Guía de Seguridad de las TIC
CCN-STIC 883

Anexo II. Plan de Adecuación al ENS 20.000>Ayuntamientos <75.000 (habitantes)

Mayo 2020

MINISTERIO DE DEFENSA

Edita:

NIPO :083-19-183-2

Fecha de Edición: mayo de 2020

ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día __ de _____ de ____ por resolución del Alcaldía del Ayuntamiento de _____.

2. INTRODUCCIÓN

FUNDAMENTOS JURÍDICOS

La *"Disposición transitoria. Adecuación de sistemas"* del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, establecía:

1. Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

2. Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo**, se dispondrá de un plan de adecuación** que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

3. Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo.

Plazo que venció en enero de 2014

Posteriormente, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, estableció un nuevo plazo para la implantación de las nuevas medidas, recogido también en su *"Disposición transitoria única. Adecuación de sistemas".*

Las entidades incluidas dentro en el ámbito de aplicación del presente real decreto dispondrán de un plazo de veinticuatro meses contados a partir de la fecha de la entrada en vigor del presente real decreto, para la adecuación de sus sistemas a lo dispuesto en el mismo.

Plazo que venció en noviembre de 2017.

CONCLUSIONES

El Ayuntamiento de _____, **considera que la necesidad de realizar el Plan de Adecuación sigue manteniéndose vigente y que, además, lo considera como necesario para llevar a cabo el proceso de implantación del ENS**,

motivo por el cual se ha elaborado el siguiente documento, que se estructura en los apartados que se indican a continuación.

3. POLÍTICA DE SEGURIDAD

El Ayuntamiento de _____, dispone de una Política de Seguridad aprobada el ___de _____ de _____. Esta Política de Seguridad ha sido desarrollada teniendo en cuenta los principios básicos y en base a los requisitos mínimos de seguridad establecidos por la normativa del ENS y conforme a lo exigido en el Anexo II del Real Decreto ENS, contemplando los requisitos exigidos en la sección [org. 1].

En el **Anexo I**, del presente documento, se adjunta la **Política de Seguridad** junto con el documento de designación de roles de seguridad y de constitución del Comité de Seguridad

En el Plan de Mejora de la Seguridad (**Anexo V**) se detalla cómo se planea adaptar la política a las exigencias del Anexo II del Real Decreto ENS.

4. CATEGORIZACIÓN DEL SISTEMA

En el **Anexo II,** del presente documento, se adjunta la **Categorización del Sistema** del Ayuntamiento de _____ compuesta por el **Inventario y Valoración de los Servicios y de la Información asociada a los mismos,** junto con su justificación, y la **categorización del sistema**, según lo establecido en el Anexo I del Real Decreto 3/2010.

5. ANÁLISIS DE RIESGOS

El Ayuntamiento de _____, ha realizado un análisis de riesgos, según lo establecido en el Anexo II del Real Decreto en su sección [op.pl.1], conforme a lo establecido en el Perfil de Cumplimiento Específico de aplicación a Ayuntamientos de más de 20.000 habitantes y de menos de 75.000 habitantes.

En el **Anexo III**, del presente documento, se adjunta el **Informe de Análisis de Riesgos y aceptación de riesgos residuales**. El análisis de riesgos ha sido realizado usando la metodología MAGERIT en su versión 3.0 (MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica).

6. DECLARACIÓN DE APLICABILIDAD

En el **Anexo IV**, del presente documento, se adjunta la **Declaración de Aplicabilidad** del Ayuntamiento de _____conforme a lo establecido en el Perfil de Cumplimiento Específico de aplicación a Ayuntamientos de más de 20.000 habitantes y de menos de 75.000 habitantes.

7. PLAN DE MEJORA DE LA SEGURIDAD

En el **Anexo V**, del presente documento, se adjunta el **Plan de Mejora de la Seguridad** del Ayuntamiento de _____ que contiene las acciones necesarias para subsanar las carencias detectadas en el sistema, y que se encuentran recogidas en el **informe de insuficiencias,** también incluido en dicho anexo.

ANEXO I POLÍTICA DE SEGURIDAD

ÍNDICE

1. MODELO DE DECRETO DE CREACIÓN DE ORGANO Y DESIGNACIÓN DE ROLES DE SEGURIDAD DE LA INFORMACIÓN

PROPUESTA DE DECRETO DE ALCALDÍA DEL AYUNTAMIENTO DE _____ POR EL QUE SE ASIGNAN FUNCIONES AL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y SE DESIGNAN ROLES Y FUNCIONES DE SEGURIDAD DE LA INFORMACIÓN EN EL AYUNTAMIENTO, EN CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD

El Concejal/Jefe de servicio o área _____del Ayuntamiento de_____ eleva a la Alcaldía la propuesta de Decreto para la creación de los órganos y definición de puestos necesarios para el cumplimiento del Esquema Nacional de Seguridad Real Decreto_____, a la Alcaldía de la entidad, en virtud de las funciones atribuidas en el Decreto de Alcaldía _____ por el que se le delegan las competencias en administración electrónica, de acuerdo con los siguientes

ANTECEDENTES DE HECHO

Primero. - Las Administraciones Públicas se han fijado como objetivo crear las condiciones adecuadas para el desarrollo de nuevos servicios ligados a la evolución de la tecnología y promover e impulsar, de igual modo, su uso entre la ciudadanía y las empresas. Esta evolución, conlleva también una mayor facilidad para el tratamiento de gran cantidad de información, la cual debe ser debidamente protegida.

A ello contribuyó, en la hoy derogada Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que promovió el uso de medios electrónicos para el desarrollo de la actividad y el ejercicio de las competencias en las Administraciones Públicas.

Segundo. - La consagración del derecho a comunicarse con la Administración Pública a través de medios electrónicos, se recogió en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Esta Ley, además, manifestó la necesidad de una adecuada protección de la información y de los servicios, que permitiera usar los medios electrónicos con confianza.

Tercero.- Para dar respuesta a un marco común de seguridad de la información en las administraciones públicas y su sector público, en desarrollo de la Ley 11/2007, de 22 de junio, se aprobó el Real Decreto 3/2010, de 8 de enero, por el que se reguló el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, mediante el que se establecen los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios. En dicho Decreto se definen y asignan competencias específicas dentro de la organización y que se incluyen en la política general de seguridad, con la atribución de funciones concretas e incluyendo la creación de un órgano con funciones de asesoramiento y resolución.

Cuarto. - Con la aprobación de la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común y la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, se da un impulso definitivo a la implantación de los procesos electrónicos en las administraciones públicas, citando expresamente la necesidad de respetar un marco común de seguridad de la información. Además, Con la entrada en vigor de ambas leyes, consagra la comunicación electrónica entre la Administración y la ciudadanía, haciéndose imprescindible garantizar el cumplimiento de los principios básicos y requisitos mínimos estableciendo las medidas de seguridad necesarias que habrán de ser proporcionales a las dimensiones de seguridad relevantes y a la categoría del sistema de información a proteger.

FUNDAMENTOS JURÍDICOS

Primero. - La Ley 39/2015, de 1 de octubre, de procedimiento administrativo común y la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, reiteran en su articulado la necesidad de cumplir con las medidas de seguridad de la información y, en concreto, se cita de forma explícita el ENS en el artículo 155 de la Ley 40/2015.

Segundo.- Así mismo, tras la entrada en vigor, el día 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), se deberán adoptar medidas técnicas, organizativas, así como de protección legal y cumplimiento, entre las que se encuentran la designación de la figura del Delegado de Protección de Datos. Designación que ha sido realizada mediante [indicar nº de Decreto y día] y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de derechos digitales, en cuya Disposición Adicional Primera vincula la seguridad de los datos personales a las medidas del Esquema Nacional de Seguridad.

Tercero. - En aplicación del Real Decreto que regula el Esquema Nacional de Seguridad, que deroga al Real Decreto 3/2010, el Ayuntamiento debe implantar una serie de medidas de seguridad que se aplicarán tanto en el marco organizativo, como en el operacional y de protección. Entre ellas destaca la creación de la Política de Seguridad de la Información, la cual recoge entre otros aspectos:

- Los **roles o funciones de seguridad**, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación
- La estructura del **Comité de Seguridad de la Información** para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

Por lo expuesto, se propone a la Alcaldía la aprobación del Decreto por el que se crea el comité de seguridad de la información, se regula su composición y funcionamiento y se designan las funciones en seguridad de la información en el Ayuntamiento de _____, en los términos que a continuación se detallan**.**

DECRETO [INDICAR Nº DE DECRETO Y DÍA] DE LA ALCALDÍA, POR EL QUE SE ASIGNAN FUNCIONES AL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, SE REGULA SU COMPOSICIÓN Y FUNCIONAMIENTO Y SE DESIGNAN ROLES Y FUNCIONES EN SEGURIDAD DE LA INFORMACIÓN EN EL AYUNTAMIENTO DE _____

De acuerdo con lo dispuesto con la potestad de auto-organización de la entidad reconocida en el artículo 4 de la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local y a propuesta del Área con competencias en la administración electrónica y la seguridad de la información del Ayuntamiento, teniendo en cuenta lo establecido en el Real Decreto _____ por el que se regula el Esquema Nacional de Seguridad.

DISPONGO

Artículo 1.- Objeto

1.- El objeto del presente Decreto es la constitución de un órgano colegiado con capacidad decisoria en materia de seguridad de la información del Ayuntamiento denominado Comité de Seguridad de la Información, incluyendo la regulación de sus composición y funciones.

2.- En el presente Decreto se designan también las funciones que en materia de seguridad de la información deben atribuirse al Responsable de Servicio, Responsable de la Información, Responsable de Seguridad y Responsable del Sistema, de acuerdo con lo dispuesto en el artículo 11. Organización e implantación del proceso de seguridad e implantación del proceso de seguridad del Real Decreto por el que se regula el Esquema Nacional de Seguridad.

Artículo 2.- Naturaleza jurídica del órgano

1.- El Comité de Seguridad de la información es un órgano colegiado con capacidad decisoria en la seguridad de la información de la entidad, sin personalidad jurídica propia.

2.- El órgano colegiado está integrado por las personas designadas de acuerdo a los roles establecidas en la normativa reguladora del Esquema Nacional de Seguridad aplicable a la entidad.

Artículo 3.- Régimen jurídico

El Comité de Seguridad de la Información se rige por las disposiciones del presente Decreto, así como por la regulación establecida para la regulación del Esquema Nacional de Seguridad y la Política de Seguridad del Ayuntamiento y por otras instrucciones o criterios interpretativos u otras regulaciones que puedan emitir los organismos de control que se relacionen con la materia de la seguridad de la información.

Artículo 4.- Funciones

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas 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.
    - 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 horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración 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.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con el Dirección General.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.

- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

Asimismo, podrán ser delegadas otras funciones por otro órgano de la entidad con competencias en la materia. Las funciones atribuidas al Comité por otro órgano no podrán ser delegadas si bien podrán ser revocadas en cualquier momento.

El Comité se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

Artículo 5.- Composición

Nota: se recomienda que el cargo de presidente lo ocupe un cargo con responsabilidad o cargo político para asegurar que las decisiones que se tomen se lleven a cabo.

- Presidente/a: _____
- Secretario/a: _____ nota: también puede ser cualquiera de los miembros
- Vocales:
  - Responsable/s de Información. [opcional]
  - Responsable/s de Servicios. [[opcional]
  - Delegado de Protección de Datos.
  - Responsable de Seguridad.
  - Responsable del Sistema.

El Delegado de Protección de Datos participará con voz, pero sin voto, en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

Los Responsables de la Información y de los Servicios serán convocados en función de los asuntos a tratar, pudiendo el Comité de Seguridad recoger las funciones y obligaciones de los Responsables de la Información y de los Servicios en aquellas acciones transversales en las que le sea solicitado y/o se considere necesario.

Asimismo, y con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

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

Los miembros serán designados por Resolución de la Alcaldía Presidencia o concejalía en quien delegue.

Artículo 6.- Régimen de funcionamiento y convocatorias

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias del Ayuntamiento de_____ con periodicidad [indicar periodicidad] previa convocatoria al efecto realizada por la Presidencia del mismo con 72 horas de antelación. En la convocatoria se incluirán los asuntos del Orden del Día a tratar.

Se podrán realizar reuniones con carácter extraordinario, siendo la convocatoria con un plazo de 24 horas. En la misma se referenciará el carácter extraordinario y urgente de la convocatoria, así como los asuntos del Orden del día a tratar. En las sesiones extraordinarias no se incluirá el apartado de ruegos y preguntas.

