromete a difundirla y a revisarla periódicamente con la finalidad de introducir los cambios que sean convenientes.

2 INTRODUCCIÓN

Metropolitano de Tenerife S.A. (en adelante Metrotenerife), es una empresa pública del Cabildo de Tenerife que opera y mantiene las líneas de metro ligero en Tenerife. Proporciona un servicio de transporte público de calidad y ofrece mejoras y alternativas al desarrollo de nuevas soluciones de transporte en la isla.

Para lograr una gestión eficaz y eficiente de las mismas, Metrotenerife se apoya en sus sistemas de tecnologías de la información y las comunicaciones, (STIC).

Estos sistemas se convierten en pilares básicos para su funcionamiento, por lo que deben ser objeto de una especial protección a fin de que cumplan los requisitos definidos en el RD 311/2022 Esquema Nacional de Seguridad (en adelante, ENS).

La Política de Seguridad de la Información, que se plasma en este documento, recoge la forma en que Metrotenerife gestiona y protege la información y los servicios. En concreto, aquellos que hace uso el ciudadano por medios electrónicos para el ejercicio de derechos y el cumplimiento de deberes en su relación con Metrotenerife.

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.

Los STIC deben estar protegidos contra amenazas, de rápida evolución, con potencial para incidir en la integridad, disponibilidad, autenticidad, trazabilidad, confidencialidad, 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 continuidad de los servicios prestados.

Esto implica que los diferentes departamentos en que se articula Metrotenerife deben cerciorarse de que la seguridad de los STIC es una parte integral de cada etapa de sus actividades y, desde su concepción hasta la retirada de servicio, deben aplicar las medidas mínimas de seguridad exigidas por el ENS para evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad, realizar un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes. El nivel de seguridad se establecerá según la categoría del sistema de

información reflejado en el informe de categorización de los sistemas de Metrotenerife y en función de los riesgos a los que está expuesto, como se indica en el Artículo 40 del ENS.

3 ALCANCE

Esta política aplica y será de obligado cumplimiento para todos los departamentos de Metrotenerife, así como para terceras partes con las que Metrotenerife comparta información o reciba algún servicio que implique el acceso a la misma.

Para facilitar su conocimiento y cumplimiento, estará disponible en el sitio web de Metrotenerife, así como en la intranet corporativa.

4 MISIÓN

Metrotenerife nace para poner en marcha un transporte alternativo en forma de líneas ferroviarias en la isla de Tenerife. En la actualidad gestiona dicho servicio ferroviario, que contribuye a aliviar la congestión circulatoria y a facilitar y satisfacer las demandas de movilidad de la población de Tenerife y de sus visitantes.

Metrotenerife es miembro de la UITP, "Union Internationale des Transports Publics" y es uno de los dos representantes españoles que participan como miembros en su Comité de Metros Ligeros. También pertenece a la Asociación Latinoamericana de Metros y Subterráneos (ALAMYS) y a la Asociación de Empresas Gestoras de los Transportes Urbanos Colectivos (ATUC).

5 MARCO NORMATIVO

Las referencias tenidas en cuenta para la redacción de esta política y el resto de normativa y procedimientos han sido las indicadas en el documento marco: **“NOR-000: Legislación y Normativa Aplicable”** que de manera periódica se actualiza, atendiendo aquella normativa de aplicación principalmente en lo relativo a protección de datos personales y seguridad de la información.

Además, se ha tenido en cuenta en especial la Guía “CCN-STIC-821 Normas de seguridad en el ENS” y el Anexo I de la Guía “CCN-STIC-822” - Procedimientos de seguridad en el ENS”.

Así mismo, Metrotenerife, también será responsable de identificar las guías de seguridad del CCN, que serán de aplicación para mejorar el cumplimiento de lo establecido en el ENS.

6 PRINCIPIOS BÁSICOS

Todos los servicios deben estar preparados para cumplir con sus objetivos utilizando sistemas de información, por lo que deben asegurar que se cumplen los siguientes principios básicos:

6.1 SEGURIDAD INTEGRAL

La seguridad de la información es un proceso integral del que forman parte todos los elementos técnicos, humanos, materiales y organizativos de Metrotenerife. En este sentido, se prestará la máxima atención a la formación y concienciación de las personas que intervienen en el proceso de seguridad y concretamente de los responsables en materia de seguridad, que deberán recibir formación específica.

Metrotenerife formará e informará a todo su personal acerca de los deberes y obligaciones en materia de seguridad y garantizará que la atención, revisión y auditoría de los sistemas de seguridad se lleven a cabo por personal cualificado, bajo criterios de profesionalidad, exigiendo además que las organizaciones que le presten servicios cuenten con profesionales y técnicos cualificados y con niveles idóneos de calidad y excelencia en la prestación de sus servicios.

