Índice de Contenidos

Fecha	Edición.Revisión	Cambios Realizados
14-01-2021	0.1	Borrador inicial del documento
15-11-2021	1.0	Revisión con CIT y versión definitiva
04-01-2023	1.1	Actualización referencias nuevo ENS (RD 311/2023)
18-07-2023	1.2	Cambio de alcance de Ayuntamientos a Entidades

1 Introducción

1.1 Justificación de la Política de Seguridad

Las Administraciones Públicas dependen de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos como Organización. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, 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. Es por ello que el Esquema Nacional de Seguridad (ENS, en adelante), operado por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su artículo 12 establece que "*Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente*".

Trasladando esta exigencia al marco de las Entidades, esto implica que las diferentes áreas de las Entidades deben aplicar las medidas mínimas de seguridad exigidas por el 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.

Todas las áreas deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, 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 planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC. Las áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al ENS.

1.2 Principios básicos

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- 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 iniciativas estratégicas de las Entidades para conformar un todo coherente y eficaz.
- Responsabilidad diferenciada: En los sistemas TIC se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. 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, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

- 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.
- 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. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

1.3 Objetivos de la Seguridad

Las Entidades establecen como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información de las Entidades se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de las Entidades.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.
- Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.

- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

2 Alcance

Esta política de seguridad aplica a todos los sistemas de información de las Entidades adheridas al Marco de Gobernanza Insular de Seguridad de la Información, promovido y soportado desde el Cabildo Insular de Tenerife, contemplando tanto los **servicios comunes**, que el Cabildo pueda poner a disposición de las Entidades, como los **servicios propios** que existan en cada Entidad.

Las Entidades 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 las diferentes entidades en cualquiera de sus formas y formatos. Aplica con independencia de cuál sea la relación o adscripción con el mismo.

3 Misión y servicios prestados

Las Entidades, 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.

Las Entidades desean 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 las Entidades, creando la confianza necesaria entre ciudadano y las Entidades en esa relación.
- Reducir los tiempos de tramitación.
- Reducir las cargas administrativas.
- Hacer transparente la actividad de las Entidades.
- Fomentar la participación y colaboración.

4 Marco normativo

- El marco legal en materia de seguridad de la información en que se desarrollan las actividades de las Entidades en el ámbito de la prestación de los servicios electrónicos a los beneficiarios viene establecido en el documento **NOR-000 Legislación y Normativa aplicable**.

5 Organización de la seguridad

5.1 Definición de roles

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 las Entidades.

La guía CCN-STIC 801 establece para la gobernanza de la seguridad tres grandes bloques de responsabilidad:

- La **responsabilidad legal** y la **especificación de necesidades**, que corresponde a la **Dirección** y a los **responsables del tratamiento, de la información y del servicio**.
- La **supervisión**, que corresponde al **Responsable de la Seguridad y al Delegado de Protección de Datos**, en sus respectivos ámbitos.
- La **operación** del sistema de información, que corresponde al **Responsable del Sistema**.

Partiendo de estos bloques de responsabilidad, esta guía propone un **modelo de referencia** basado en **tres niveles**: Nivel de **Gobierno**, Nivel **Ejecutivo y Supervisión** y Nivel **Operacional** (ver figura 1).

Figura 1. Niveles de la estructura de seguridad (fuente: Guía CCN-STIC 801)

En base a lo anterior, el Marco de Gobernanza Insular de la Seguridad de la Información propuesto se ha estructurado en torno a estos tres niveles y las funciones generales identificadas.