La Presidencia del Comité tendrá la facultad de suspender la celebración de las sesiones del Comité de Seguridad de la Información como consecuencia de los periodos vacacionales, cuando ello no suponga un menoscabo a la seguridad, así como para posponer o adelantar la celebración de las sesiones ordinarias del Comité, dentro de la misma semana de su celebración, cuando el día fijado sea festivo.

El Comité quedará constituido con la presencia de la mitad de las personas integrantes en segunda convocatoria. En el caso de que no exista quorum suficiente, la Presidencia procederá a convocar la sesión en el plazo de 48 horas.

Las reuniones del Comité no serán retribuidas, a excepción de los gastos por desplazamiento que, en su caso, puedan producirse.

Artículo 7.- Designación de puestos en seguridad de la información

1.- La atribución de las funciones de seguridad en los distintos puestos serán realizadas por resolución de la Alcaldía Presidencia o Concejalía delegada.

El Responsable de Información será un puesto de nivel directivo, al ser el responsable último de la información municipal, según se describe en la Política del Ayuntamiento.

El Responsable del Servicio establece los requisitos de servicio en materia de seguridad, estableciendo los niveles de seguridad de los servicios.

El Responsable de Información o Servicio podrán recaer en un único puesto u órgano.

El Responsable de Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la organización. Se podrán crear Responsables Delegados de Seguridad en función de la complejidad municipal, según lo establecido en la Política de Seguridad del Ayuntamiento.

El Responsable del Sistema se establece a nivel operativo. Se pueden designar Delegados de dicho responsable según lo establecido en la Política de Seguridad del Ayuntamiento.

2.- Los roles de seguridad y la descripción de los puestos que los ocuparán son los siguientes

Responsable/s de Información _____

Responsable de los Servicios: _____

Responsable de Seguridad: _____

Responsable del Sistema: _____

3.- Las competencias atribuidas al puesto se integrarán en la descripción de funciones de los puestos del Ayuntamiento, en su caso.

Artículo 8.- Responsable del Servicio

- Al Responsable del Servicio se le atribuyen las siguientes funciones:
- Establecer y aprobar los requisitos de seguridad aplicables al servicio dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad y/o Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afecten al Servicio.

Artículo 9.- Responsable de la Información

Al Responsable de la Información se le atribuyen las siguientes funciones:

- Establecer y aprobar los requisitos de seguridad aplicables a la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad y/o Comité de Seguridad de la Información
- Aceptar los niveles de riesgo residual que afecten a la Información.

Artículo 10.- Responsable de Seguridad

El Responsable de Seguridad desempeñará las siguientes funciones:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad; identificar medidas de seguridad; determinar configuraciones necesarias; elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.

- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

El Responsable de Seguridad, en función de la complejidad de la organización, podrá proponer Delegados de sus funciones por áreas diferenciadas que serán designados por la Alcaldía Presidencia o Concejalía delegada. Dichos delegados tendrán dependencia funcional directa y serán responsables en el ámbito asignado.

Artículo 11.- Responsable del Sistema

El Responsable de Sistemas realizará las siguientes funciones:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad y/o el Comité de Seguridad 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.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - 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.
    - 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.
    - 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.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá proponer para la designación por la Alcaldía Presidencia o Concejalía delegada, a los responsables del sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

Artículo 12.- Grupos de trabajo

Para el desarrollo de las funciones del Comité se podrán constituir grupos de trabajo que desarrollarán tareas específicas y de temática concreta y especializada.

La composición de los Grupos de trabajo podrá estar integrada por personas empleadas de la entidad o bien por especialistas externos a la organización, si bien la Presidencia de las mismas recaerá siempre en un miembro del Comité.

Las funciones, composición y régimen de funcionamiento se definirán en el acuerdo de constitución aprobado por el Comité de Seguridad

Disposición adicional Primera. - Habilitación de desarrollo y aplicación

El Comité de Seguridad podrá desarrollar el presente Decreto dictando normas internas o instrucciones que fuesen necesarias.

Disposición final primera. - Comunicaciones

La designación de estos responsables y sus funciones será comunicada a las personas afectadas.

La designación como miembro del Comité y sus funciones será comunicada al Departamento de régimen interior, así como a las personas designadas.

Este Decreto tendrá eficacia desde su aprobación.

Nota: para su elaboración como apoyo adicional se puede utilizar la Guía CCN-STIC 801. Esquema Nacional de Seguridad.

2. MODELO DE POLÍTICA DE SEGURIDAD

ÍNDICE

APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día __ de _____ de ____ por resolución del Alcaldía del Ayuntamiento de _____.

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

Nota: motivación del porqué de la política- texto extraído de la CCN-STIC-805 Política de Seguridad de la Información

El Ayuntamiento de _____, depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. 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.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

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. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.

Los diferentes departamentos 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.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

3. MISIÓN DEL AYUNTAMIENTO DE _____

Nota: Describir los objetivos de servicio del organismo

4. ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de _____, que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del alcance del Esquema Nacional de Seguridad (ENS).

5. MARCO NORMATIVO

Nota: revisar – tener en cuenta normativa sectorial y/o autonómica, etc.

La base normativa que afecta al desarrollo de las actividades y competencias del Ayuntamiento de _____, en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, modificado por Real Decreto 951/2015, de 23 de octubre.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, y su normativa de desarrollo.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Política de firma electrónica del Ayuntamiento de _____.

- Reglamento por el que se establece la Sede Electrónica del Ayuntamiento de _____.
- Nota: completar con demás normativa que sea de aplicación.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de _____, derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política.

El mantenimiento del marco normativo será responsabilidad del Ayuntamiento de _____, y se mantendrá en un Anexo a este documento. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el "Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad".

Así mismo, el Ayuntamiento de _____, también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

6. CUMPLIMIENTO DE ARTÍCULOS

El Ayuntamiento de _____, para lograr el cumplimiento de los artículos del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral (artículo 6) y seguridad por defecto (artículo 19)

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al Ayuntamiento de _____, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

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

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) 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.

Reevaluación periódica (artículo 9) e integridad y actualización del sistema (Artículo 2)

El Ayuntamiento de _____, ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a 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. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Gestión de personal (artículo 14) y profesionalidad (artículo 15)

Todos los miembros del Ayuntamiento de _____, dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, 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.

Gestión de la seguridad basada en los riesgos (artículo 6) y análisis y gestión de riesgos (artículo 13)

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos cada una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad (artículo 24), prevención, reacción y recuperación (artículo 7)

El Ayuntamiento de _____, ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, el Ayuntamiento de _____, implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

El Ayuntamiento de _____, establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un 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).

- Para garantizar la disponibilidad de los servicios, el Ayuntamiento de _____, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa (artículo 8) y prevención ante otros sistemas interconectados (artículo 22)

El Ayuntamiento de _____, ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Función diferenciada (artículo 10) y organización e implantación del proceso de seguridad (artículo 12)

El Ayuntamiento de _____, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Autorización y control de los accesos (artículo 16)

El Ayuntamiento de _____, ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 17)

El Ayuntamiento de _____, ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 18)

Para la adquisición de productos, el Ayuntamiento de _____, tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición,

salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito (artículo 21) y continuidad de la actividad (artículo 25)

El Ayuntamiento de _____, ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

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.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de Ayuntamiento de _____. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad (artículo 23)

El Ayuntamiento de _____, ha habilitado registros de la actividad 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. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, 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.

7. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la Seguridad de la Información en el Ayuntamiento de _____, se establece en la forma que se indica a continuación.

7.1. Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Delegado de Protección de Datos (DPD): _____
- Responsable/s de Información: _____

- Responsable/s de los Servicios: _____
- Responsable de Seguridad: _____
- Responsable del Sistema: _____

7.2. Comité de Seguridad de la Información

El Ayuntamiento de _____, ha constituido un Comité de Seguridad de la Información, como órgano colegiado, y está formado por los siguientes miembros:

- Presidente: _____
- Secretario/a: _____ nota: también puede ser cualquiera de los miembros
- Miembros:
  - Responsable/s de la Información. [opcional]
  - Responsable/s de los Servicios. [opcional]
  - Delegado de Protección de Datos.
  - Responsable de Seguridad.
  - Responsable del Sistema.

Los Responsables de la Información y de los Servicios serán convocados en función de los asuntos a tratar.

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

Nota: en caso de que los Responsables de Información y Responsables de Servicios no se hayan incluido como miembros del comité.

Los Responsables de la Información y los Servicios serán convocados en función de los asuntos a tratar.

Con carácter opcional, otros miembros del Ayuntamiento de _____, podrán incorporarse a las labores del Comité, incluidos grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias del Ayuntamiento de _____, con periodicidad [indicar periodicidad], previa convocatoria al efecto realizada por el Presidente de dicho Comité.

7.3. Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de los roles de seguridad ENS:

Funciones del Responsable de la Información y de los Servicios

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta al Responsable de Seguridad ENS, y/o Comité de Seguridad de la Información
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del Responsable de Seguridad

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

Funciones del Responsable del Sistema

Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

Elaborar los procedimientos operativos necesarios.

Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

Prestar al Responsable de Seguridad de la Información y/o el Comité de Seguridad 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.

Llevar a cabo las funciones del administrador de la seguridad del sistema:

- 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.
- 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.
- 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.

Cuando la complejidad del sistema lo justifique, el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

7.4 Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.

- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas 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.
    - 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 horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración 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.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
    - Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

7.5. Procedimientos de designación

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política ha sido realizada por Alcaldía del Ayuntamiento de _____, y comunicada a las partes afectadas [indicar como se ha procedido].

Los miembros del Comité, así como los roles de seguridad serán revisados cada [cuatro años] o con ocasión de vacante.

7.6. Resolución de conflictos

El [Comité de Seguridad de la Información], se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

2.8. DATOS DE CARÁCTER PERSONAL

El solo 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.

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del Reglamento (UE) A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los datos 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.

Nota: hacer referencia a la política de protección de datos

2.9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El [Comité de Seguridad de la Información] ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al [Comité de Seguridad de la Información] la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte del [indicar el órgano competente para su aprobación] competente por razón de la materia del Ayuntamiento de _____.

2.10. TERCERAS PARTES

Cuando el preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. El Ayuntamiento de _____, definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de actuaciones que el Ayuntamiento de _____, lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el Ayuntamiento de _____, utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad. De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogidas en el artículo 29 "Instrucciones técnicas de seguridad y guías de seguridad" del Real Decreto Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica modificado por el Real Decreto 951/2015 de 23 de octubre, y en consideración a la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS 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.

Nota: para su elaboración como apoyo adicional se puede utilizar la Guía CCN-STIC 805 Esquema Nacional de Seguridad. Política de Seguridad de la Información.

ANEXO II CATEGORIZACIÓN DEL SISTEMA

ÍNDICE

1. VALORACIÓN DE SERVICIOS E INFORMACIÓN

El presente registro recoge el inventario de servicios y de la información (gestionada por estos) junto con la valoración y su justificación.

0

1.1. Identificación e Inventario de Servicios e Información

Competencias de los Ayuntamientos de entre 20.000 y 75.000 habitantes

Para la identificación de servicios que se encuentran dentro del alcance de ENS, se ha tomado como base el análisis de las competencias recogidas en artículo 25 y lo establecido en el artículo 26 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL), donde la distribución de los servicios se gradúa en función del número de habitantes en varios rangos, teniendo un régimen diferenciado los municipios de menos de 5.000 habitantes, los de más de 20.000 y los que tienen una población superior a los 50.000 habitantes, sin perjuicio de las especialidades de los Ayuntamientos denominados de gran población, regulados en el Título X de la LBRL.

En el caso de los municipios de más de 20.000 habitantes, determinadas competencias son obligatorias. En concreto en el apartado 1 del artículo 26 se indica que:

> *c) En los Municipios con población superior a 20.000 habitantes, además: protección civil, evaluación e información de situaciones de necesidad social y la atención inmediata a personas en situación o riesgo de exclusión social, prevención y extinción de incendios e instalaciones deportivas de uso público.*
>
> *d) En los Municipios con población superior a 50.000 habitantes, además: transporte colectivo urbano de viajeros y medio ambiente urbano.*

Estos municipios no cuentan con la cooperación de la Diputación o Comunidad Autónoma uniprovincial en la prestación de servicios que se destina a los de menor población, como se indica en el artículo 26.3 de la LBRL.

Por último, no puede obviarse que los Ayuntamientos, independientemente de su población, tienen diversas potestades, entre otras, de auto-organización, tributaria y financiera (artículo 4 de la LBRL), además de gestionar su personal, fomentar la participación ciudadana o el Padrón de habitantes.