6.2 GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS

La gestión de los riesgos es parte fundamental para el proceso de seguridad. Metrotenerife, a través de los responsables en materia de seguridad, deberá implementar mecanismos de gestión del riesgo, minimizándolos hasta niveles aceptables mediante el despliegue de medidas de seguridad, en todo caso garantizando el equilibrio entre la naturaleza de la información, los riesgos a los que se expone y las medidas de seguridad a adoptar.

6.3 PREVENCIÓN

Todos los servicios de Metrotenerife deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional que sea preciso establecer tras una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

6.4 DETECCIÓN

Dado que los servicios son vulnerables y se pueden degradar rápidamente debido a incidentes que pueden producir desde una simple desaceleración hasta su detención, se monitorizarán las operaciones de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables de seguridad de forma regular, y especialmente cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

6.5 RESPUESTA

Metrotenerife debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Establecer un punto de contacto para comunicar incidentes detectados en otros servicios o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6.6 RECUPERACIÓN

Se tendrá en cuenta la importancia de la recuperación de los STIC y la disponibilidad de los servicios críticos en caso de incidencia, incluyendo la copia de seguridad de los sistemas de información.

6.7 EXISTENCIA DE LÍNEAS DE DEFENSA

Metrotenerife cuenta con una estrategia de protección formada por múltiples capas de seguridad que permitan reaccionar ante incidentes inevitables; reducir la probabilidad de que el sistema quede comprometido y minimizar el impacto de un incidente ya producido. En este sentido, será de especial importancia para la seguridad de la información las siguientes actuaciones de Metrotenerife:

- El control y limitación del acceso a los sistemas de información, el registro de las actividades de los usuarios, y la identificación conductas indebidas o no autorizadas.
- La protección física de las instalaciones de las que tengan control, a través de áreas supervisadas y separadas.
- La adquisición de productos de seguridad que cumplan con las garantías de seguridad necesarias en atención a la categoría de los sistemas y nivel de seguridad de la información afectada.
- La protección de la información almacenada o en tránsito a través de entornos inseguros, como los equipos portátiles, periféricos, soportes de información y comunicaciones.
- La protección de la información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica.
- La protección del perímetro y el análisis de los riesgos derivados de la interconexión del sistema con otros sistemas a través de redes.

6.8 REEVALUACIÓN PERIÓDICA Y VIGILANCIA CONTINUA

Metrotenerife implementará mecanismos para la detección de actividades o comportamientos anómalos y su oportuna respuesta.

Del mismo modo, se incluirá el proceso de seguridad en un ciclo de actualización y mejora continua. En este sentido, las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y de los sistemas de protección, bien por la aparición o incremento de los riesgos o bien en cumplimiento de la normativa vigente en cada momento.

6.9 DIFERENCIACIÓN DE RESPONSABILIDADES

A través de la presente Política de Seguridad y la normativa que la desarrolle se definirán los distintos roles intervinientes en el sistema de información, distinguiendo en cualquier caso, entre responsable de la información, el responsable del servicio, el responsable de seguridad y el responsable del sistema, así como se indicarán las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos, existiendo en todo momento una obligación de cooperación y colaboración entre los distintos roles y responsables.