5.2 Estructura de gobernanza

En base al modelo indicado en el apartado anterior, y considerando la realidad y situación actual de la Isla de Tenerife, se ha propuesto un Marco de Gobernanza Insular de la Seguridad de la Información, que se desarrolla en los siguientes apartados, con las siguientes características generales:

- Se estructura en los niveles previstos en la CCN-STIC 801.
- El Nivel de Gobierno se distribuye entre la Comisión de Modernización Insular (CMI), como órgano político de dirección y estrategia ya existente, y el Comité de Seguridad Insular (CSI), como órgano ejecutivo de aprobación y supervisión en el ámbito concreto de la seguridad de la información.
- Se gradúan las responsabilidades en función de que se trate de servicios comunes o propios en las Entidades.
- Se gradúa la participación/responsabilidad de las Entidades en función de su dimensión y por tanto de las capacidades y recursos que dispongan.
- Se plantea una nueva figura de Responsable de Seguridad Insular, centralizado en el Cabildo de Tenerife y con responsabilidad sobre los sistemas propios de las Entidades pequeñas y con menor capacidad.
- Se integra con la protección de datos al incorporar la figura también centralizada en el Cabildo de Tenerife del Delegado de Protección de Datos de las Entidades.

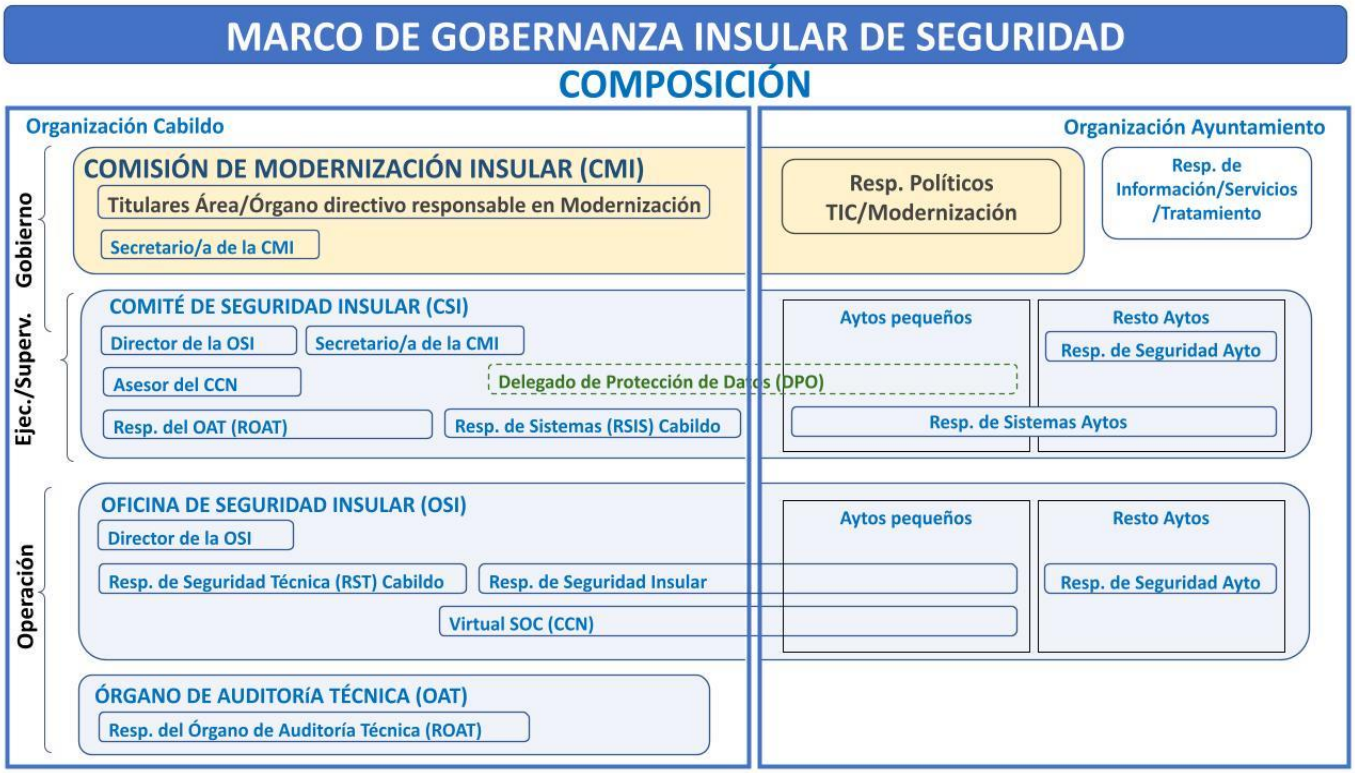

Figura 2. Marco de gobernanza insular de la seguridad (fuente: elaboración propia)