También, pueden tener competencias delegadas en las materias relacionadas en el artículo 27 de la LBRL, así como prestar servicios atribuidos por normas específicas como las relacionadas con la atención a las personas con un grado de dependencia. Es necesario puntualizar, también, que la delegación de las competencias puede realizarse por las Comunidades Autónomas por lo que la casuística de los servicios prestados puede diferenciarse en función del territorio, cuestión por la diversidad de normativa no puede ser tenida en cuenta en la Guía.

A continuación, se exponen las competencias recogidas en el artículo 25 LBRL.

COMPETENCIA	DESCRIPCIÓN
URBANISMO	Planeamiento, gestión, ejecución y disciplina urbanística. Protección y gestión del Patrimonio histórico. Promoción y gestión de la vivienda de protección pública con criterios de sostenibilidad financiera. Conservación y rehabilitación de la edificación
MEDIO AMBIENTE URBANO	En particular, parques y jardines públicos, gestión de la recogida y la gestión de los residuos sólidos urbanos y protección contra la contaminación acústica, lumínica y atmosférica en las zonas urbanas.
ABASTECIMIENTO DE AGUA	Abastecimiento de agua potable a domicilio y evacuación y gestión de aguas residuales.
INFRAESTRUCTURA	Infraestructura viaria y otros equipamientos de su titularidad.
SOCIAL	Evaluación e información de situaciones de necesidad social y la atención inmediata a personas en situación o riesgo de exclusión social.
PROTECCIÓN Y PREVENCIÓN	Policía local, protección civil, prevención y extinción de incendios.
TRÁFICO Y MOVILIDAD	Tráfico, estacionamiento de vehículos y movilidad. Transporte colectivo urbano.
TURISMO	Información y promoción de la actividad turística de interés y ámbito local.
COMERCIO	Ferias, abastos, mercados, lonjas y comercio ambulante.
SALUBRIDAD	Protección de la salubridad pública.
ACTIVIDADES FUNERARIAS	Cementerios y actividades funerarias.
DEPORTE	Promoción del deporte e instalaciones deportivas y de ocupación del tiempo libre.
CULTURA	Promoción de la cultura y equipamientos culturales
EDUCACIÓN	Participar en la vigilancia del cumplimiento de la escolaridad obligatoria y cooperar con las Administraciones educativas correspondientes en la obtención de solares necesarios para la construcción de nuevos centros docentes. La conservación, mantenimiento y vigilancia de los edificios de titularidad local destinados a centros públicos de educación infantil, de educación primaria o de educación especial.
ADMINISTRACION ELECTRÓNICA	Promoción de la participación de los vecinos en el uso eficiente y sostenible de las tecnologías de la información y las comunicaciones

COMPETENCIA	DESCRIPCIÓN
PROMOCIÓN DE LA IGUALDAD	Actuaciones de promoción de la igualdad entre hombre y mujeres así como contra la violencia de género

Identificación e inventario de Servicios

En base a lo indicado en el punto anterior y a las actividades realizadas en el Ayuntamiento a través de medios electrónicos, se han identificado los siguientes servicios dentro del alcance del ENS.

ID	SERVICIOS	DESCRIPCIÓN	COMPETENCIA *
S 01	URBANISMO	Tramitación y resolución de solicitudes, autorizaciones y licencias de obras. Gestión de desarrollos urbanístico y obras públicas	URBANISMO
S 02	MEDIO AMBIENTE	Mantenimiento de parques y jardines públicos. Gestión de la limpieza de viaria. Promoción, prevención e inspecciones relacionadas con la contaminación acústica, lumínica y atmosférica.	MEDIO AMBIENTE URBANO
S 03	AGUAS, SANEAMIENTO Y RECOGIDA DE RESIDUOS	Gestión y control de los servicios municipales de aguas y saneamiento y recogida de basuras.	MEDIO AMBIENTE URBANO ABASTECIMIENTO DE AGUAS
S 04	MANTENIMIENTO E INFRAESTRUCTURAS	Mantenimiento de la vía pública e instalaciones municipales.	INFRAESTRUCTURA
S 05	BIENESTAR SOCIAL	Servicios de evaluación y orientación para personas en situaciones de necesidad social, así como la atención inmediata a personas en situación o riesgo de exclusión social.	SOCIAL
S 06	ACTUACIONES SOCIALES Y ATENCIÓN A LA DEPENDENCIA	Gestión de las prestaciones y actuaciones sociales a personas y colectivos vulnerables incluyendo las relacionadas con la atención a la dependencia y la cooperación al desarrollo.	No contemplado en la LBRL. Ley de Promoción de la Autonomía Personal y Atención a la Dependencia. normativa sectorial y autonómica

ID	SERVICIOS	DESCRIPCIÓN	COMPETENCIA *
S 07	SEGURIDAD CIUDADANA Y PROTECCIÓN CIVIL	Servicios de Policía Local incluyendo la seguridad ciudadana, seguridad de las instalaciones municipales y la regulación del tráfico, gestión del estacionamiento de vehículos y el servicio de grúa y depósito municipal. Protección Civil.	PROTECCIÓN Y PREVENCION TRÁFICO Y MOVILIDAD
S 08	TRANSPORTE PÚBLICO	Servicio público de transportes en el municipio. Aparcamientos en superficie.	TRÁFICO Y MOVILIDAD
S 09	SERVICIO DE EXTINCIÓN DE INCENDIOS	Servicios de extinción de incendios y Protección Civil.	PROTECCIÓN Y PREVENCIÓN
S 10	PROMOCIÓN DE LA ENTIDAD LOCAL	Promoción de la entidad local mediante la organización de diversas actividades, así como la promoción del turismo.	TURISMO
S 11	COMERCIO Y MERCADOS	Ferias, abastos, mercados, lonjas y comercio ambulante.	COMERCIO
S 12	SERVICIOS FUNERARIOS	Gestión del cementerio municipal y de los servicios funerarios.	ACTIVIDADES FUNERARIAS
S 13	DEPORTES	Gestión de instalaciones deportivas y promoción del deporte en la entidad local.	DEPORTE
S 14	CULTURA	Promoción de la cultura y equipamientos culturales. Gestión de la biblioteca municipal.	CULTURA
S 15	EDUCACIÓN Y FORMACIÓN	Cooperación con las administraciones con competencias en educación, así como cualquier actividad formativa desarrollada por la entidad local.	EDUCACIÓN
S 16	ESCUELAS INFANTILES	Gestión de las escuelas infantiles municipales	EDUCACIÓN
S 17	IGUALDAD	Promoción de la igualdad entre hombres y mujeres, así como contra la violencia de género.	IGUALDAD

ID	SERVICIOS	DESCRIPCIÓN	COMPETENCIA *
S 18	REGISTRO GENERAL	Gestión de la entrada de escritos o comunicaciones presentados en el Ayuntamiento, así como la salida de los escritos y comunicaciones oficiales dirigidas a otros órganos o particulares.	No contemplado en la LBRL. Previsto en normativa de desarrollo ROF y en LPAC.
S 19	ARCHIVO	Organización y localización de expedientes, documentos o registros del Ayuntamiento que han pasado al Archivo Municipal. Gestión de las consultas, copias y préstamos de documentos del Archivo Municipal. Conservación y consulta de los documentos recibidos y producidos por la entidad local.	No contemplado en la LBRL. Previsto en normativa de desarrollo ROF y en LPAC.
S 20	CONTRATACIÓN	Gestión de los procedimientos de contratación pública, así como el seguimiento y control de los adjudicatarios	No contemplado en la LBRL. Contratación electrónica LCSP.
S 21	PARTICIPACIÓN CIUDADANA	Procesos participativos. Gestión de entidades ciudadanas y voluntariado del municipio. Publicidad activa y derecho de acceso a la información. Gestión de solicitudes de información, quejas, reclamaciones e iniciativas recibidas en el Ayuntamiento.	Asociado al artículo 70 y siguientes de la LBRL. LTABG.
S 22	INTERVENCIÓN	Control y fiscalización interna de la gestión económica, financiera y presupuestaria.	No contemplado en la LBRL. Desarrollo en LHL.
S 23	GESTIÓN TRIBUTARIA	Gestión de inspección y trámites relacionados con tributos y otros ingresos de derecho público	No contemplado en la LBRL. Desarrollo en LHL.
S 24	TESORERÍA	Gestión de los recursos financieros, incluyendo dinero, valores o créditos por operaciones presupuestarias o extrapresupuestarias.	No contemplado en la LBRL. Desarrollo en LHL.

ID	SERVICIOS	DESCRIPCIÓN	COMPETENCIA *
S 25	PERSONAL	Gestión del personal interno (vacaciones, bajas, consultas, etc.). Prevención de riesgos laborales y accidentes de trabajo. Gestión y publicación de ofertas de empleo público de personal de la entidad local.	No contemplado en la LBRL. Desarrollo en LHL.
S 26	VIVIENDA	Promoción de la vivienda pública en el municipio.	URBANISMO
S 27	INFORMÁTICA Y COMUNICACIONES	Gestión y control de los sistemas informáticos y de comunicaciones del Ayuntamiento, así como la gestión de la seguridad de los mismos. WIFI público Actuaciones y centros de promoción	No contemplado en la LBRL. Previsto en LRJSP y desarrollo ENS. ADMINISTRACIÓN ELECTRÓNICA
S 28	JUVENTUD	Asesoramiento e información a la población joven del municipio, así como la realización de actividades y eventos enfocados a este colectivo.	No contemplado en la LBRL. Legislación sectorial vinculada a la legislación sobre menores y juventud
S 29	SECRETARÍA MUNICIPAL	Gestión, seguimiento y control sobre los actos municipales y los miembros de la corporación local. Gestión de expedientes relacionados con la actividad municipal, defensa jurídica y responsabilidad patrimonial. Gestión de las obligaciones en materia de protección de datos.	Organización municipal de la LBRL
S 30	ESTADÍSTICA	Gestión del Padrón municipal.	Organización municipal de la LBRL
S 31	CONSUMO	Servicios de mediación en materia de consumo.	No contemplado en la LBRL. Legislación sectorial vinculada a los derechos de los consumidores

(*) En la descripción de las competencias se emplean las abreviaturas de las siguientes leyes:

- Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local (LBRL);
- Ley 39/2015, de 1 de octubre, de procedimiento administrativo común (LPAC);
- Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público (LRJSP);
- Ley 9/2017, de 8 de noviembre, de contratos del sector público (LCSP);
- Ley Reguladora de las Haciendas Locales (R.D. Legislativo2/2004, de 5 de marzo) (LHL);
- Estatuto Básico del Empleado Público (R.D. Legislativo 5/2015, de 30 de octubre) (EBEP)
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno (LTAIBG);
- Ley 39/2016, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las Personas en situación de Dependencia (Ley Dependencia);
- Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales (ROF).

Identificación e inventario de Información

A continuación, se han identificado los siguientes activos de información, que se encuentran gestionados por los servicios relacionados en apartado anterior. Para su determinación se tenido en cuenta el Registro de Actividades de Tratamiento (RAT).

ID	INFORMACIÓN	DESCRIPCIÓN
I 01	GESTIÓN URBANISMO MUNICIPAL	Gestión y control de los procedimientos y actividades realizados por el Ayuntamiento en materia de urbanismo, incluyendo planeamiento, gestión, restauración de la legalidad urbanística, expropiaciones urbanísticas y demás cuestiones de competencia municipal.
I 02	LICENCIAS, AUTORIZACIONES Y CONCESIONES	Gestión y tramitación de los expedientes de licencias, permisos, concesiones y autorizaciones de cualquier tipo gestionadas desde el Ayuntamiento.
I 03	ATENCIÓN A LA CIUDADANÍA	Tramitación y gestión de solicitudes de información, quejas, reclamaciones e iniciativas recibidas en el Ayuntamiento. Gestión de las solicitudes de acceso a la información pública y de la publicidad activa (transparencia) del Ayuntamiento.
I 04	GESTIÓN DEL CICLO DEL AGUA Y RESIDUOS	Gestión y control de la información relacionada con el ciclo del agua desde el abastecimiento al saneamiento y los controles necesarios para la prestación del servicio. Además, de los residuos municipales.
I 05	GESTIÓN DE LAS OBRAS MANTENIMIENTO E INFRAESTRUCTURAS	Gestión de la información relacionada con el mantenimiento de la vía pública e instalaciones municipales.
I 06	PROMOCIÓN DE LA VIVIENDA	Actuaciones relacionadas con la promoción de la vivienda pública en el municipio y para facilitar el acceso de diferentes colectivos al alquiler o compra.