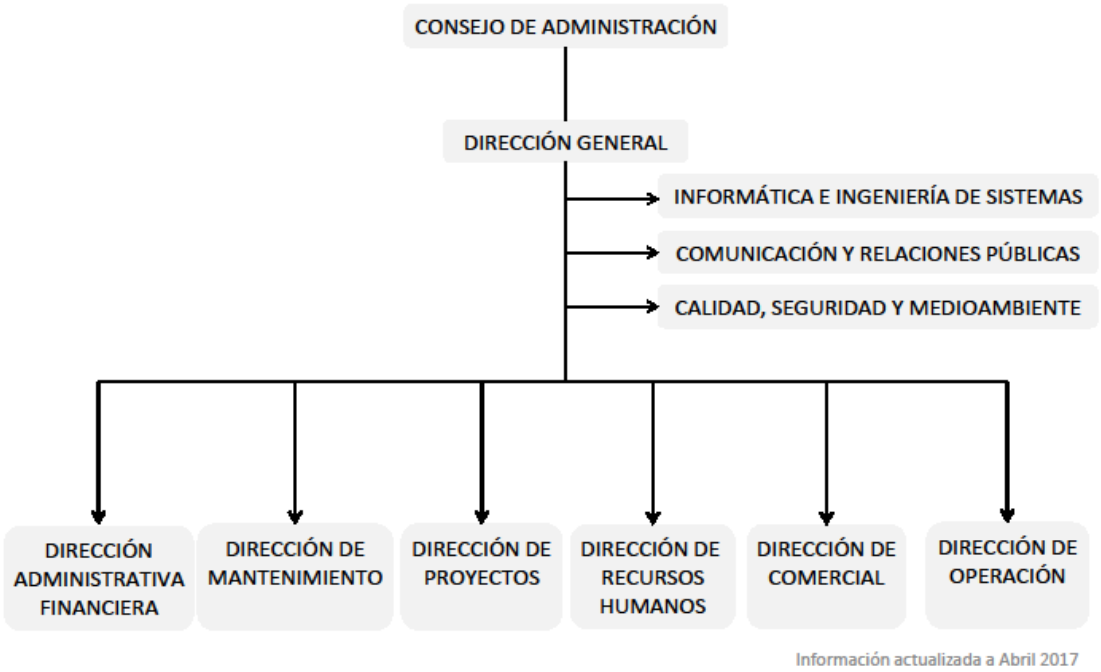
7 ORGANIZACIÓN DE LA SEGURIDAD

La gestión de la seguridad de la información implica la existencia de una estructura organizativa que, en consonancia con el ENS, defina unas responsabilidades diferenciadas en relación con los requisitos de la información, del servicio y de la seguridad.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información de Metrotenerife, son responsables de la seguridad de la información, así como de los recursos y medios puestos a su disposición para el manejo de dicha información. En ellos recae la responsabilidad de un uso correcto, siempre de acuerdo a las atribuciones profesionales y competencias.

Como extensión a la estructura de seguridad de Metrotenerife, se establecerán relaciones de cooperación en materia de seguridad con las autoridades competentes, autonómicas o estatales, proveedores de servicios informáticos o de comunicación, así como organismos públicos y privados dedicados a promover la seguridad de los sistemas de información.

Metrotenerife asocia la responsabilidad de los servicios, de la información, de la seguridad y del sistema con los directores y responsables de área directamente concernidos en el ámbito de aplicación del ENS y que se representan en el siguiente organigrama:



7.1 DEFINICIÓN DE ROLES DE SEGURIDAD

A continuación, se identifican los roles que participaran en la Seguridad de la Información de Metrotenerife:

Rol	**Funciones**
Dirección General	Es el órgano encargado de establecer la misión y los objetivos de Metrotenerife. Se ocupa del nombramiento de los componentes del Comité de Seguridad de la Información.
Comité de Seguridad de la Información	Es el órgano encargado de tomar decisiones que concretan cómo alcanzar los objetivos marcados por Metrotenerife.
Responsable de Seguridad	Funciona como supervisor de la operación del sistema y vehículo de reporte al Comité de Seguridad de la Información. Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de los servicios.
Responsable de la Información	Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por

	Metrotenerife y en qué condiciones debe llevarse a cabo su tratamiento.
Responsable del Servicio	Tiene la responsabilidad última de determinar los niveles de servicio aceptables y la seguridad que requiere la información manejada en su Servicio o área. Determinan los requisitos de seguridad de la información tratada y de los servicios prestados dentro de su Servicio o área.
Responsable del Sistema	A nivel operacional, toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.
Administradores de Seguridad	Implementa, ejecuta y mantiene las medidas de seguridad aplicables a los sistemas de información.
Delegado de Protección de Datos (DPD)	Persona o empresa encargada de asesorar a los Responsables en materia de seguridad (Dirección, Comité de Seguridad de la Información, Responsable de la Información, Responsable de Servicio, Responsable de Seguridad, Responsable del Sistema) acerca del cumplimiento de la normativa de protección de datos personales. Su nombramiento es obligatorio para Metrotenerife y sus funciones vienen recogidas en el RGPD.

7.2 PROCESO DE TOMA DE DECISIONES Y COORDINACIÓN

Los diferentes roles de seguridad de la información se articularán mediante la siguiente jerarquía: el Comité de Seguridad de la Información, dará instrucciones al Responsable de la Seguridad que se encargará de supervisar que el Responsable y administradores de sistemas implementan las medidas de seguridad según lo establecido en la Política de Seguridad de Metrotenerife.

El Responsable del Sistema:

- Informa al Responsable de la Información/Servicio de las incidencias funcionales relativas a la información que le compete.
- Informa al Responsable de la Información/Servicio de las incidencias funcionales relativas al servicio que le compete.
- Da cuenta al Responsable de la Seguridad en las siguientes materias:
    - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.

- Resumen consolidado de los incidentes de seguridad.
- Medidas de la eficacia de las medidas de protección que se deben implantar.

