Área de Presidencia, Hacienda y Modernización
Dirección Insular de Modernización

Fecha: 21/12/2020 **Teléfono:** 922 84 34 23
Referencia: CBP

Asunto: Marco de Gobernanza Insular de Seguridad de la Información

Marco de Gobernanza Insular de Seguridad de la Información para la Isla de Tenerife

Objeto

El presente documento tiene por objeto la definición de un marco de gobernanza conjunto a nivel insular, entre el Cabildo y los Ayuntamientos de la Isla de Tenerife que se adhieran al mismo, para la gestión de la seguridad de la información, teniendo en consideración los recursos, ámbitos de actuación y responsabilidades de cada entidad, y con el objetivo de dar una **respuesta de la forma más eficiente y eficaz** posible, tanto a nivel de las exigencias derivadas de la **adecuación a las normativas** de seguridad de la información y protección de datos vigentes, como a nivel de **protección ante incidentes de seguridad**.

Alcance

El presente marco se ha diseñado con las siguientes características:

- **Conjunto:** organización y documentación común con aplicación sobre todos los ayuntamientos: planes de adecuación, política de seguridad, normativas, procedimientos, medidas, instrucciones, etc.
- **Asistido**: se dispondrá del soporte del Cabildo, designando roles centralizados en el Cabildo para el apoyo a los ayuntamientos con menos recursos, ampliando al ámbito del Esquema Nacional de Seguridad (ENS), la estrategia de asistencia ya puesta en marcha en el 2018, en el ámbito del Reglamento General de Protección de Datos (RGPD), en la que se estableció la figura centralizada del Delegado de Protección de Datos (DPO) municipal).
- **Insular**: se dirige principalmente a los ayuntamientos con menos recursos, ofreciéndoles una asistencia más extensa, sin embargo, también es posible la incorporación del resto de municipios, aunque con un apoyo más limitado en proporción a sus recursos.
- **Horizontal**: se contempla en el modelo tanto la adecuación normativa de los servicios comunes, que el Cabildo pueda poner a disposición de los ayuntamientos, como los servicios propios/específicos de cada ayuntamiento.
- **Integral**: incorpora todos los niveles de gestión de la seguridad necesarios: Gobierno (dirección y estrategia), Ejecutivo y supervisión (aprobación) y Operación, a través de la creación y apoyo en los órganos, grupos de trabajo y roles necesarios.

Calle Clavel, 2
38003 Santa Cruz de Tenerife
Tfno.: 922 239 999
Fax: 922 239 468
www.tenerife.es

En cualquier caso, lo indicado en el presente documento **aplicará solamente a los ayuntamientos que se adhieran efectivamente al marco propuesto**, a través del correspondiente proyecto, dentro del anual en el que se incluya, aceptando los términos y condiciones que se establezcan de forma específica.

En concreto, la ejecución del presente marco arranca dentro del plan anual 2021 (https://transparencia.tenerife.es/archivos/110/documento-plan-37-11-02-2021-plan-de-proyectos-2021-7187.pdf), en el que se ha incorporado el proyecto **P21.3B. Marco de gobernanza insular de seguridad de la información**, con una duración de **2 años**, y al que han solicitado adhesión los siguientes 23 ayuntamientos:

- **Prioridad 1 (<20.000 hab)**: Arafo, Arico, Buenavista del Norte, El Rosario, El Sauzal, El Tanque, Fasnia, Garachico, La Matanza de Acentejo, La Victoria de Acentejo, Los Silos, San Juan de la Rambla, Santa Úrsula, Santiago del Teide, Tegueste y Vilaflor de Chasna.
- **Prioridad 2 (entre 20.000 y 30.000 hab.)**: Candelaria, Guía de Isora, Güímar e Icod de los Vinos.
- **Prioridad 3 (más de 30.000 hab.)**: Granadilla de Abona, Puerto de la Cruz y San Cristóbal de La Laguna.

Antecedentes

El marco que se establece se ha diseñado en base a las siguientes iniciativas/propuestas de referencia:

- **Marco de referencia para el Gobierno de la Seguridad**: establecido en la guía **CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones**, emitida por el Centro Criptológico Nacional (CCN), a través del CCN-CERT, para el gobierno de la seguridad de la información en las entidades del sector público, basado en niveles y con distintas formas de implementación.
- **Marco de certificación del ENS para EELL**: es el modelo propuesto por el CCN para facilitar el cumplimiento normativo con el Esquema Nacional de Seguridad (ENS) de los ayuntamientos con menos recursos, a través de un marco común liderado y asistido desde los Cabildos/Diputaciones.
- **Reglamento de Asistencia Integral a los Municipios**: es la nueva normativa (https://transparencia.tenerife.es/archivos/105/informe-15-29-12-2020-3097.pdf) que en el ámbito del Cabildo y los Ayuntamientos de la Isla de Tenerife, establece entre otras cosas; el marco general de asistencia a los municipios, y en concreto, la estrategia, la forma de gestionar y la organización asociada al gobierno del servicio de asistencia técnica en modernización administrativa a nivel insular, en donde se encuentra incluida la asistencia prevista.