ID	INFORMACIÓN	DESCRIPCIÓN
I 07	ATENCIONES Y PRESTACIONES SOCIALES	Gestión de la historia social para la prestación de los servicios sociales en el ámbito municipal. Asistencia y asesoramiento dirigidos al colectivo de mujeres víctimas de violencia de género o en riesgo de exclusión social. Desarrollo de políticas de atención a la infancia, igualdad, mayores
I 08	GESTIÓN DE LOS SISTEMAS DE ATENCIÓN A LA DEPENDENCIA Y OTRAS PRESTACIONES	Gestión de la información relacionada con el Sistema de Atención a la Dependencia (SAAD), el Plan Concertado y otras prestaciones relacionadas con personas o colectivos vulnerables.
I 09	AYUDAS Y SUBVENCIONES	Tramitación y gestión de las ayudas, becas y subvenciones existentes en los diferentes programas o líneas de subvención del Ayuntamiento.
I 10	POLICÍA LOCAL	Gestión y control de los procedimientos y actividades realizados por la Policía Local en el ámbito de sus competencias, incluyendo atestados, policía judicial, seguridad ciudadana, tráfico, movilidad, objetos perdidos, así como el servicio de grúa y depósito de vehículos. Así como la gestión de los sistemas de videovigilancia para garantizar la seguridad en las vías públicas.
I 11	PROTECCIÓN CIVIL	Gestión de las actuaciones e intervenciones de Protección Civil.
I 12	GESTIÓN DE LA MOVILIDAD URBANA	Gestión de la información relacionada con el transporte público en el municipio y la regulación de los aparcamientos municipales.
I 13	GESTIÓN DEL SERVICIO DE EXTINCIÓN DE INCENDIOS	Gestión de la información relacionada con los servicios de extinción de incendios.
I 14	PROCEDIMIENTOS SANCIONADORES	Gestión y control de toda clase de procedimientos sancionadores abiertos a consecuencia de infracciones tipificadas en las ordenanzas municipales y demás normativa reguladora de las competencias del Ayuntamiento.
I 15	SERVICIOS TELEMÁTICOS Y COMUNICACIONES	Gestión de las personas usuarias de los servicios telemáticos puestos a disposición de la ciudadanía: servicios web; equipos de uso público; otros servicios tecnológicos municipales puestos a disposición de la ciudadanía. Servicios de comunicaciones informativas.

ID	INFORMACIÓN	DESCRIPCIÓN
I 16	GESTIÓN DE SERVICIOS FUNERARIOS	Gestión del cementerio municipal y de los servicios funerarios.
I 17	GESTIÓN DE INGRESOS PÚBLICOS	Gestión de la recaudación de tasas e impuestos municipales ejecutada en plazo voluntario o ejecutivo, gestión de los distintos padrones municipales y actuaciones de inspección tributaria.
I 18	GESTIÓN DE SERVICIOS DEPORTIVOS	Gestión de las instalaciones deportivas y actividades deportivas desarrolladas en las mismas, así como el fomento, promoción del deporte en el municipio.
I 19	GESTIÓN DE SERVICIOS CULTURALES	Gestión de las actividades culturales organizadas o promocionadas por el Ayuntamiento, incluida la gestión de las bibliotecas municipales.
I 20	GESTIÓN DE SERVICIOS EDUCATIVOS	Gestión de los servicios, actividades y eventos educativos organizados y promovidos por el Ayuntamiento.
I 21	GESTIÓN DEL ARCHIVO MUNICIPAL	Organización, archivo de expedientes, documentos, contenidos audiovisuales, fondos o registros del Ayuntamiento que han pasado al Archivo Municipal. Gestión de las peticiones de acceso, consultas, copias y extracciones de documentos.
I 22	GESTIÓN DE LAS ESCUELAS INFANTILES	Gestión de la información relacionada con las escuelas de 0 a 3 años y las guarderías municipales.
I 23	CONTRATACIÓN PÚBLICA	Gestión del proceso de contratación municipal y seguimiento de los licitadores para el cumplimiento del servicio contratado.
I 24	GESTIÓN DEL PERSONAL	Gestión de la nómina del personal funcionario y laboral del Ayuntamiento, así como la obtención de todos los productos derivados de la misma. Gestión del personal del Ayuntamiento: Control de incompatibilidades; situación laboral; formación de los empleados municipales. Cumplimento de las obligaciones en materia de prevención de riesgos laborales. [categorías especiales de datos]
I 25	GESTIÓN PRESUPUESTARIA ECONÓMICA Y CONTABLE	Gestión económica y contable del Ayuntamiento con el fin de fiscalizar los ingresos y gastos del mismo. Realización de pagos correspondientes, gestión de la facturación, control presupuestario y gestión fiscal.

ID	INFORMACIÓN	DESCRIPCIÓN
I 26	GESTIÓN DE LOS ÓRGANOS MUNICIPALES DE GOBIERNO	Gestión de los datos de los miembros de la corporación del Ayuntamiento con la finalidad de realizar un seguimiento y control sobre los actos municipales, pago de las remuneraciones por las funciones desempeñadas, control de incompatibilidades, registro de bienes e intereses.
I 27	PADRÓN MUNICIPAL DE HABITANTES	Gestión del padrón municipal de habitantes acorde a los fines que establece al respecto la Ley de Bases de Régimen Local y demás normativa local aplicable. Gestión del censo electoral según establece la Ley de Régimen Electoral General y usos también con fines históricos, estadísticos y científicos.
I 28	REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS	Gestión del registro de entrada y salida de documentos en el Ayuntamiento en los términos y condiciones establecidas en la Ley de procedimiento administrativo común y en la normativa reguladora del funcionamiento de las entidades locales.
I 29	DEFENSA JURÍDICA Y RESPONSABILIDAD PATRIMONIAL	Gestión de los expedientes de responsabilidad patrimonial del Ayuntamiento. Gestión y seguimiento de los expedientes administrativos, así como de otras actuaciones realizadas desde la Secretaria Municipal.
I 30	SEGURIDAD DE INSTALACIONES MUNICIPALES	Sistemas de videovigilancia y control de accesos con el fin de garantizar la seguridad bienes e instalaciones municipales, así como de las personas que acceden o trabajan en las mismas.
I 31	GESTIÓN DE SERVICIOS JUVENILES MUNICIPALES	Gestión y control de los servicios, programas, actividades y recursos dirigidos a la población juvenil del municipio y de los participantes.
I 32	GESTIÓN DE LA PARTICIPACIÓN CIUDADANA	Gestión y control del registro municipal de entidades ciudadanas y de las consultas populares, presupuestos participativos, y demás procedimientos y actividades de participación ciudadana realizados o promovidos por el Ayuntamiento.
I 33	VOLUNTARIADO	Gestión y control de las personas que realizan algún tipo de actividad de voluntariado en el Ayuntamiento y de las actividades realizadas
I 34	GESTIÓN DE LAS OBRAS MANTENIMIENTO E INFRAESTRUCTURAS	Gestión de la información relacionada con el mantenimiento de las vías públicas e instalaciones municipales.
I 35	GESTIÓN DE LA PROMOCIÓN LOCAL Y EL TURISMO	Gestión de las actividades de promoción de la entidad local y de la promoción del turismo.

ID	INFORMACIÓN	DESCRIPCIÓN
I 36	SERVICIOS DE CONSUMO	Gestión de la información relacionada con la prestación de los servicios para la defensa de consumidores.
I 37	PROMOCIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA	Tratamiento de la información relacionada con la prestación de servicios para la promoción de la administración electrónica.
I 38	SISTEMAS DE INFORMACIÓN	Gestión interna de los sistemas de información y comunicaciones del Ayuntamiento para garantizar su correcto funcionamiento y el cumplimiento de las obligaciones de seguridad y protección de datos legalmente establecidas.

Relación entre Servicios e información

A continuación, se establece la relación entre Servicios e Información

SERVICIOS	INFORMACIÓN
URBANISMO	GESTIÓN URBANISMO MUNICIPAL LICENCIAS, AUTORIZACIONES Y CONCESIONES PROCEDIMIENTOS SANCIONADORES
MEDIO AMBIENTE	GESTIÓN DE LAS OBRAS MANTENIMIENTO E INFRAESTRUCTURAS PROCEDIMIENTOS SANCIONADORES GESTIÓN DEL CICLO DEL AGUA Y RESIDUOS
AGUAS, SANEAMIENTO Y RECOGIDA DE RESIDUOS	GESTIÓN DEL CICLO DEL AGUA Y RESIDUOS PROCEDIMIENTOS SANCIONADORES GESTIÓN DE LAS OBRAS MANTENIMIENTO E INFRAESTRUCTURAS
MANTENIMIENTO E INFRAESTRUCTURAS	GESTIÓN DE LAS OBRAS MANTENIMIENTO E INFRAESTRUCTURAS
BIENESTAR SOCIAL	ATENCIONES Y PRESTACIONES SOCIALES AYUDAS Y SUBVENCIONES
ACTUACIONES SOCIALES Y ATENCIÓN A LA DEPENDENCIA	ATENCIONES Y PRESTACIONES SOCIALES AYUDAS Y SUBVENCIONES GESTIÓN DE LOS SISTEMAS DE ATENCIÓN A LA DEPENDENCIA Y OTRAS PRESTACIONES
SEGURIDAD CIUDADANA Y PROTECCIÓN CIVIL	POLICÍA LOCAL PROTECCIÓN CIVIL PROCEDIMIENTOS SANCIONADORES SEGURIDAD DE INSTALACIONES MUNICIPALES
TRANSPORTE PÚBLICO	GESTIÓN DE LA MOVILIDAD URBANA POLICÍA LOCAL

SERVICIOS	INFORMACIÓN
SERVICIO DE EXTINCIÓN DE INCENDIOS	GESTIÓN DEL SERVICIO DE EXTINCIÓN DE INCENDIOS PROTECCIÓN CIVIL
PROMOCIÓN DE LA ENTIDAD LOCAL	ATENCIÓN A LA CIUDADANÍA GESTIÓN DE LA PROMOCIÓN LOCAL Y EL TURISMO AYUDAS Y SUBVENCIONES
COMERCIO Y MERCADOS	LICENCIAS, AUTORIZACIONES Y CONCESIONES PROCEDIMIENTOS SANCIONADORES
SERVICIOS FUNERARIOS	GESTIÓN DE SERVICIOS FUNERARIOS
DEPORTES	GESTIÓN DE SERVICIOS DEPORTIVOS AYUDAS Y SUBVENCIONES
CULTURA	GESTIÓN DE SERVICIOS CULTURALES AYUDAS Y SUBVENCIONES
EDUCACIÓN Y FORMACIÓN	GESTIÓN DE SERVICIOS EDUCATIVOS AYUDAS Y SUBVENCIONES
ESCUELAS INFANTILES	GESTIÓN DE LAS ESCUELAS INFANTILES
IGUALDAD	ATENCIONES Y PRESTACIONES SOCIALES AYUDAS Y SUBVENCIONES
REGISTRO GENERAL	REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS
ARCHIVO	GESTIÓN DEL ARCHIVO MUNICIPAL
CONTRATACIÓN	CONTRATACION PÚBLICA
INTERVENCIÓN	GESTIÓN PRESUPUESTARIA ECONÓMICA Y CONTABLE
GESTIÓN TRIBUTARIA	GESTIÓN DE INGRESOS PÚBLICOS
TESORERÍA	GESTIÓN PRESUPUESTARIA ECONÓMICA Y CONTABLE
PERSONAL	GESTIÓN DEL PERSONAL
VIVIENDA	PROMOCIÓN DE LA VIVIENDA GESTIÓN URBANISMO MUNICIPAL LICENCIAS, AUTORIZACIONES Y CONCESIONES
PARTICIPACIÓN CIUDADANA	GESTIÓN DE LA PARTICIPACIÓN CIUDADANA ATENCIÓN A LA CIUDADANÍA VOLUNTARIADO
INFORMÁTICA Y COMUNICACIONES	SERVICIOS TELEMÁTICOS Y COMUNICACIONES SISTEMAS DE INFORMACIÓN PROMOCIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA
JUVENTUD	GESTIÓN DE SERVICIOS JUVENILES MUNICIPALES AYUDAS Y SUBVENCIONES
SECRETARÍA MUNICIPAL	DEFENSA JURÍDICA Y RESPONSABILIDAD PATRIMONIAL GESTIÓN DE LOS ORGÁNOS MUNICIPALES DE GOBIERNO
ESTADÍSTICA	PADRÓN MUNICIPAL DE HABITANTES
CONSUMO	SERVICIOS DE CONSUMO PROCEDIMIENTOS SANCIONADORES

1.2. Valoración de servicios e información

El Responsable de Seguridad, contando con la opinión del Responsable del Sistema, ha realizado una propuesta de valoración inicial de los activos de Servicios e Información. Valoración que ha trasladado al/los Responsable/s de los Servicios y de la Información, para su valoración definitiva teniendo en cuenta la naturaleza de cada uno y la normativa que pudiera serle de aplicación.