El Responsable de Seguridad:

- Informar al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Informar al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Da cuenta al Comité de Seguridad de la Información, como **secretario**:
  - Resumen consolidado de actuaciones en materia de seguridad.
  - Resumen consolidado de incidentes relativos a la seguridad de la información.
  - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

7.3 PROCESO DE DESIGNACIÓN Y RESOLUCIÓN DE CONFLICTOS

La Dirección General, nombrará formalmente y de conformidad con su régimen de funcionamiento interno:

- Al Responsable de Seguridad.
- Al Responsable de la Información.
- Al Responsable del Servicio.
- Al Responsable del Sistema.
- Al Administrador de Sistemas.
- Al Delegado de Protección de Datos.
- A los integrantes del Comité de Seguridad de la Información.

La resolución de conflictos entre los distintos roles y responsabilidades del sistema, así como las posibles incompatibilidades serán analizadas por el Comité de Seguridad de la Información, quien elevará su opinión a la Dirección General para la toma de decisiones.

7.4 DETALLE DE LOS ROLES

7.4.1 Dirección (Dirección General)

La función de dirección la desempeñará la Dirección General, que determina los objetivos a alcanzar y efectúa el seguimiento de su nivel de cumplimiento.

Le corresponde:

1. Designar los diferentes roles encargados de la gestión de la seguridad, así como los miembros del Comité de Seguridad de la Información
2. Fijar anualmente unos objetivos de nivel de riesgo aceptable. Los objetivos deben ser vigentes y estar alineados con el propósito y la estrategia de Metrotenerife, ser medibles o estimables y coherentes con las presentes directrices. El Comité de Seguridad de la Información apoyará a la Dirección General en la fijación y aprobación de estos objetivos y reportará anualmente la evolución de dichos objetivos.
3. Aprobar el Plan de Adecuación al ENS.
4. Aprobar la Política de Seguridad.
5. Aprobar, tras cada proceso de apreciación del riesgo que se realice, el Plan de Tratamiento del Riesgo que se elabore.
6. Proporcionar los recursos necesarios para el aseguramiento del cumplimiento de estos objetivos y para la operación del Sistema Integrado de Gestión.

7.4.2 Comité de Seguridad de la Información

El Comité de Seguridad de la Información de Metropolitano coordina la seguridad de la información. Los miembros del Comité actúan con voz y voto y sus acuerdos se adoptan por mayoría simple de sus miembros, salvo que se establezca alguna otra mayoría cualificada.

Composición:

El Comité de Seguridad de la Información está compuesto por los siguientes miembros:

Presidente	Gerente
Secretario	Responsable de Seguridad
Vocales	Dirección Financiera
	Dirección Comercial
	Área de Informática e Ingeniería de Sistema (IeIS)
	Delegado de Protección de Datos (DPD)

La Dirección General (Gerente) asume a nivel Organizativo, las funciones de Responsable de la Información y del Servicio, no obstante, dichas funciones son delegadas en cada uno de los directores de los diferentes departamentos.

Cada integrante del Comité actúa con voz y voto a excepción del Delegado de Protección de Datos (DPD) que no tendrá voto, y sus acuerdos se adoptan por mayoría simple de sus integrantes, salvo que se establezca alguna otra mayoría cualificada.

A requerimiento del Comité de Seguridad de la Información se convocará a cualesquiera otros responsables, propios o de terceras organizaciones subcontratadas para la prestación de los servicios, cuya intervención sea precisa por estar afectados por el ENS y por la regulación en materia de Protección de Datos.

Los miembros del Comité serán renovados cada cuatro años o con ocasión de vacante.

Funciones del Secretario:

- Convocar las reuniones del Comité de Seguridad de la información
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Funciones del Comité de Seguridad de la Información:

1. Atender las necesidades de la Dirección General y de los diferentes departamentos de la Organización.
2. Informar regularmente del estado de la seguridad de la información a la Dirección General.
3. Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
4. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la Organización en materia de seguridad.
5. Coordinar los esfuerzos de los diferentes departamentos para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
6. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
7. Elaborar y revisar regularmente la Política de Seguridad de la Información.
8. Elaborar la estrategia de evolución de Metrotenerife en lo que respecta a la seguridad de la información.
9. Aprobar en su caso la Declaración de Aplicabilidad, la categorización del sistema y el análisis de riesgos.
10. Aprobar la normativa y procedimientos de seguridad de la información que afecte al conjunto de la Organización.
11. Elaborar y aprobar los requisitos de formación y cualificación de técnicos y usuarios desde el punto de vista de seguridad de la información.