Estos instrumentos, que se describen en los siguientes apartados, han servido de base para el diseño del marco de gobernanza insular propuesto, realizando las adaptaciones necesarias para hacerlo compatible con la situación actual, del Cabildo y ayuntamientos de la Isla de Tenerife, y el alcance previsto.

Marco de referencia para el Gobierno de la seguridad

La guía **CCN-STIC 801** establece para la gobernanza de la seguridad la necesidad de definir y establecer 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, esta guía propone un **modelo de referencia** basado en **tres niveles** (ver figura 1):

- Nivel de **Gobierno**
- Nivel **Ejecutivo y Supervisión**
- Nivel **Operacional**

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

En base a lo anterior, el presente marco se ha diseñado en torno a una gobernanza basada en niveles y funciones generales.

Marco de certificación del ENS para EELL

Este modelo propuesto por el CCN pretende **facilitar la adecuación y posterior certificación de los Ayuntamientos con menos recursos** al Esquema Nacional de Seguridad (ENS), a través de **mecanismos de adecuación, implantación, auditoría y certificación comunes y/o multi-organismo** residentes en las Diputaciones/Cabildos. El proceso de implantación propuesto por este modelo es gradual, empezando con una **muestra representativa** de ayuntamientos (ver figura 2), con el objetivo de definir de forma

consistente y completa los procesos necesarios, procediendo luego a la integración, de forma sencilla y rápida, de los restantes municipios.

Este modelo de referencia, en un primer acercamiento al Cabildo y a los Ayuntamientos de la Isla de Tenerife, se ha previsto con la siguiente organización y funciones generales (ver figura 2):

- **Comité de Seguridad (Cabildo y Ayuntamientos)**: Órgano de decisión y aprobación.
- **Oficina de Seguridad (Cabildo)**: incorpora un vSoC (Centro de Operación de la Ciberseguridad Virtual, es decir centralizado en el Cabildo y compartido con los ayuntamientos) y se encarga del apoyo directo a la adecuación y prestación de los servicios de Seguridad que se vayan determinando.
- **Órgano de Auditoría Técnica (Cabildo**): se encargará de la verificación y certificación del cumplimiento normativo (acreditación del mantenimiento en el tiempo de la adecuación).

Figura 2. Propuesta Marco de Certificación EELL para el Cabildo (fuente: CCN-CERT)

Para el presente marco se han adoptado los órganos más específicos y funciones de este modelo, pero se han incorporado las modificaciones necesarias para contemplar el tratamiento de los servicios propios/locales de los ayuntamientos, ya que son los mayoritarios en la situación actual (se está trabajando en la implantación progresiva de servicios comunes prestados desde el Cabildo para minimizar la necesidad de servicios propios/locales en los ayuntamientos), así como la incorporación de ayuntamientos de

cualquier dimensión, modulando el apoyo prestado a los mismos en función de los recursos disponibles.

Reglamento de Asistencia Integral a los Municipios

Esta normativa, en su **Sección 2ª**, desarrolla los términos y condiciones específicos del servicio de **Asistencia técnica en materia de modernización administrativa**, que el Cabildo presta a los ayuntamientos de la Isla de Tenerife, y en el que se encuentra incluida la asistencia en materia de seguridad de la información objeto del marco propuesto. Dentro de este reglamento, se establece como órgano de **coordinación, participación, seguimiento y garantía del desarrollo integral de las actuaciones** a la **Comisión de Modernización Insular (CMI)**, que se dota con las siguientes funciones:

- a) **Diseño, definición, delimitación, planificación y coordinación** de las actuaciones a realizar.
- b) **Evaluación** del **estado de las infraestructuras y servicios** de las entidades locales, con el objetivo de consensuar la evolución de las mismas y adecuar las actuaciones a las infraestructuras tecnológicas existentes en cada momento.
- c) **Comunicación y seguimiento** de la ejecución de las actuaciones.
- d) **Aprobación de los acuerdos específicos** que se consideren oportunos, que no impliquen modificación del plan anual de proyectos, para mejorar la realización de su objeto.
- e) Elaboración conjunta de un **informe de valoración del resultado** de los planes de proyecto anuales.
- f) Elaboración de **propuestas para modificar** el presente servicio.
- g) Las **cuestiones litigiosas o controversias** que puedan surgir entre las administraciones afectadas en relación con la ejecución interpretación, modificación, resolución y efectos del servicio de asistencia técnica en modernización y/o la ejecución de los Planes Anuales de Proyectos, se deberán solventar por mutuo acuerdo de las partes en esta Comisión.
- h) **Gobierno de la seguridad de la información en los marcos de actuación conjuntos que se establezcan, asumiendo las competencias directivas y estratégicas necesarias**.