Valoración de Servicios

Para valorar los Servicios, se ha tenido en cuenta:

- Que estos, como norma general, disponen de requisitos relevantes en términos de Disponibilidad [D].
- Que los requisitos de Confidencialidad [C], Integridad [I], Autenticidad [A] y Trazabilidad [T], se heredarán de los de la Información asociada al servicio correspondiente.
- Cuando un aspecto no requiere medidas de seguridad, en el apartado de valoración se indica: "Sin Valorar" [S].

CÓD.	SERVICIO	[C]	[I]	[D]	[A]	[T]
S 01	URBANISMO	-	-	[M]	-	-
S 02	MEDIO AMBIENTE	-	-	[B]	-	-
S 03	AGUAS, SANEAMIENTO Y RECOGIDA DE RESIDUOS			[B]		
S 04	MANTENIMIENTO E INFRAESTRUCTURAS	-	-	[B]	-	-
S 05	BIENESTAR SOCIAL	-	-	[M]	-	-
S 06	ACTUACIONES SOCIALES Y ATENCIÓN A LA DEPENDENCIA			[M]		
S 07	SEGURIDAD CIUDADANA Y PROTECCIÓN CIVIL	-	-	[M]	-	-
S 08	TRANSPORTE PÚBLICO			[M]		
S 09	SERVICIO DE EXTINCIÓN DE INCENDIOS			[M]		
S 10	PROMOCIÓN DE LA ENTIDAD LOCAL	-	-	[B]	-	-
S 11	COMERCIO Y MERCADOS	-	-	[B]	-	-
S 12	SERVICIOS FUNERARIOS	-	-	[M]	-	-
S 13	DEPORTES	-	-	[B]	-	-
S 14	CULTURA	-	-	[B]	-	-
S 15	EDUCACIÓN Y FORMACIÓN	-	-	[B]	-	-
S 16	ESCUELAS INFANTILES			[B]		
S 17	IGUALDAD	-	-	[B]	-	-
S 18	REGISTRO GENERAL	-	-	[M]	-	-
S 19	ARCHIVO	-	-	[M]	-	-
S 20	CONTRATACIÓN	-	-	[M]	-	-
S 21	PARTICIPACIÓN CIUDADANA	-	-	[B]	-	-

CÓD.	SERVICIO	[C]	[I]	[D]	[A]	[T]
S 22	INTERVENCIÓN	-	-	[M]	-	-
S 23	GESTIÓN TRIBUTARIA	-	-	[M]	-	-
S 24	TESORERÍA	-	-	[M]	-	-
S 25	PERSONAL	-	-	[M]	-	-
S 26	VIVIENDA	-	-	[M]	-	-
S 27	INFORMÁTICA Y COMUNICACIONES	-	-	[M]	-	-
S 28	JUVENTUD	-	-	[B]	-	-
S 29	SECRETARÍA MUNICIPAL			[M]		
S 30	ESTADÍSTICA			[M]		
S 31	CONSUMO			[B]		
	NIVEL MÁXIMO DE LOS SERVICIOS			**[M]**		

Justificación de la valoración de los Servicios

La justificación de la valoración de los Servicios se ha realizado en base a las consecuencias que tendría un incidente de seguridad en la dimensión de Disponibilidad [D], siendo la expuesta a continuación.

Se ha determinado que las consecuencias de un incidente de seguridad que afectará a la dimensión de **Disponibilidad [D]** de todos los Servicios, impidiendo que una persona autorizada pudiera acceder al servicio provocaría:

VALORACIÓN DE LOS SERVICIOS		[D]
SIN VALORAR	Cuando el RTO es superior a 5 días laborables Cuando la información es prescindible por tiempo indefinido.	
CAPACIDAD (Alcanzar sus objetivos)	Perjuicio muy grave [A] La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose	
	Perjuicio grave [M] Reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose	X
	Perjuicio limitado [B] Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	X
DAÑO ACTIVO (Protección del activo)	Perjuicio muy grave [A] El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	
	Perjuicio grave [M]	X

VALORACIÓN DE LOS SERVICIOS		[D]
	El sufrimiento de un daño significativo por los activos de la organización	
	Perjuicio limitado [B] El sufrimiento de un daño menor por los activos de la organización	X
CUMPLIMENTO SERVICIO (Obligaciones diarias del servicio)	Perjuicio muy grave [A] Anulada la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio grave [M] Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio limitado [B] Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
CUMPLIMIENTO LEY (Legislación vigente)	Perjuicio muy grave [A] El incumplimiento grave de alguna ley o regulación	
	Perjuicio grave [M] El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	X
	Perjuicio limitado [B] El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
CIUDADANIA (Respeto de los derechos de las personas)	Perjuicio muy grave [A] Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	
	Perjuicio grave [M] Causar un perjuicio significativo a algún individuo, de difícil reparación	X
	Perjuicio limitado [B] Causar un perjuicio menor a algún individuo, que aun siendo molesto, pueda ser fácilmente reparable	X
RTO (Tiempo de Recuperación del Servicio)	< 4 horas [A]	
	4 horas < RTO < 1 día [M]	X
	1 día < RTO < 5 días [B]	X

Valoración de la Información

Para valorar la Información se ha considerado que:

- La Información impone requisitos relevantes en las dimensiones de Confidencialidad [C], Integridad [I], Autenticidad [A] y Trazabilidad [T]. Los requisitos de disponibilidad se asocian a los Servicios que la tratan.
- El nivel de seguridad requerido en el aspecto de Confidencialidad [C] se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.
- El nivel de seguridad requerido en el aspecto de Integridad [I] se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.
- El nivel de seguridad requerido en el aspecto de Autenticidad [A] se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.
- El nivel de seguridad requerido en el aspecto de Trazabilidad [T] se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a, o modificado, una cierta información.
- Cuando un aspecto no requiere medidas de seguridad, en el apartado de valoración se indicará "Sin Valorar" [S].

Los niveles alcanzados para las dimensiones de Confidencialidad [C], Integridad [I], Autenticidad [A] y Trazabilidad [T], serían los siguientes:

ID	INFORMACIÓN	[C]	[I]	[D]	[A]	[T]
I 01	GESTIÓN URBANISMO MUNICIPAL	[B]	[M]	-	[M]	[M]
I 02	LICENCIAS, AUTORIZACIONES Y CONCESIONES	[B]	[M]	-	[M]	[M]
I 03	ATENCIÓN A LA CIUDADANÍA	[B]	[M]	-	[M]	[M]
I 04	GESTIÓN DEL CICLO DE AGUA Y RESIDUOS	[B]	[M]	-	[M]	[M]
I 05	GESTIÓN DE LAS OBRAS MANTENIMIENTO E INFRAESTRUCTURAS	[B]	[B]	-	[B]	[B]
I 06	PROMOCIÓN DE LA VIVIENDA	[M]	[M]		[M]	[M]
I 07	ATENCIONES Y PRESTACIONES SOCIALES	[M]	[M]	-	[M]	[M]
I 08	GESTIÓN DE LOS SISTEMAS DE ATENCIÓN A LA DEPENDENCIA Y OTRAS PRESTACIONES	[M]	[M]	-	[M]	[M]
I 09	AYUDAS Y SUBVENCIONES	[M]	[M]	-	[M]	[M]
I 10	POLICÍA LOCAL	[M]	[M]	-	[M]	[M]
I 11	PROTECCIÓN CIVIL	[M]	[M]	-	[M]	[M]
I 12	GESTIÓN DE LA MOVILIDAD URBANA	[B]	[B]	-	[B]	[B]
I 13	GESTIÓN DEL SERVICIO DE EXTINCIÓN DE INCENDIOS	[M]	[M]	-	[M]	[M]
I 14	PROCEDIMIENTOS SANCIONADORES	[M]	[M]	-	[M]	[M]

ID	INFORMACIÓN	[C]	[I]	[D]	[A]	[T]
I 15	SERVICIOS TELEMÁTICOS Y COMUNICACIONES	[M]	[M]	-	[M]	[M]
I 16	GESTIÓN DE SERVICIOS FUNERARIOS	[M]	[B]	-	[B]	[M]
I 17	GESTIÓN INGRESOS PÚBLICOS	[M]	[M]	-	[M]	[M]
I 18	GESTIÓN DE SERVICIOS DEPORTIVOS	[B]	[B]	-	[B]	[B]
I 19	GESTIÓN DE SERVICIOS CULTURALES	[B]	[B]	-	[B]	[B]
I 20	GESTIÓN DE SERVICIOS EDUCATIVOS	[M]	[M]	-	[M]	[M]
I 21	GESTIÓN DEL ARCHIVO MUNCIPAL	[M]	[M]	-	[M]	[M]
I 22	GESTIÓN DE LAS ESCUELAS INFANTILES	[M]	[M]	-	[M]	[M]
I 23	CONTRATACIÓN PÚBLICA	[B]	[M]	-	[M]	[M]
I 24	GESTIÓN DEL PERSONREAL	[M]	[M]	-	[M]	[M]
I 25	GESTIÓN PRESUPUESTARIA ECONÓMICA Y CONTABLE	[M]	[M]	-	[M]	[M]
I 26	GESTIÓN DE LOS ORGANISMOS MUNICIPALES DE GOBIERNO	[M]	[M]	-	[M]	[M]
I 27	PADRÓN MUNICIPAL DE HABITANTES	[M]	[M]	-	[M]	[M]
I 28	REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS	[M]	[M]	-	[M]	[M]
I 29	DEFENSA JURÍDICA Y RESPONSABILIDAD PATRIMONIAL	[M]	[M]	-	[M]	[M]
I 30	SEGURIDAD DE INSTALACIONES MUNICIPALES	[M]	[B]	-	[B]	[B]
I 31	GESTIÓN DE SERVICIOS JUVENILES MUNICIPALES	[B]	[B]	-	[B]	[B]
I 32	GESTIÓN DE LA PARTICIPACIÓN CIUDADANA	[B]	[B]	-	[B]	[B]
I 33	VOLUNTARIADO	[M]	[M]	-	[M]	[M]
I 34	GESTIÓN DE LAS OBRAS MANTENIMIENTO E INFRAESTRUCTURAS	[B]	[B]	-	[B]	[B]
I 35	GESTIÓN DE LA PROMOCIÓN LOCAL Y EL TURISMO	[B]	[B]	-	[B]	[B]
I 36	SERVICIOS DE CONSUMO	[B]	[B]	-	[B]	[B]
I 37	PROMOCIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA	[M]	[M]	-	[M]	[M]
I 38	SISTEMA DE INFORMACIÓN	[M]	[M]	-	[M]	[M]
	NIVEL MÁXIMO DE LA INFORMACIÓN	**[M]**	**[M]**	**-**	**[M]**	**[M]**

Justificación de la valoración de la Información

La justificación de la valoración otorgada en cada una de las dimensiones afectadas se ha realizado en base a las consecuencias que tendría un incidente de seguridad, siendo la expuesta a continuación.