12. Aprobar planes de mejora de la seguridad de la información y coordinación de diferentes planes que puedan realizarse en diferentes departamentos.
13. Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
14. Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos, coordinando los diferentes departamentos de seguridad.

7.4.3 Responsable de Seguridad

El Responsable de Seguridad de la Información gestiona el proceso de seguridad de la información.

Funciones:

1. Elaborar y revisar la normativa de seguridad de la información, para su aprobación por el Comité de Seguridad de la Información.
2. Aprobar los Procedimientos de Seguridad de la Información
3. Coordinar y controlar las medidas de seguridad tanto técnicas como organizativas que apliquen en virtud de lo dispuesto por el RGPD y la normativa relacionada.
4. Coordinar la elaboración de la documentación de Seguridad del Sistema.
5. Promover la formación y concienciación en materia de seguridad de la información dentro de Metrotenerife. Elaborar los Planes de Formación y Concienciación del personal en Seguridad de la Información.
6. Recopilar los requisitos de seguridad de los Responsables de la Información y del Servicio y determinar la categoría del Sistema.
7. Realizar el Análisis de Riesgos.
8. Facilitar a los Responsables de la Información y del Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
9. Elaborar y en su caso aprobar la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
10. Elaborar, junto al Responsable del Sistema, planes de mejora de la seguridad y continuidad de sistemas, para su aprobación por el Comité de Seguridad de la Información.
11. Facilitar periódicamente al Comité de Seguridad de la Información un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).

7.4.4 Responsable del Servicio y de la Información

Funciones:

1. Determinar los niveles de seguridad de la información en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del ENS, previa propuesta de la persona Responsable de la Seguridad.
2. Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Aprobar el riesgo residual resultante de aplicar los controles de seguridad.
3. Supervisar el uso adecuado y la protección de la información y responder de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
4. Tiene la responsabilidad última del uso que se haga de determinados servicios/información y, por tanto, de su protección.
5. Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios/información. Aunque la aprobación formal de los niveles corresponda a la persona Responsable del Servicio o de la Información, se puede recabar una propuesta a la persona Responsable de la Seguridad y conviene que se escuche la opinión de la persona Responsable del Sistema.
6. Aprobar el riesgo residual (resultante una vez aplicados los controles de seguridad).
7. En cuanto a lo dispuesto en el RGPD y la normativa relacionada, por delegación de la persona Responsable del Tratamiento se encomienda a la persona Responsable del Servicio o de la Información el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su área en concreto.

7.4.5 *Responsable del Sistema*

El Responsable del Sistema de seguridad es la persona que toma las decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.

Funciones:

1. Elaborar y revisar los Procedimientos de Seguridad de la Información, así como, aprobar las Instrucciones Técnicas
2. Implementar, gestionar y mantener las medidas de seguridad que sean de aplicación a los sistemas de información.
3. Gestionar, mantener, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
4. Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.

5. Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de la actividad, de forma que ésta se ajuste a lo autorizado.
6. Proponer 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. La decisión de la suspensión debe ser acordada con el Responsable de Seguridad y con los Responsables del Servicio e Información antes de ser ejecutada.
7. Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
8. Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y pruebas.
9. Elaborar Procedimientos de Seguridad.
10. Establecer planes de contingencia y emergencia, llevando a cabo ejercicios que permitan su conocimiento por parte del personal de Metrotenerife.
11. Aplicar los procedimientos de seguridad aprobados, monitorizando el estado de seguridad e informando al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

7.4.6 *Administrador de seguridad*

La función de Administrador de seguridad en lo relativo a la implantación de las medidas de seguridad técnicas recae en el personal del Área de Informática e Ingeniería de Sistemas (dependiente de su responsable que es el Responsable del Sistema).

Funciones:

1. Elaborar y revisar las Instrucciones Técnicas.
2. Elaborar Procedimientos de Seguridad.
3. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
4. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
5. La gestión de las autorizaciones concedidas a los usuarios del sistema en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
6. La aplicación de los Procedimientos de Seguridad.
7. Aplicar los cambios de configuración del sistema de información.
8. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
9. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

10. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
11. Informar a los respectivos Responsables de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
12. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución

7.4.7 *Delegado de Protección de Datos (DPD)*

Siguiendo lo indicado en el RGPD y en la LOPDGDD, el Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben en relación al RGPD y otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros 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.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

8 DATOS DE CARÁCTER PERSONAL

Metrotenerife trata datos de carácter personal de acuerdo con el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018 cuyo objeto es adaptar al mismo el ordenamiento jurídico español y completar sus disposiciones.

La Organización sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

De este modo, con la LOPDGDD se han adaptado las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos. De este análisis de riesgos se pueden derivar medidas que se superpongan a las ya descritas como obligatorias para el ENS según la categorización del sistema.