5.2.1 Nivel de Gobierno

Comisión de Modernización Insular (CMI)

Es el **órgano colegiado** regulado en el artículo 25 del Reglamento de Asistencia Integral a los Municipios, aprobado de forma definitiva en la sesión del 1 de marzo de 2021 del Pleno del Cabildo Insular de Tenerife, y que asumirá entre otras funciones con respecto a la asistencia técnica en materia de modernización administrativa que el Cabildo de Tenerife presta a las Entidaddes de la Isla de Tenerife, el gobierno de la seguridad de la información, asumiendo las **competencias directivas y estratégicas** necesarias.

Miembros

- **Presidente**: la persona titular del área competente en materia de modernización administrativa del Cabildo Insular de Tenerife.
- **Vicepresidente**: la persona titular del órgano directivo competente en materia de modernización administrativa del Cabildo Insular de Tenerife.
- **Vocales**: un vocal por cada uno de los municipios de la Isla, que deberá ser el responsable político con competencias en materia de implantación de tecnología de la información y de las comunicaciones, administración electrónica y/o modernización en la Corporación respectiva, o persona en quien delegue.
- **Secretario/a**: un funcionario designado por la persona titular del área competente en materia de modernización administrativa del Cabildo Insular de Tenerife

Funciones

- Elaborar la estrategia de evolución de las Entidades en lo que respecta a la seguridad de la información.

- Coordinar los esfuerzos en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Conocer e informar regularmente del estado de la Seguridad de la Información a los máximos responsables de cada entidad.
- Resolver los conflictos de responsabilidad que puedan aparecer en todo el modelo.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios comunes que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de las Entidades en materia de seguridad de la Información, conociendo los resultados y definiendo la estrategia necesaria para su mejora.
- Liderar, coordinar y velar por el correcto desarrollo de los proyectos de adecuación al ENS que se impulsen en las Entidades adheridas al marco de gobernanza insular, adoptando las medidas que correspondan, de acuerdo a los fines establecidos en el mismo.
- Alentar los procesos de Certificación de la Conformidad con el ENS para tanto los servicios comunes prestados a las Entidades, como los propios.
- Conocer, y reorientar si se estimase necesario, la aprobación por el CSI de los niveles de seguridad de la información, niveles de seguridad de los servicios y de la Política de Seguridad conjunta.

5.2.2 Nivel Ejecutivo/Supervisión

Comité de Seguridad Insular (CSI)

Se trata de un **grupo de trabajo** que se constituye para dar respuesta a las exigencias de seguridad de la información derivadas de la Adecuación al Esquema Nacional de Seguridad (ENS, RD 311/2022, de 5 de mayo) desde el punto de vista ejecutivo y de supervisión.

Miembros

Permanentes:

- Vocales:
  - **Director de la Oficina de Seguridad Insular (OSI)**, también asumirá el cargo de Secretario del CSI.
  - **Secretario/a** de la CMI.
  - **Resp. de Seguridad de Entidad (RSE)**: un máximo de 3 representantes (rotario en cada sesión según orden de población atendida, empezando por los de menor población).
  - **Resp. de Sistemas (RSIS) del Cabildo de Tenerife**.
  - **Resp. de Sistemas de las Entidades**: un máximo de 3 representantes (rotario en cada sesión según orden de población atendida, empezando por los de menor población).
  - **Resp. del Órgano de Auditoría Técnica (ROAT)**.
- Asesores: con voz pero sin voto
  - **Asesor del Centro Criptológico Nacional (CCN)**.