Se ha determinado que las **consecuencias que tendría que un incidente de seguridad que afectará a la dimensión de Confidencialidad [C]** de la Información provocando su

revelación a personas no autorizadas o que no necesitan conocer la información, ocasionaría un:

VALORACIÓN DE LA INFORMACIÓN		[C]
SIN VALORAR	Perjuicio despreciable [S] Información de carácter público, accesible por cualquier persona.	X
CAPACIDAD (Alcanzar sus objetivos)	Perjuicio muy grave [A] La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose	
	Perjuicio grave [M] El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado [B] Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	X
DAÑO ACTIVO (Protección del activo)	Perjuicio muy grave [A] El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	
	Perjuicio grave [M] El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado [B] El sufrimiento de un daño menor por los activos de la organización	X
CUMPLIMENTO SERVICIO (Obligaciones diarias del servicio)	Perjuicio muy grave [A] Anulada la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio grave [M] Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio limitado [B] Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
CUMPLIMIENTO LEY	Perjuicio muy grave [A] El incumplimiento grave de alguna ley o regulación	
	Perjuicio grave [M]	X

VALORACIÓN DE LA INFORMACIÓN		[C]
(Legislación vigente)[1]	El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	
	Perjuicio limitado [B] El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
CIUDADANIA (Respeto de los derechos de las personas)	Perjuicio muy grave [A] Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	
	Perjuicio grave [M] Causar un perjuicio significativo a algún individuo, de difícil reparación	X
	Perjuicio limitado [B] Causar un perjuicio menor a algún individuo, que aun siendo molesto, pueda ser fácilmente reparable	X

Se ha determinado que las **consecuencias que tendría que un incidente de seguridad que afectará a la dimensión de Integridad [I]** de la Información provocando que pudiera ser modificada por alguien que no está autorizado, ocasionaría un:

VALORACIÓN DE LA INFORMACIÓN		[I]
SIN VALORAR	Perjuicio despreciable [S] Cuando los errores en su contenido carecen de consecuencias o son fácil o rápidamente reparables	
CAPACIDAD (Alcanzar sus objetivos)	Perjuicio muy grave [A] La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose	
	Perjuicio grave [M] El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado [B] Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	

[1] Entre otras normas de aplicación a la información, se ha tenido en cuenta el cumplimiento de la normativa de Protección de Datos Personales

VALORACIÓN DE LA INFORMACIÓN		[I]
DAÑO ACTIVO (Protección del activo)	Perjuicio muy grave [A] El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	
	Perjuicio grave [M] El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado [B] El sufrimiento de un daño menor por los activos de la organización	X
CUMPLIMENTO SERVICIO (Obligaciones diarias del servicio)	Perjuicio muy grave [A] Anulada la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio grave [M] Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio limitado [B] Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
CUMPLIMIENTO LEY (Legislación vigente)[2]	Perjuicio muy grave [A] El incumplimiento grave de alguna ley o regulación	
	Perjuicio grave [M] El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	X
	Perjuicio limitado [B] El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
CIUDADANIA (Respeto de los derechos de las personas)	Perjuicio muy grave [A] Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	
	Perjuicio grave [M] Causar un perjuicio significativo a algún individuo, de difícil reparación	X
	Perjuicio limitado [B] Causar un perjuicio menor a algún individuo, que aun siendo molesto, pueda ser fácilmente reparable	X

[2] Entre otras normas de aplicación a la información, se ha tenido en cuenta el cumplimiento de la normativa de Protección de Datos Personales

Se ha determinado que las consecuencias que tendría que un incidente de seguridad que afectará a la dimensión de Autenticidad [A] de la Información provocando que esta no sea autentica, ocasionaría un:

VALORACIÓN DE LA INFORMACIÓN		[A]
SIN VALORAR	Perjuicio despreciable [S] Cuando el origen es irrelevante o ampliamente conocido por otros medios. Cuando el destinatario es irrelevante, por ejemplo por tratarse de información de difusión anónima.	
CAPACIDAD (Alcanzar sus objetivos)	Perjuicio muy grave [A] La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose	
	Perjuicio grave [M] El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado [B] Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	X
DAÑO ACTIVO (Protección del activo)	Perjuicio muy grave [A] El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	
	Perjuicio grave [M] El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado [B] El sufrimiento de un daño menor por los activos de la organización	X
CUMPLIMENTO SERVICIO (Obligaciones diarias del servicio)	Perjuicio muy grave [A] Anulada la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio grave [M] Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio limitado [B] Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
CUMPLIMIENTO LEY	Perjuicio muy grave [A] El incumplimiento grave de alguna ley o regulación	

VALORACIÓN DE LA INFORMACIÓN		[A]
(Legislación vigente)[3]	Perjuicio grave [M] El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	X
	Perjuicio limitado [B] El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
CIUDADANIA (Respeto de los derechos de las personas)	Perjuicio muy grave [A] Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	
	Perjuicio grave [M] Causar un perjuicio significativo a algún individuo, de difícil reparación	X
	Perjuicio limitado [B] Causar un perjuicio menor a algún individuo, que aun siendo molesto, pueda ser fácilmente reparable	X

Se ha determinado que las **consecuencias que tendría que un incidente de seguridad que afectará a la dimensión de Trazabilidad [A]** de la Información impidiendo que se pueda rastrear a posteriori quien ha accedido o modificado cierta información, ocasionaría un:

VALORACIÓN DE LA INFORMACIÓN		[T]
SIN VALORAR	Perjuicio despreciable [S] Cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios. Cuando no se pueden perpetrar delitos relevantes, o su investigación es fácilmente realizable por otros medios	
CAPACIDAD (Alcanzar sus objetivos)	Perjuicio muy grave [A] La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose	
	Perjuicio grave [M] El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado [B]	X

[3] Entre otras normas de aplicación a la información, se ha tenido en cuenta el cumplimiento de la normativa de Protección de Datos Personales

VALORACIÓN DE LA INFORMACIÓN		[T]
	Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	
DAÑO ACTIVO (Protección del activo)	Perjuicio muy grave [A] El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	
	Perjuicio grave [M] El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado [B] El sufrimiento de un daño menor por los activos de la organización	X
CUMPLIMENTO SERVICIO (Obligaciones diarias del servicio)	Perjuicio muy grave [A] Anulada la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio grave [M] Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio limitado [B] Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
CUMPLIMIENTO LEY (Legislación vigente)[4]	Perjuicio muy grave [A] El incumplimiento grave de alguna ley o regulación	
	Perjuicio grave [M] El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	X
	Perjuicio limitado [B] El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
CIUDADANIA (Respeto de los derechos de las personas)	Perjuicio muy grave [A] Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	
	Perjuicio grave [M] Causar un perjuicio significativo a algún individuo, de difícil reparación	X

[4] Entre otras normas de aplicación a la información, se ha tenido en cuenta el cumplimiento de la normativa de Protección de Datos Personales

VALORACIÓN DE LA INFORMACIÓN		[T]
	Perjuicio limitado [B] Causar un perjuicio menor a algún individuo, que aun siendo molesto, pueda ser fácilmente reparable	X

2. CATEGORÍA DEL SISTEMA

El presente registro recoge la categorización del sistema del Ayuntamiento, realizada por el Responsable del Sistema, que ha determinado que la categoría del sistema que soporta los Servicios e Información, es MEDIA, tal y como se establece al determinar los niveles máximos alcanzados para los dichos activos. Los cuales se exponen a continuación.

SISTEMA DE INFORMACIÓN DEL AYUNTAMIENTO					
NIVELES MÁXIMOS	**[C]**	**[I]**	**[D]**	**[A]**	**[T]**
NIVEL MÁXIMO DE LOS SERVICIOS	[M]	[M]	[M]	[M]	[M]
NIVEL MÁXIMO DE LA INFORMACIÓN	[M]	[M]	[M]	[M]	[M]
NIVELES MÁXIMOS	**[M]**	**[M]**	**[M]**	**[M]**	**[M]**
CATEGORÍA MEDIA [C=M, I =M, D=M, A=M, T=M]					

ANEXO III INFORME DE ANÁLISIS DE RIESGOS Y ACEPTACIÓN DE RIESGOS RESIDUALES

ÍNDICE

Nota: en este apartado incluir los siguientes documentos aprobados por el /los Responsable/s de Servicios y el/los Responsable/s de Información

- Informe de Análisis de Riesgos
- Acta de aceptación de riesgos residuales

ANEXO IV DECLARACIÓN DE APLICABILIDAD

ÍNDICE

1. OBJETIVO

El presente documento tiene por objeto dar cumplimiento al "Artículo 27. Cumplimiento de requisitos mínimos", entre los cuales se establece:

[…]

4. La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de seguridad.

5. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de seguridad.

2. SELECCIÓN DE MEDIDAS DE SEGURIDAD

Para la selección de las medidas de seguridad se ha tenido en cuenta lo indicado en el Anexo II Medidas de seguridad en su apartado 2, donde se establece:

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

a) Identificación de los tipos de activos presentes.

b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.

c) Determinación del nivel correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.

d) Determinación de la categoría del sistema, según lo establecido en el Anexo I.

e) Selección de las medidas de seguridad apropiadas de entre las contenidas en este Anexo, de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.

Por tanto, para cada una de las medidas de seguridad, se indicará, las dimensiones de seguridad afectadas, su aplicación para nivel medio, según sea el caso, si aplica o no, con la justificación y el documento principal de referencia donde se explica cómo se encuentra implementada la medida. En caso, de utilizar medidas compensatorias se indicará en dicho campo.

3. DECLARACIÓN DE APLICABILIDAD

A continuación, se muestra la Declaración de Aplicabilidad de los sistemas de información propiedad del Ayuntamiento de _____.

Se establecen los siguientes supuestos:

- **Servicios alojados en el Ayuntamiento**, donde el Perfil de Cumplimiento Específico será de aplicación al sistema de información del Ayuntamiento.
- **Servicios del Ayuntamiento externalizados en la modalidad de software como servicio (SaaS)**. En este caso, será necesario que el sistema de información que soporta los servicios externalizados disponga de la conformidad en categoría MEDIA, siendo de aplicación el Perfil de Cumplimiento Específico al Sistema de Información del Ayuntamiento desde el que se accede a los servicios.

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
org	Marco organizativo									
org.1	Política de seguridad	Todas	aplica	=	=	MEDIO	Designación de roles de seguridad y constitución de Comité Política de Seguridad Plan de Adecuación (categorización, plan de mejora, etc.)	MEDIO	Documento de designación de roles de seguridad y constitución de Comité y de Política de seguridad Plan de Adecuación (categorización, plan de mejora, etc.)	Cubierto por Conformidad ENS
org.2	Normativa de seguridad	Todas	aplica	=	=	MEDIO	Normativa de Uso de Recursos y Accesos a Sistemas de Información Curso normativa	MEDIO	Normativa de Uso de Recursos y Accesos a Sistemas de Información Curso normativa	Cubierto por Conformidad ENS
org.3	Procedimientos de seguridad	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de la documentación Inventario de documentos Repositorio de procedimientos, instrucciones técnicas y registros.	MEDIO	Procedimiento de Gestión de la documentación Inventario de documentos Repositorio de procedimientos, instrucciones técnicas y registros.	Cubierto por Conformidad ENS
org.4	Proceso de autorización	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de Autorizaciones Herramienta evidencias	MEDIO	Procedimiento de Gestión Autorizaciones Herramienta evidencias	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op	Marco operacional									
op.pl	Planificación									
op.pl.1	Análisis de riesgos	Todas	aplica	+	++	MEDIO	Procedimiento de análisis de riesgos Archivo análisis de riesgos (PILAR) Informe de análisis de riesgos Acta de aceptación de riesgos	MEDIO	Procedimiento de análisis de riesgos Archivo análisis de riesgos (PILAR) Informe de análisis de riesgos Acta de aceptación de riesgos	Cubierto por Conformidad ENS
op.pl.2	Arquitectura de Seguridad	Todas	aplica	=	=	MEDIO	Esquemas de red físicos y lógicos Sistema de Gestión de Seguridad de la Información (SGSI)	MEDIO	Esquemas de red físicos y lógicos Sistema de Gestión de Seguridad de la Información (SGSI)	Cubierto por Conformidad ENS Documentación proporcionada por el proveedor sobre las comunicaciones con el Ayuntamiento, y con otros sistemas interconectados
op.pl.3	Adquisición de nuevos componentes	Todas	aplica	=	=	MEDIO	Procedimiento de adquisición de nuevos componentes Informes de estudios previos a la adquisición	MEDIO	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS
op.pl.4	Dimensionamiento/Gestión de capacidades	Todas	n/a	aplica	=	MEDIO*	Procedimiento de dimensiones y gestión de la capacidad Informes de estudio de dimensionamiento y gestión de la capacidad	n/a*.	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS Documentación regular proporcionada por el proveedor sobre los recursos disponibles y consumidos

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op.pl.5	Componentes certificados	Todas	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a
op.acc	Control de acceso									
op.acc.1	Identificación	A T	aplica	=	=	MEDIO	Procedimiento de control de acceso Herramienta solicitudes	MEDIO	Procedimiento de control de acceso Herramienta solicitudes	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el proveedor de configuración de los mecanismos de identificación de los usuarios en los servicios
op.acc.2	Requisitos de acceso	I C A T	aplica	=	=	MEDIO	Procedimiento de control de acceso Herramienta solicitudes	MEDIO	Procedimiento de control de acceso Herramienta solicitudes	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el proveedor de configuración de roles/perfiles de acceso a los servicios