9 ANÁLISIS Y GESTIÓN DE RIESGOS. INCLUSIÓN DE LOS RIESGOS CON DATOS PERSONALES

Todos los sistemas sujetos a la presente Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Responsable de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Conocer los riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para Metrotenerife, ya que únicamente si se conoce el estado de seguridad podrán tomarse las decisiones adecuadas para mitigar los riesgos a los que se enfrenta.

Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la LOPDGDD. El responsable o el encargado del tratamiento, asesorado por el Delegado de Protección de Datos, realizará un análisis de riesgos conforme al artículo 24 del RGPD y, en los supuestos de su artículo 35, una Evaluación de Impacto en la Protección de Datos (EIPD). Del resultado de ese análisis pueden derivarse medidas adicionales a implantar.

Metrotenerife utiliza la metodología ***Magerit*** para analizar los riesgos, realizando un análisis detallado de los riesgos que afecten a los activos recogidos en un inventario de activos, que queda documentado en un documento de Análisis de Riesgos.

La Organización determina los niveles de riesgo a partir de los cuales toma acciones de tratamiento sobre los mismos. Un Riesgo se considera aceptable cuando implementar más controles de seguridad se estima que consumiría más recursos que el posible impacto asociado.

Una vez llevado a cabo el proceso de evaluación de riesgos, la dirección de Metrotenerife es la responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

En el caso de las medidas implantadas en el ENS, si el análisis de riesgos establece medidas más importantes, se añadirán éstas a las descritas en el ENS.

10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

10.1 INSTRUMENTOS DE DESARROLLO Y GESTIÓN DE LA DOCUMENTACIÓN

Esta Política de Seguridad de la Información se desarrollará a través de los siguientes instrumentos:

- ***Normativa de seguridad (NOR)***: uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de las personas usuarias. Son de carácter obligatorio. La normativa de seguridad estará a disposición de cada integrante de Metrotenerife que necesite conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Esta normativa deberá ir firmada y avalada por la Presidencia del Comité de Seguridad de la Información.

- ***Procedimientos Técnicos de Seguridad (PRO)***: Afaontan tareas concretas, indicando lo que hay que hacer, paso a paso, sin entrar en detalles de proveedores, marcas comerciales o comandos técnicos. Son útiles en tareas repetitivas.

Al margen de estos instrumentos, podrán incorporarse guías informativas o instrucciones técnicas susceptibles de revisión por parte de la persona Responsable de Seguridad o el Comité de Seguridad de la Información y que se dirijan a aspectos concretos sobre la aplicación de medidas concretas sobre seguridad de la información.

10.2 ESTRUCTURA GENERAL

El desarrollo de la normativa de seguridad en su conjunto se llevará a cabo basándose en el análisis de riesgos y aspectos específicos de la Seguridad de la Información tales como las medidas de seguridad indicadas en el Anexo II del ENS:

- ***Marco organizativo***: orientado a administrar la seguridad de la información dentro de Metrotenerife. Partiendo de la presente Política de Seguridad de la Información se desarrollará el resto del marco normativo de seguridad.
- ***Marco operacional***: constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
  - ✓ ***Organización y Planificación***: mediante análisis de riesgos, controlando la arquitectura de seguridad y la adquisición de nuevos componentes entre otros aspectos.

- ✓ ***Control de Acceso***: orientado a controlar el acceso lógico a la información.
- ✓ ***Explotación***: medidas para la gestión de la seguridad en explotación; partiendo del inventario de activos y controlando la gestión de incidencias, cambios, gestión de la configuración, registros de actividad, entre otros.
- ✓ ***Servicios externos***: medidas de seguridad orientadas a garantizar que empresas y personas terceras que realicen servicios de cualquier clase contratados por Metrotenerife o que de alguna manera se presten bajo el control y/o la dirección de Metrotenerife cumplan las políticas y normas de seguridad de la información establecidas por parte de Metrotenerife.
- ✓ ***Continuidad del servicio***: acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.
- ✓ ***Monitorización del sistema***: orientado a garantizar la disponibilidad de las actividades diarias y proteger los procesos críticos de los efectos de fallas significativas o desastres.