No permanentes:

- **Delegado de Protección de Datos**: cuando se traten temas asociados a la protección de datos de carácter personal y con responsabilidad sobre los servicios comunes y los servicios propios de las Entidades.
- **Especialistas externos o internos**: de los sectores público, privado y/o académico, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Funciones

- Aprobar, y mantener actualizada, la Política de Seguridad de la Información.
- Proponer para su análisis o revisión y, en su caso, aprobar y publicar Normas, Procedimientos, Criterios o Buenas Prácticas en materia de Seguridad y Adecuación al ENS y Certificación de su Conformidad.
- Asesorar a las Entidades en materia de seguridad de la información y en la adecuación normativa al ENS, respecto de los métodos, procedimientos, herramientas y criterios en materia de Certificación de su Conformidad y, en general, con su implantación, orientando su gestión al mejor servicio del sector público.
- Informar a la CMI de la aprobación y/o modificación de los niveles de seguridad de la información, niveles de seguridad de los servicios y de la Política de Seguridad conjunta.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección, remitiendo para ello la información a la CMI. También se encargará de la remisión de información a las organizaciones públicas y privadas que corresponda sobre el grado de implantación de la Certificación de Conformidad con el ENS.
- Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
- Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.
- Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, para que sean elevadas a la CMI.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información.
- Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Identificar y diseñar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información en todas las Entidades.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre sus miembros, elevando si fuese necesario el asunto a la CMI.
- Velar por la coordinación de las diferentes áreas de seguridad.
- Delegadas de los responsables de Información:
    - Establecer los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
    - Determinar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
    - Aprobación formal de los niveles de seguridad de la información.

- Delegadas de los responsables de Servicios:
    - 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.
    - Aprobación formal de los requisitos de los servicios en materia de seguridad.
    - Aprobar el riesgo residual (el resultante una vez aplicados los controles de seguridad).

5.2.3 Nivel Operativo

Oficina de Seguridad Insular (OSI)

Grupo de trabajo de naturaleza técnica y carácter permanente, que se establece como elemento operativo de la seguridad de la información.

Miembros

Permanentes:

- **Director de la OSI**: Responsable en el Cabildo de Tenerife del proyecto de asistencia técnica de la seguridad informática para las Entidades.
- **Resp. de Seguridad Técnica (RST) del Cabildo de Tenerife**.
- **Resp. de Seguridad Insular (RSIN)**.
- **Resp. de Seguridad de Entidad (RSE)**.
- **Equipo vSOC (CCN)**: Jefe de Proyecto y técnicos del Virtual SOC designados por el CCN.

No permanentes:

- **Resp. de Sistemas (RSIS) del Cabildo**.

Funciones

- Redactar o actualizar Normas, Procedimientos, Criterios o Buenas Prácticas en materia de Seguridad y Adecuación al ENS y Certificación de su Conformidad, proponiendo su aprobación al CSI.
- Realización de análisis de riesgos.
- Monitorizar los principales riesgos residuales asumidos por las Entidades y recomendar al CSI posibles actuaciones respecto de ellos
- Seguridad en las interconexiones y conectividad.
- Vigilancia y determinación de superficie de exposición.
- Monitorización y gestión de incidentes.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos al CSI.
- Observatorio digital y cibervigilancia.
- Otras funciones conexas o concordantes.
- Análisis y debate de las cuestiones relacionadas con la seguridad de los sistemas de información de las Entidades que hubieren sido presentadas por los Responsables de las Entidades.
- Mantener informado al CSI del resumen del estado, así como actuaciones e incidentes relevantes.
- Redacción y presentación de propuestas al CSI.
- Para las Entidades adheridas al Marco de menos de 20.000 habitantes atendidas, y a través del vSOC:
    - La gestión operativa de los servicios comunes de seguridad de las Entidades adheridas al marco, su explotación y mantenimiento.

- 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.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Órgano de Auditoría Técnica

Se constituye como el **elemento de verificación y conformidad** de las Entidades adheridas al marco. Se implementará a través de un **servicio externalizado** de naturaleza técnica especializada y reconocida según los criterios establecidos por el CCN-CERT.