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op.acc.3	Segregación de funciones y tareas	I C A T	n/a	aplica	=	MEDIO*	Procedimiento de control de acceso Herramienta solicitudes y evidencias Definición de medida compensatoria en caso de sea necesario	MEDIO*	Procedimiento de control de acceso Herramienta solicitudes y evidencias Definición de medida compensatoria en caso de sea necesario	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el proveedor de configuración de roles/perfiles de acceso a los servicios
op.acc.4	Protección de gestión de derechos de acceso	I C A T	aplica	=	=	MEDIO	Procedimiento de control de acceso Herramienta solicitudes Evidencias de revisiones de accesos	MEDIO	Procedimiento de control de acceso Herramienta solicitudes Evidencias de revisiones de accesos	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el proveedor de configuración de roles/perfiles de acceso a los servicios
op.acc.5	Mecanismo de autenticación	I C A T	aplica	+	++	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de bastionado de dominio y de aplicaciones	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de bastionado de dominio y de aplicaciones	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el proveedor de los mecanismo de autenticación de acceso a los servicios

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op.acc.6	Acceso local (local logon)	I C A T	aplica	+	++	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de bastionado de dominio y de aplicaciones	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de bastionado de dominio y de aplicaciones	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el proveedor de configuración de los requisitos del control: limitación de intentos de acceso, aviso de obligaciones, información sobre el último acceso
op.acc.7	Acceso remoto (remote login)	I C A T	aplica	+	=	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de configuración de acceso remoto	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de configuración de acceso remoto	Cubierto por Conformidad ENS
op.exp	Explotación									
op.exp.1	Inventario de activos	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de activos Herramienta de inventario de activos	MEDIO	Procedimiento de Gestión de activos Herramienta de inventario de activos	Cubierto por Conformidad ENS
op.exp.2	Configuración de seguridad	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de la Configuración Instrucciones Técnicas de bastionado equipamiento, máquinas virtuales Informes CLARA Informes ROCIO	MEDIO	Procedimiento de Gestión de la Configuración Instrucciones Técnicas de bastionado equipamiento, máquinas virtuales Informes CLARA Informes ROCIO	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op.exp.3	Gestión de la configuración de seguridad	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de la Configuración Herramienta solicitudes y evidencias	MEDIO	Procedimiento de Gestión de la Configuración Herramienta solicitudes y evidencias	Cubierto por Conformidad ENS
op.exp.4	Mantenimiento	Todas	aplica	=	=	MEDIO	Procedimiento de mantenimiento Herramienta de solicitudes y evidencias	MEDIO	Procedimiento de mantenimiento Herramienta de solicitudes y evidencias	Cubierto por Conformidad ENS Procedimientos documentados de coordinación con el Ayuntamiento para realizar acciones de mantenimiento sobre el sistema que soportan los servicios
op.exp.5	Gestión de cambios	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de cambios Herramienta de solicitudes y evidencias	MEDIO	Procedimiento de Gestión de cambios Herramienta de solicitudes y evidencias	Cubierto por Conformidad ENS Procedimientos documentados de coordinación con el Ayuntamiento para realizar cambios sobre el sistema que soporta los servicios
op.exp.6	Protección frente a código dañino	Todas	aplica	=	=	MEDIO	Procedimiento de Protección frente a Código dañino Consola antivirus e informes	MEDIO	Procedimiento de Protección frente a Código dañino Consola antivirus e informes	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op.exp.7	Gestión de incidentes	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de Incidentes Procedimiento de Gestión de Brechas de Seguridad Informes de incidentes Herramienta interna gestión incidencias Herramienta LUCIA	MEDIO	Procedimiento de Gestión de Incidentes Procedimiento de Gestión de Brechas de Seguridad Informes de incidentes Herramienta interna gestión incidencias	Cubierto por Conformidad ENS Procedimientos documentados de coordinación con el Ayuntamiento para la gestión incidentes y de comunicación de los mismos autoridades de control
op.exp.8	Registro de la actividad de los usuarios	Todas	aplica	+	++	MEDIO	Procedimiento de Gestión de logs. Registros de actividad Informes de revisión	MEDIO	Registros de actividad Informes de revisión Sistema proveedor que soporta los servicios cubierto por Conformidad ENS y Procedimientos de Gestión de logs.	Cubierto por Conformidad ENS Procedimientos documentados de configuración de los registros de actividad de los usuarios a los servicios Información/plataforma de visualización proporcionada por el proveedor de los accesos de los administradores del sistema que soporta los servicios (en caso de que se hayan requerido)

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op.exp.9	Registro de la gestión de incidentes	Todas	n/a	aplica	aplica	MEDIO	Procedimiento de Gestión de Incidentes Procedimiento de Gestión de Brechas de Seguridad Informes de incidentes Herramienta interna gestión incidencias Herramienta LUCIA	MEDIO	Procedimiento de Gestión de Incidentes Procedimiento de Gestión de Brechas de Seguridad Informes de incidentes Herramienta interna gestión incidencias	Cubierto por Conformidad ENS Procedimientos documentados de coordinación con el Ayuntamiento para la gestión incidentes y de comunicación de los mismos autoridades de control
op.exp.10	Protección de los registro de actividad	T	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a
op.exp.11	Protección de claves criptográficas	Todas	aplica	+	=	MEDIO	Procedimiento de Protección de Claves Criptográficas	MEDIO	Procedimiento de Protección de Claves Criptográficas	Cubierto por Conformidad ENS Procedimientos documentados de protección de las claves criptográficas del Ayuntamiento que se encuentren alojadas en el sistema que soporta los servicios

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op.ext	Servicios externos									
op.ext.1	Contratación y acuerdos de nivel de servicio	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de Servicios Externos Clausulado de seguridad (confidencialidad, conformidad, ENS, comunicación incidente, etc.) pliegos Contratos y SLAs proveedores Certificados Conformidad ENS proveedores relacionados con el alcance	MEDIO	Procedimiento de Gestión de Servicios Externos Clausulado de seguridad (confidencialidad, conformidad, ENS, comunicación incidente, etc.) pliegos Contratos y SLAs Certificados Conformidad ENS servicios externalizados y de otros proveedores relacionados con el alcance	Cubierto por Conformidad ENS Certificados de Conformidad ENS de los servicios subcontratados por el proveedor
op.ext.2	Gestión diaria	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de Servicios Externos Informes de revisión de SLA	MEDIO	Procedimiento de Gestión de Servicios Externos Informes de revisión de SLA	Cubierto por Conformidad ENS Informes/herramientas seguimiento SLA proporcionadas por el proveedor
op.ext.9	Medios alternativos	Todas	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a
op.cont	Continuidad del servicio									
op.cont.1	Análisis de impacto	D	n/a	aplica	=	MEDIO	Procedimiento de Análisis de Impacto Informe de Análisis de Impacto	MEDIO	Procedimiento de Análisis de Impacto Informe de Análisis de Impacto	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op.cont.2	Plan de continuidad	D	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a
op.cont.3	Pruebas periódicas	D	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a
op.mon	Monitorización del sistema									
op.mon.1	Detección de intrusión	Todas	n/a	aplica	=	MEDIO	Procedimiento de Detección de Intrusión Herramientas IDS	MEDIO	Procedimiento de Detección de Intrusión Herramientas IDS	Cubierto por Conformidad ENS
op.mon.2	Sistema de métricas	Todas	aplica	+	++	MEDIO	Procedimiento de Métricas e Indicadores Registro de métricas e indicadores Registro de IM e IC	MEDIO	Procedimiento de Métricas e Indicadores Registro de métricas e indicadores Registro de IM e IC	Cubierto por Conformidad ENS
mp	Medidas de protección									
mp.if	Protección de las instalaciones e infraestructuras									
mp.if.1	Áreas separadas y con control de acceso	Todas	aplica	=	=	MEDIO	Procedimiento de Protección de las Instalaciones Planos instalaciones e infraestructuras	MEDIO	Procedimiento de Protección de las Instalaciones Planos instalaciones e infraestructuras	Cubierto por Conformidad ENS
mp.if.2	Identificación de las personas	Todas	aplica	=	=	MEDIO	Procedimiento de Protección de las Instalaciones Registros de los accesos Informes de revisión de los accesos	MEDIO	Procedimiento de Protección de las Instalaciones Registros de los accesos Informes de revisión de los accesos	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.if.3	Acondicionamiento de los locales	Todas	aplica	=	=	MEDIO	Procedimiento de Protección de las Instalaciones Herramientas sensores temperaturas e humedad Revisiones mantenimientos	MEDIO	Procedimiento de Protección de las Instalaciones Herramientas sensores temperaturas e humedad Revisiones mantenimientos	Cubierto por Conformidad ENS
mp.if.4	Energía eléctrica	D	aplica	+	=	MEDIO	Procedimiento de Protección de las Instalaciones Revisiones de SAI Revisiones mantenimientos Informes pruebas de capacidad	BAJO	Procedimiento de Protección de las Instalaciones Revisiones mantenimientos	Cubierto por Conformidad ENS
mp.if.5	Protección frente a incendios	D	aplica	=	=	MEDIO	Procedimiento de Protección de las Instalaciones Documentación medidas de prevención y extinción de incendios Revisiones de mantenimiento	MEDIO	Procedimiento de Protección de las Instalaciones Documentación medidas de prevención y extinción de incendios Revisiones de mantenimiento	Cubierto por Conformidad ENS
mp.if.6	Protección frente a inundaciones	D	n/a	aplica	=	MEDIO*	Procedimiento de Protección de las Instalaciones Documentación medidas de protección frente a inundaciones Revisiones de mantenimiento	n/a*	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.if.7	Registro de entrada y salida de equipamiento	Todas	aplica	=	=	MEDIO	Procedimiento de Registro Entrada/Salida de equipamiento Herramienta evidencias entrada y salida de equipamiento	MEDIO	Procedimiento de Registro Entrada/Salida de equipamiento Herramienta evidencias entrada y salida de equipamiento	Cubierto por Conformidad ENS
mp.if.9	Instalaciones alternativas	Todas	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	
mp.per	Gestión del personal									
mp.per.1	Caracterización del puesto de trabajo	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de Personal Relación de Puestos de Trabajo (RPT) Fichas perfiles puesto de trabajo Designación de roles y designación como miembros del Comité	MEDIO	Procedimiento de Gestión de Personal Relación de Puestos de Trabajo (RPT) Fichas perfiles puesto de trabajo Designación de roles y designación como miembros del Comité	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.per.2	Deberes y obligaciones	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de Personal Política de Seguridad Normativa de Uso de Recursos y Accesos a Sistemas de Información Acuerdos de confidencialidad personal propio Acuerdos de confidencialidad con empresas proveedoras, en caso de personal ajeno trabajando en las instalaciones	MEDIO	Procedimiento de Gestión de Personal Política de Seguridad Normativa de Uso de Recursos y Accesos a Sistemas de Información Acuerdos de confidencialidad personal propio Acuerdos de confidencialidad con empresas proveedoras, en caso de personal ajeno trabajando en las instalaciones	Cubierto por Conformidad ENS
mp.per.3	Concienciación	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de Personal Plan de concienciación anual Cartelería/fondos de pantalla/cursos online	MEDIO	Procedimiento de Gestión de Personal Plan de concienciación anual	Cubierto por Conformidad ENS
mp.per.4	Formación	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de Personal Plan de formación anual Plataforma Vanesa Cursos online CCN	MEDIO	Procedimiento de Gestión de Personal Plan de concienciación anual Plataforma Vanesa Cursos online CCN	Cubierto por Conformidad ENS
mp.per.9	Personal alternativo	D	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.eq	Protección de los equipos									
mp.eq.1	Puesto de trabajo despejado	Todas	aplica	+	=	MEDIO	Procedimiento de Protección de los Equipos Normativa de Uso de Recursos y Accesos a Sistemas de Información	MEDIO	Procedimiento de Protección de los Equipos Normativa de Uso de Recursos y Accesos a Sistemas de Información	Cubierto por Conformidad ENS
mp.eq.2	Bloqueo de puesto de trabajo	A	n/a	aplica	+	MEDIO	Procedimiento de Protección de los Equipos Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de bastionado de dominio	MEDIO	Procedimiento de Protección de los Equipos Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de bastionado de dominio	Cubierto por Conformidad ENS
mp.eq.3	Protección de equipos portátiles	Todas	aplica	=	+	MEDIO	Procedimiento de Protección de los Equipos y equipamiento de red Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de bastionado de equipos portátiles Procedimiento de Autorización Procedimiento de Gestión de Activos Herramienta Inventario de Activos Herramienta Evidencias	MEDIO	Procedimiento de Protección de los Equipos y equipamiento de red Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de bastionado de equipos portátiles Procedimiento de Autorización Procedimiento de Gestión de Activos Herramienta Inventario de Activos Herramienta Evidencias	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.eq.9	Medios alternativos	D	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	
mp.com	Protección de las comunicaciones									
mp.com.1	Perímetro seguro	Todas	aplica	=	+	MEDIO	Procedimiento de Protección de las Comunicaciones Herramienta evidencias	MEDIO	Procedimiento de Protección de las Comunicaciones Herramienta evidencias	Cubierto por Conformidad ENS
mp.com.2	Protección de la confidencialidad	C	n/a	+	++	MEDIO	Procedimiento de Protección de las Comunicaciones	MEDIO	Procedimiento de Protección de las Comunicaciones	Cubierto por Conformidad ENS Documentos proporcionados por el proveedor con información sobre los mecanismos de cifrado implementados en las comunicaciones
mp.com.3	Protección de la autenticidad y de la integridad	I A	aplica	+	++	MEDIO	Procedimiento de Protección de las Comunicaciones	MEDIO	Procedimiento de Protección de las Comunicaciones	Cubierto por Conformidad ENS Documentos proporcionados por el proveedor con información sobre los mecanismos implementados para proteger la autenticidad y de la integridad
mp.com.4	Separación de redes	Todas	n/a	n/a	aplica	ALTO*	Procedimiento de segmentación de redes Esquemas de red	ALTO*	Procedimiento de segmentación de redes Esquemas de red	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.com.9	Medios alternativos	Todas	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	
mp.si	Protección de los soportes de información									
mp.si.1	Etiquetado	C	aplica	=	=	(n/a/ MEDIO) *	Cuando sea de aplicación: Procedimiento de Gestión de Soportes de Información Procedimiento de Marcado de Soportes Normativa de Uso de Recursos y Accesos a Sistemas de Información Procedimiento de Autorización Herramienta Evidencias	(n/a/ MEDIO) *	Procedimiento de Gestión de Soportes de Información Procedimiento de Marcado de Soportes Normativa de Uso de Recursos y Accesos a Sistemas de Información Herramienta Evidencias	Cubierto por Conformidad ENS
mp.si.2	Criptografía	I C	n/a	aplica	+	(n/a/ MEDIO) *	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de Criptografía	(n/a/ MEDIO) *	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de Criptografía	Cubierto por Conformidad ENS
mp.si.3	Custodia	Todas	aplica	=	=	(n/a/ MEDIO) *	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información	(n/a/ MEDIO) *	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.si.4	Transporte	Todas	aplica	=	=	(n/a/ MEDIO) *	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Registro entrada/salida de soportes	(n/a/ MEDIO) *	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Registro entrada/salida de soportes	Cubierto por Conformidad ENS
mp.si.5	Borrado y destrucción	D	aplica	+	=	MEDIO*	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de borrado de soportes	MEDIO*	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de borrado de soportes	Cubierto por Conformidad ENS
mp.sw	Protección de las aplicaciones informáticas									
mp.sw.1	Desarrollo de aplicaciones	Todas	n/a	aplica	=	MEDIO*	Procedimiento de Desarrollo Seguro Herramientas de desarrollo	n/a*	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.sw.2	Aceptación y puesta en servicio	Todas	aplica	+	++	MEDIO*	Procedimiento de Aceptación y Puesta en Servicio Plan de Pruebas- Informe resultados	n/a*	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el proveedor de coordinación con el Ayuntamiento para la realización de pruebas de aceptación y puesta en servicio. Informes resultados pruebas y plan de acción
mp.info	Protección de la información									
mp.info.1	Datos de carácter personal	Todas	aplica	=	=	MEDIO	Registro de Actividades de Tratamiento (RAT) Delegado de Protección de Datos Análisis de Riesgo RGPD Evaluaciones de Impacto (EIPD) Regulación de la recogida de datos Regulación de terceros. Contratos de Encargado del Tratamiento. Deber de Diligencia	MEDIO	Registro de Actividades de Tratamiento (RAT) Delegado de Protección de Datos Análisis de Riesgo RGPD Evaluaciones de Impacto Regulación de la recogida de datos Regulación de terceros. Contratos de Encargado del Tratamiento. Deber de Diligencia	Cubierto por Conformidad ENS Documentos /plataformas online, proporcionados por el proveedor, con evidencias de cumplimiento de la normativa de protección de datos