- ***Medidas de protección***: para la protección de activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.
  - ✓ ***Protección de las instalaciones e infraestructuras***: destinado a impedir accesos no autorizados, daños e interferencias a las instalaciones e infraestructuras de Metrotenerife.
  - ✓ ***Gestión del personal***: orientado a reducir los riesgos de error humano o uso inadecuado de las instalaciones y equipamientos.
  - ✓ ***Protección de los equipos***: medidas para la protección de los equipos.
  - ✓ ***Protección de las comunicaciones***: dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y elementos y sistemas de comunicación.
  - ✓ ***Protección de los soportes de información***: para garantizar la información que contienen.
  - ✓ ***Protección de las aplicaciones informáticas***: orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.
  - ✓ ***Protección de la información***: cumpliendo lo dispuesto en el RGPD y en la LOPDGDD.
  - ✓ ***Calificación de la Información:*** estableciendo los requisitos, tipos y flujos de información que se producen, así como los procesos de elaboración, aprobación y acceso a la documentación.
  - ✓ ***Protección de los servicios***: definiendo las medidas necesarias para mantener la seguridad de los servicios TI.

10.3 GESTIÓN DE LA DOCUMENTACIÓN

La gestión de la documentación relacionada con la seguridad de la información tendrá en cuenta el ciclo de vida de la misma (generación, aprobación, modificación), de modo que se establezcan distintas responsabilidades en cada fase del ciclo de vida.

En este sentido, la gestión de la documentación contará con los siguientes roles relacionados:

- Dirección General (Dirección)
- Comité de Seguridad de la Información (CSI)
- Responsable de Seguridad de la Información (RSI)
- Responsable del Sistema (RS)
- Administrador de Seguridad (AS)
- Usuarios (US)

De acuerdo a lo anterior, en función del tipo de documento y el ciclo de vida, se ha establecido la siguiente matriz:

	Generación	**Aprobación**	**Modificación**
Políticas	CSI	Dirección	CSI
Normativas	RSI	CSI	RSI
Procedimientos	RS	CSI - RSI	RS
Instrucciones	AS	RS	AS

10.4 SANCIONES PREVISTAS POR INCUMPLIMIENTO

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características de los preceptos incumplidos.

El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

11 SEGURIDAD DE LA INFORMACIÓN

Se dispondrá un sistema de etiquetado o nombrado para los documentos, de manera que el destinatario de la información pueda conocer el tipo de información que contiene el documento, departamento o área a la que pertenece, categoría de información que contiene, existencia de datos personales o cualquier otra información que resulte relevante en materia de datos personales.

11.1 CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información que obra en los sistemas de información responsabilidad de Metrotenerife deberá contar con medidas de seguridad, de acuerdo con lo previsto en el ENS, que garanticen la protección respecto a todas las dimensiones de la seguridad. Estas medidas de seguridad se establecerán de acuerdo a unos criterios basados en el acceso a la información, su difusión y la materia que aborden.

En este sentido, se ha establecido un cuadro de calificación de documentos, que se indica a continuación, basado en los siguientes criterios, sin perjuicio de su desarrollo a través de la normativa o procedimientos técnicos pertinentes:

- (R) Requisitos legales, como los derivados de la normativa sobre secretos oficiales.
- (D) Difusión de la información, esto es, las personas autorizadas para acceder a la información.

R	*D*	*Descripción*	*Ejemplos*
	Pública	Información de difusión no controlada para el público general. Apto para difusión entre todo tipo de organismos y entidades. La información no es confidencial y puede ser hecha pública sin ninguna implicación para Metrotenerife. La pérdida de la disponibilidad debido al tiempo de inactividad del sistema es un riesgo aceptable. La integridad es importante pero no vital.	• Catálogos de servicios ampliamente distribuidos. • La información disponible en el dominio público, incluyendo áreas de acceso público del sitio web. • Descargas de software de Metrotenerife. • Información publicada al amparo de la normativa de Transparencia o aquella originada por obligación legal y siguiendo los principios de la normativa de protección de datos.

R	D	Descripción	Ejemplos
Uso oficial	***Interna***	Documento de difusión parcialmente controlada no apto para su difusión pública y protegido del acceso externo. Su uso se restringe únicamente al personal interno y entidades colaboradoras. Para acceder internamente a esta información hace falta un permiso explicito por parte de un superior. El acceso no autorizado podría influenciar la eficacia operacional de Metrotenerife y causar un importante daño. La integridad de la información es vital. Estará dirigida a los usuarios internos, así como responsables, comités y dirección.	• La información sobre los procedimientos de seguridad de Metrotenerife. • Información interna de los departamentos de Metrotenerife. • Procedimientos normalizados de trabajo utilizados en todas las áreas. • Todo el código y aplicaciones, así como portales web desarrollados por y para Metrotenerife.
	Confidencial	Información especialmente sensible para Metrotenerife. Su acceso está restringido únicamente a aquellos empleados que necesiten conocerla para desempeñar sus funciones. Se entenderá dentro de esta clasificación la información recopilada y utilizada por Metrotenerife en la contratación de personas, prestación de servicios a los ciudadanos o gestión de las finanzas. El acceso a esta información debe ser muy	• La información sobre los procedimientos de seguridad de Metrotenerife. • Datos internos de contabilidad e informes financieros. • Acuerdos privados con los proveedores. • Planes futuros de Metrotenerife. • Contraseñas. • Información interna de los