Miembros

- **Resp. del Órgano de Auditoría Técnica (ROAT)**.
- **Equipo de auditores técnicos**.

Funciones

- Verificación de las medidas técnicas de seguridad adoptadas en las Entidades.
- La gestión de la emisión de la certificación de conformidad correspondiente.
- La inspección documental del marco normativo y otras tareas relacionadas con la conformidad al marco normativo.
- Realización de auditorías de seguridad y de conformidad con el ENS de los sistemas de información tanto comunes del Cabildo como propios en las Entidades.

5.3 Roles de seguridad

5.3.1 Responsables de la Información/Servicio/Tratamiento

Ámbito:

- Se tratará de una o varias figuras nombradas en cada Entidad.
- Las funciones más técnicas y específicas previstas en el ENS para este rol se han trasladado al CSI, quedando en esta figura solamente aquellas funciones que por ámbito competencial se entiende indelegables.

Funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- En cuanto a lo dispuesto en el RGPD, por delegación del Responsable del Fichero se le encomienda el desarrollo de las tareas relacionadas con la gestión de los ficheros y tratamientos de datos personales que se realizan en su área en concreto, lo cual deberá realizar en coordinación con el Delegado de Protección de Datos.

5.3.2 Responsables de Seguridad

Ámbitos

- **Resp. de Seguridad Técnica (RST) del Cabildo de Tenerife**: ejercerá las funciones de responsable de seguridad sobre los servicios comunes que presta el Cabildo de Tenerife a las Entidades.
- **Resp. de Seguridad Insular (RSIN)**: ejercerá las funciones de responsable de seguridad sobre los servicios propios de las Entidades de menos de 20.000 habitantes atendidas.
- **Resp. de Seguridad de Entidad (RSE)**: ejercerá las funciones de responsable de seguridad sobre los servicios propios en las Entidades de 20.000 o más habitantes atendidas y será designado por la propia Entidad.

Funciones

Dentro de su ámbito de actuación:

- Política, Normativa y Procedimientos
  - Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política y Normativa de Seguridad de la Información, para su aprobación por el CSI.
  - Elaborará los Procedimientos Operativos de Seguridad de la Información para su aprobación por el CSI.
- Formación y concienciación
  - Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
  - Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el CSI.
- Gestión de la Seguridad
  - Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de las Entidades.
  - Proporcionar asesoramiento para la determinación de la categoría del sistema contando con la colaboración de la OSI. Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.
  - Participar dentro de la Oficina de Seguridad en la ejecución del análisis de riesgos, de la declaración de aplicabilidad; identificar medidas de seguridad; determinar configuraciones necesarias; elaborar documentación.
  - Facilitará a los Responsable de Información y a los Responsables de Servicio información, así como al propio CSI, 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.
  - Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
  - Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el CSI.
  - Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el CSI y probados periódicamente por el Responsable de Sistemas.
  - Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
  - Participar en el análisis, diseño y toma de decisiones y propuesta de mejoras en los servicios comunes.
  - Gestionar las revisiones externas o internas del sistema.

    - Apoyar la gestión de incidentes de seguridad y la actividad de la OSI
    - Coordinar y apoyar los procesos de certificación con el soporte de la OAT.
- CSI.
    - Facilitará periódicamente al CSI 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).

5.3.3 Responsable de Sistemas

Ámbitos

- **Resp. de Sistemas (RSIS) del Cabildo de Tenerife**: tendrá responsabilidad sobre los servicios comunes que presta el Cabildo de Tenerife a las Entidades.
- **Resp. de Sistemas de las Entidades**: tendrán responsabilidad sobre los sistemas propios de cada Entidad.

Funciones

En los sistemas bajo su responsabilidad:

- Prestar al Responsable de Seguridad y/o el CSI asesoramiento para la determinación de la Categoría del Sistema
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado, salvo los que sean realizados de forma centralidad desde la OSI.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Gestionar el Sistema
    - Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
    - Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
    - Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Establecer directrices y medidas
    - Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
    - Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
    - Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
    - Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.

    - Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Elaborar y aplicar
    - Elaborar procedimientos operativos de seguridad.
    - Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Aprobar
    - Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
    - Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Monitorizar
    - Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.

5.3.4 Administrador de la Seguridad

Ámbitos

- **Oficina de Seguridad Insular (virtual SOC)**: asumirá las funciones de este rol, a través del virtual SOC, sobre los servicios comunes que presta el Cabildo de Tenerife a las Entidades.
- **Resp. de Sistemas de las Entidades**: tendrán la responsabilidad de este rol sobre los sistemas propios de cada Entidad.

Funciones

- Implementar, gestionar y mantener la seguridad
    - La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
    - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    - Informar a los Responsables de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
    - Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- Gestión, configuración y actualización
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - 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.
- Gestión de las autorizaciones
    - 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.
- Monitorizar la seguridad
    - 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.

6 Datos de carácter personal

Las Entidades tratan 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 de las Entidades 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.

7 Gestión de riesgos

7.1 Justificación

Todos los sistemas sujetos a esta Política deberán someterse a 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.

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 en 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.

7.2 Criterios de evaluación de riesgos

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

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará las Entidades, basándose 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 las Entidades de forma grave.

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

7.3 Proceso de aceptación del riesgo residual

Los riesgos residuales serán **determinados por el Responsable de Seguridad de la Información.**

Los niveles de Riesgo residuales esperados sobre cada Información 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 de esa Información.

Los niveles de Riesgo residuales esperados 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 de ese Servicio.

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

8 Gestión de incidentes de seguridad

8.1 Prevención de incidentes

Los Departamentos o unidades de las Entidades 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. El ENS a través de su artículo 19 establece la que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. De igual forma, el artículo 17 del citado ENS define que los sistemas de instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Para ello las áreas deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los Departamentos o unidades deben:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

8.2 Monitorización y detección de incidentes

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de las Entidades, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.

8.3 Respuesta ante incidentes

Se deberá:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos 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) que resulten de aplicación, en su caso.

9 Obligaciones del personal

Los miembros de las Entidades tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de las Entidades atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a los miembros de las Entidades, 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 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 responsabilidades en el mismo.

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos las Entidades, constituyendo su incumplimiento infracción grave a efectos laborales.

10 Terceras partes

Cuando se presten servicios o se gestione información de otras organizaciones, 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 se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad 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 esta Política.

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 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.

11 Revisión y aprobación de la Política de Seguridad

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 11 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

12 Estructura y desarrollo de la Política de Seguridad

La estructura jerárquica de la documentación de seguridad es 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 en la herramienta AMPARO proporcionada por CCN • Disponible en la intranet de la Entidad o a través de la web del MGISI del Cabildo de Tenerife
Normativa	• Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. • Es de carácter obligatorio.	• Disponible en la herramienta AMPARO proporcionada por CCN • Disponible en la intranet de la Entidad o a través de la web del MGISI del Cabildo de Tenerife
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	• Disponible en la herramienta AMPARO proporcionada por CCN • Disponible en la intranet de la Entidad o a través de la web del MGISI del Cabildo de Tenerife

Documento	Detalle	Ubicación
	otros procedimientos o con instrucciones técnicas de seguridad.	
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 importantes de seguridad que pueden materializarse de varias formas.	• Disponible en la intranet de la Entidad o a través de la web del MGISI del Cabildo de Tenerife
Registros	• Registro de actividad de la aplicación de los documentos anteriores que muestran la evidencia de su implantación y desarrollo en las Entidades	• Disponible los registros manuales en la herramienta AMPARO • Disponibles en las herramientas de gestión de los sistemas automatizados

En la guía CCN-STIC-801 Responsabilidades y Funciones, se detalla el esquema de las principales responsabilidades (quien debe elaborarlo y quién aprobarlo) para cada uno de estos documentos.

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.