Esta última función (h), se ha incorporado durante el proceso de revisión de este reglamento (que ha coincidido en el tiempo con el proceso de análisis y definición del presente marco) con el objetivo de dotar a esta Comisión de las competencias necesarias para actuar de **órgano institucional de dirección y/o gobierno** de la seguridad de la información a nivel insular.

Estructura del marco de gobernanza

En base a los modelos de referencia estándares indicados en el apartado anterior, y considerando la realidad y situación actual de la Isla de Tenerife, se ha propuesto un marco

de gobernanza, que se desarrolla en los siguientes apartados, y con las siguientes características generales (ver figura 3):

- 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 institucional 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 los ayuntamientos.
- Se gradúa la participación/responsabilidad de los ayuntamientos en función de su dimensión, y por tanto, de sus recursos disponibles.
- Se crea una nueva figura de Responsable de Seguridad Insular, centralizado en el Cabildo y con responsabilidad sobre los sistemas propios de los ayuntamientos con menos recursos.
- Se integra con la gestión de protección de datos, al incorporar la figura del Delegado de Protección de Datos de los ayuntamientos (figura centralizada en el Cabildo y ya existente desde el año 2018).

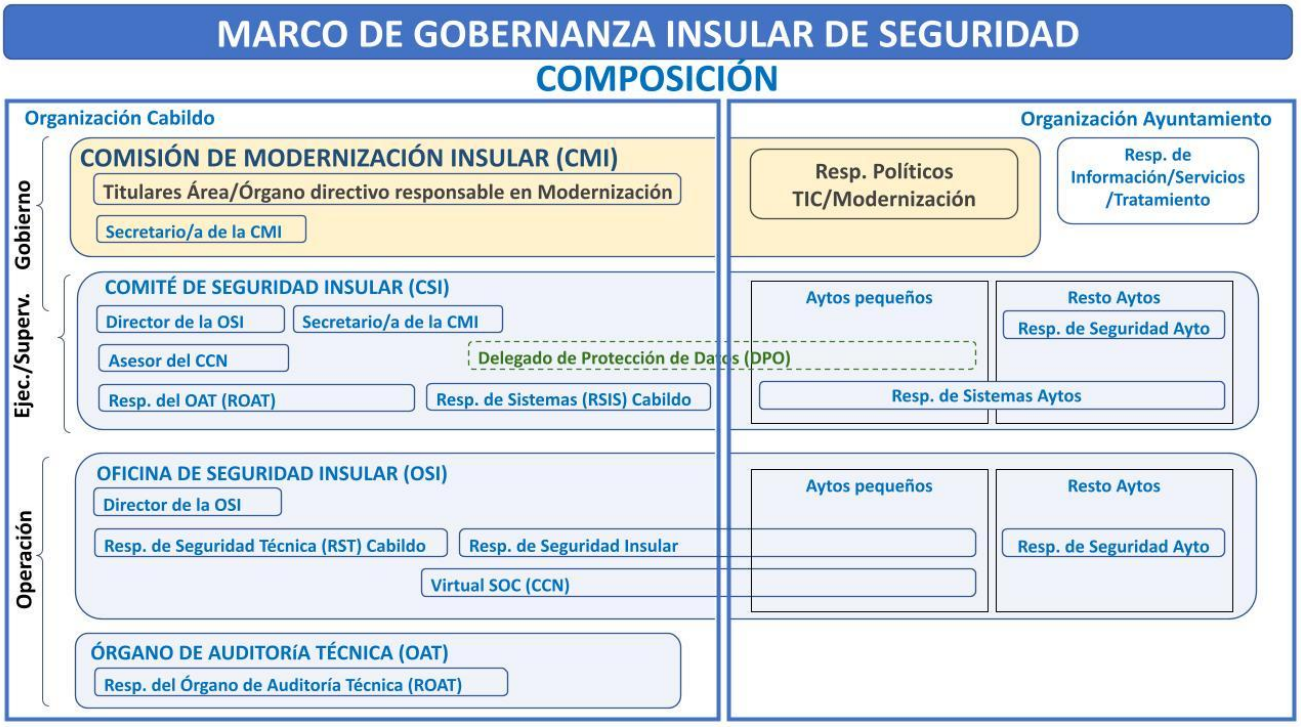

Figura 3. Marco insular de gobernanza de la seguridad (fuente: elaboración propia)

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, y que asumirá entre otras funciones con respecto a la asistencia técnica en materia de modernización administrativa que el Cabildo presta a los ayuntamientos 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 institucional 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

- Proponer 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 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 institucionales de cada entidad.
- Resolver los conflictos de responsabilidad que puedan aparecer en todo el marco.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos. 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 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 los Ayuntamientos adheridos 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 los ayuntamientos, como los propios.
- Conocer y reorientar si se estimase necesario, la aprobación por el CSI de los niveles de seguridad de la información y/o servicios y de la Política de Seguridad común.