R	D	Descripción	Ejemplos
		restringido dentro de la Organización.	departamentos de Metrotenerife. • Resoluciones de concursos. • Datos económicos y otros datos personales de empleados o ciudadanos. • Información con datos de origen étnico o racial, las opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos, salud, vida sexual, orientación sexual o condenas e infracciones penales.

Toda la documentación, digital o impresa, debe indicar la clasificación de la información que contiene, salvo la información catalogada como pública.

Para dicha clasificación se definirá un Procedimiento de Clasificación de la Documentación. La clasificación de la información debe tener en cuenta las consecuencias que se derivarían de su conocimiento por personas que no deben tener acceso a ella.

12 OBLIGACIONES DEL PERSONAL

Todos los miembros de Metrotenerife tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información.

Así mismo, deberán conocer la Normativa de Seguridad que la desarrolla en la medida que les sea de aplicación en el desempeño de sus cometidos.

El Comité de Seguridad de la Información dispondrá los medios necesarios para que tanto la Política como la Normativa lleguen a los destinatarios concernidos.

Para ello, además de que la política esté disponible en los sistemas de información de Metrotenerife, 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.

Así mismo, se establecerá un programa de concienciación continua para atender a todos los miembros de la Organización, en particular a los de nueva incorporación.

Las personas con responsabilidad 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 recomendada antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

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 a Metrotenerife cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

14 TERCERAS PARTES

Cuando Metrotenerife utilice servicios o ceda información de/a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que afecte a dichos servicios o información. La 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 esta Política. De igual modo deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el ENS cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el ENS, cuando se trate de sistemas de categorías MEDIA o ALTA, en los servicios concernidos.

Cuando Metrotenerife preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable del Sistema que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la

aprobación de este informe por el Comité de Seguridad de la Información antes de seguir adelante.

14.1 TERCERAS PARTES COMO SERVICIOS EXTERNALIZADOS DE SEGURIDAD

En el caso de servicios externalizados de seguridad, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma.

15 AUTORIZACIÓN Y CONTROL DE ACCESO

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 de la Información y del Servicio correspondiente.

Los Responsables de la Información y del Servicio 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.

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 Metrotenerife 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 si 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 de la Información y del Servicio 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.

17 ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS 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 Metrotenerife y en la contratación de servicios de seguridad, 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. Estos requerimientos se extenderán también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

18 MÍNIMO PRIVILEGIO

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

El sistema proporcionará la funcionalidad imprescindible para que Metrotenerife alcance sus objetivos competenciales o contractuales.

Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o 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.

Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

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 Metrotenerife 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 PROTECCIÓN DE 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 REGISTRO DE LA ACTIVIDAD Y DE CÓDIGO DAÑINO

Con la finalidad exclusiva de lograr el cumplimiento del objeto del ENS, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para

monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá 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 una determinada actividad.

23 INCIDENTES DE SEGURIDAD

Metrotenerife 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.

Metrotenerife contará con procedimientos de comunicación de los incidentes de seguridad de forma que en los casos de impacto significativos se pondrán en conocimiento del Centro Criptológico Nacional.

En el caso de los incidentes que afecten a datos de carácter personal, se tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el ENS. De manera que se evaluarán las Brechas de seguridad y se tratarán de manera adecuada, incluyendo su comunicación tanto a la Agencia Española de Protección de Datos como a los posibles afectados en caso de ser necesario.

24 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.

25 DESARROLLO DEL SGSI, REVISIÓN Y AUDITORÍAS

La dirección ha aprobado el desarrollo de un sistema de gestión de seguridad de la información (SGSI) que es establecido, implementado, mantenido y mejorado conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del ENS. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados. Existe un procedimiento de gestión documental que establece las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La Política y las Normas de Seguridad de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas del ENS, prestando especial atención a las guías publicadas por el Centro Criptológico Nacional como desarrollo de las medidas y controles de seguridad.

Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en el Documento de Aplicabilidad, y serán proporcionales a la criticidad de la información a proteger y a su clasificación.

El Comité de Seguridad de la Información revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la dirección. Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios tecnológicos y de negocio.

La dirección será responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en el presente documento.

El sistema de gestión de seguridad se auditará cada dos años, según un plan de auditorías desarrollado por el Comité de Seguridad de la Información.