Nivel Ejecutivo/Supervisión

Comité de Seguridad Insular (CSI)

Se trata del **órgano / grupo de trabajo** que dará respuesta desde el punto de vista ejecutivo y de supervisión a las exigencias de seguridad de la información derivadas de la Adecuación al Esquema Nacional de Seguridad (ENS, RD 3/2010, de 8 de enero).

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 Ayto (RSA)**: un máximo de 3 representantes (rotario en cada sesión según orden de población, empezando por los de menor población).
    - **Resp. de Sistemas (RSIS) del Cabildo**.
    - **Resp. de Sistemas de los Ayuntamientos**: un máximo de 3 representantes (rotario en cada sesión según orden de población, 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 los ayuntamientos.
- **Especialistas externos**: 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 común 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 los ayuntamientos 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 al 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).

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 del proyecto de asistencia técnica de la seguridad informática para los ayuntamientos.
- **Resp. de Seguridad Técnica (RST) del Cabildo**.
- **Resp. de Seguridad Insular (RSIN)**.
- **Resp. de Seguridad de Ayto (RSA)**.
- **Equipo vSOC (CCN)**: Jefe de Proyecto y técnicos del Virtual SOC designados por el CCN.

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 la Organización 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 los ayuntamientos que hubieren sido presentadas por los Responsables de los ayuntamientos.
- Mantener informado al CSI del resumen del estado, así como actuaciones e incidentes relevantes.
- Redacción y presentación de propuestas al CSI.
- Para los ayuntamientos de menos de 20.000 habitantes adheridos al marco, 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

- Su actividad se dirigirá principalmente a los ayuntamientos de población inferior a 20.000 habitantes, aunque en la medida de las posibilidades atenderá también al resto de ayuntamientos en orden de población.
- 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 los ayuntamientos.

Roles de seguridad

Responsables de la Información/Servicio/Tratamiento

Ámbito:

- Se tratará de una o varias figuras nombradas en cada ayuntamiento (se recomienda que sea única en los ayuntamientos con menos recursos).

- 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.

Responsables de Seguridad

Ámbitos

- **Resp. de Seguridad Técnica (RST) del Cabildo**: ejercerá las funciones de responsable de seguridad sobre los servicios comunes que presta el Cabildo a los ayuntamientos.
- **Resp. de Seguridad Insular (RSIN)**: ejercerá las funciones de responsable de seguridad sobre los servicios propios de los ayuntamientos de menos de 30.000 habitantes.
- **Resp. de Seguridad de Ayto (RSA)**: ejercerá las funciones de responsable de seguridad sobre los servicios propios en los ayuntamientos de 30.000 o más habitantes y será designado por el propio ayuntamiento.

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 la Organización.
  - 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).Responsables de Sistemas

Responsable de Sistemas

Ámbitos

- **Resp. de Sistemas (RSIS) del Cabildo**: tendrá responsabilidad sobre los servicios comunes que presta el Cabildo a los ayuntamientos.
- **Resp. de Sistemas de los Ayuntamientos**: tendrán responsabilidad sobre los sistemas propios de cada ayuntamiento.

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.

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 a los ayuntamientos.
- **Resp. de Sistemas de los Ayuntamientos**: tendrán la responsabilidad de este rol sobre los sistemas propios de cada ayuntamiento.

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.

Referencias

- Roles y responsabilidades:
    - Guía CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones.
    - Reglamento de Asistencia Integral a los Municipios (RAIM).
    - Guía estratégica en seguridad para entidades locales (FEMP). Tomo I.
- Marco de certificación de EELL
    - Abstract - Marco de Certificación ENS para Entidades Locales (CCN-CERT).
    - Abstract - Marco Gobernanza y COMSEG-ICTS v1.0 (CCN-CERT).
    - Proyecto MARCO CERTIFICACIÓN ENS-EELL Cabildo de Tenerife (CCN-CERT).
- Políticas de seguridad:
    - POL-ENS-000-Política de Seguridadv2.31 - Cabildo
    - POL-001 Política de Seguridad de la Información EELL_v01 Propuesta CCN.