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.info.2	Calificación de la información	C	aplica	+	=	MEDIO	Procedimiento de Calificación de la Información	MEDIO	Procedimiento de Calificación de la Información	Cubierto por Conformidad ENS
mp.info.3	Cifrado	C	n/a	n/a	+	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	
mp.info.4	Firma electrónica	I A	aplica	+	++	(n/a/ BAJO/ MEDIO) *	Cuando sea de aplicación: Procedimiento de Firma Electrónica Política de firma electrónica y certificados	(n/a/ BAJO/ MEDIO) *	Cuando sea de aplicación: Procedimiento de Firma Electrónica Política de firma electrónica y certificados	Cubierto por Conformidad ENS Documentos proporcionados por el proveedor con información sobre las medidas de protección de la firma implementadas
mp.info.5	Sellos de tiempo	T	n/a	n/a	aplica	ALTO*	Procedimiento de Sellado de Tiempo	ALTO*	Procedimiento de Sellado de Tiempo	Cubierto por Conformidad ENS Documentos proporcionados por el proveedor con información sobre las medidas de seguridad implementadas para proteger el sello de tiempo
mp.info.6	Limpieza de documentos	C	aplica	=	=	MEDIO	Normativa de Limpieza de Metadatos Instrucción Técnica de Limpieza de Metadatos	MEDIO	Normativa de Limpieza de Metadatos Instrucción Técnica de Limpieza de Metadatos	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.info.9	Copias de seguridad (backup)	D	aplica	=	=	MEDIO*	Procedimiento de copias de respaldo y pruebas de restauración	MEDIO*	Procedimiento de copias de respaldo y de restauración (si se tiene información en local en el sistema del Ayuntamiento)	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el proveedor de la política de copias de seguridad y de restauración
mp.s	Protección de los servicios									
mp.s.1	Protección del correo electrónico	Todas	aplica	=	=	MEDIO*	Procedimiento de Protección del Correo Electrónico Instrucción Técnica de Bastionado del Correo Electrónico (si lo provee proveedor externo solicitar conformidad con el ENS en categoría MEDIA y procedimiento de configuración del correo)	MEDIO*	Procedimiento de Protección del Correo Electrónico Instrucción Técnica de Bastionado del Correo Electrónico (si lo provee proveedor externo solicitar conformidad con el ENS en categoría MEDIA y procedimiento de configuración del correo)	n/a
mp.s.2	Protección de servicios y aplicaciones web	Todas	aplica	=	+	MEDIO*	Procedimiento de Protección de los Servicios y Aplicaciones Web Instrucción Técnica de Bastionado de Servicios Web	n/a*	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS Informes proporcionados por el proveedor con resultados de las inspecciones periódicas realizadas y plan de acción

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.s.8	Protección frente a denegación de servicio	D	n/a	aplica	+	MEDIO*	Procedimiento de protección frente a la denegación de servicio Instrucción técnica de bastionado de las tecnologías desplegadas para protegerse de la denegación de servicio	n/a*	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS
mp.s.9	Medios alternativos	D	n/a	n/a	+	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a

ANEXO V PLAN DE MEJORA DE LA SEGURIDAD

ÍNDICE

1. INFORME DE INSUFICIENCIAS

A continuación, se muestra el grado de cumplimiento de las medidas del Anexo II del Real Decreto ENS, a fecha [INDICAR FECHA]

Las medidas se han evaluado conforme a la escala CMM:

CMM	DESCRIPCIÓN	EFECTIVIDAD
L0	Inexistente	0%
L1	Inicial / Ad hoc	10%
L2	Reproducible, pero intuitivo	50%
L3	Proceso definido	80%
L4	Gestionado y medible	90%
L5	Optimizado	100%

Se establecen los siguientes supuestos:

- **Servicios alojados en el Ayuntamiento**, donde el Perfil de Cumplimiento Específico será de aplicación al sistema de información del Ayuntamiento.
- **Servicios del Ayuntamiento externalizados en la modalidad de software como servicio (SaaS)**. En este caso, será necesario que el sistema de información que soporta los servicios externalizados disponga de la conformidad en categoría MEDIA, siendo de aplicación el Perfil de Cumplimiento Específico al Sistema de Información del Ayuntamiento desde el que se accede a los servicios.

		SERVICIO AYUNTAMIENTO		SERVICIO DEL AYUNTAMIENTO EXTERNALIZADO		
Medidas de Seguridad		APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	SISTEMA EXTERNALIZADO NIVEL DE MADUREZ ALCANZADO
org.1	Política de seguridad	MEDIO	L0	MEDIO	L0	L3[5]
org.2	Normativa de seguridad	MEDIO	L1	MEDIO	L1	L3
org.3	Procedimientos de seguridad	MEDIO	L1	MEDIO	L1	L3
org.4	Proceso de autorización	MEDIO	L0	MEDIO	L0	L3
op.pl.1	Análisis de riesgos	MEDIO	L0	MEDIO	L0	L3
op.pl.2	Arquitectura de Seguridad	MEDIO	L1	MEDIO	L1	L3
op.pl.3	Adquisición de nuevos componentes	MEDIO*	L1	n/a*	-	L3

[5] L3 en todos los controles, si el sistema dispone de la conformidad ENS en categoría MEDIA

Medidas de Seguridad		SERVICIO AYUNTAMIENTO		SERVICIO DEL AYUNTAMIENTO EXTERNALIZADO		
		APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	SISTEMA EXTERNALIZADO NIVEL DE MADUREZ ALCANZADO
op.pl.4	Dimensionamiento/Gestión de capacidades	MEDIO*	L1	n/a*	-	L3
op.pl.5	Componentes certificados	n/a	-	n/a	-	
op.acc.1	Identificación	MEDIO	L1	MEDIO	L1	L3
op.acc.2	Requisitos de acceso	MEDIO	L1	MEDIO	L1	L3
op.acc.3	Segregación de funciones y tareas	MEDIO*	L0	MEDIO*	L0	L3
op.acc.4	Protección de gestión de derechos de acceso	MEDIO	L1	MEDIO	L1	L3
op.acc.5	Mecanismo de autenticación	MEDIO	L1	MEDIO	L1	L3
op.acc.6	Acceso local (local logon)	MEDIO	L1	MEDIO	L1	L3
op.acc.7	Acceso remoto (remote login)	MEDIO	L1	MEDIO	L1	L3
op.exp.1	Inventario de activos	MEDIO	L2	MEDIO	L2	L3
op.exp.2	Configuración de seguridad	MEDIO	L1	MEDIO	L1	L3
op.exp.3	Gestión de la configuración de seguridad	BAJO	L1	BAJO	L1	L3
op.exp.4	Mantenimiento	MEDIO	L1	MEDIO	L1	L3
op.exp.5	Gestión de cambios	MEDIO	L1	MEDIO	L1	L3
op.exp.6	Protección frente a código dañino	MEDIO	L2	MEDIO	L2	L3
op.exp.7	Gestión de incidentes	MEDIO	L1	MEDIO	L1	L3
op.exp.8	Registro de la actividad de los usuarios	MEDIO	L1	MEDIO	L1	L3
op.exp.9	Registro de la gestión de incidentes	MEDIO	L1	MEDIO	L1	L3
op.exp.10	Protección de los registros de actividad	n/a	-	n/a	-	
op.exp.11	Protección de claves criptográficas	MEDIO	L1	MEDIO	L1	L3
op.ext.1	Contratación y acuerdos de nivel de servicio	MEDIO	L1	MEDIO	L1	L3
op.ext.2	Gestión diaria	MEDIO	L0	MEDIO	L0	L3
op.ext.9	Medios alternativos	n/a	-	n/a	-	
op.cont.1	Análisis de impacto	MEDIO	L1	MEDIO	L1	L3
op.cont.2	Plan de continuidad	n/a	-	n/a	-	
op.cont.3	Pruebas periódicas	n/a	-	n/a	-	
op.mon.1	Detección de intrusión	MEDIO	L1	MEDIO	L1	L3
op.mon.2	Sistema de métricas	MEDIO	L1	MEDIO	L1	L3
mp.if.1	Áreas separadas y con control de acceso	MEDIO	L2	MEDIO	L2	L3
mp.if.2	Identificación de las personas	MEDIO	L1	MEDIO	L1	L3

Medidas de Seguridad		SERVICIO AYUNTAMIENTO		SERVICIO DEL AYUNTAMIENTO EXTERNALIZADO		
		APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	SISTEMA EXTERNALIZADO NIVEL DE MADUREZ ALCANZADO
mp.if.3	Acondicionamiento de los locales	MEDIO	L1	MEDIO	L1	L3
mp.if.4	Energía eléctrica	MEDIO	L2	BAJO	L2	L3
mp.if.5	Protección frente a incendios	MEDIO	L2	MEDIO	L2	L3
mp.if.6	Protección frente a inundaciones	MEDIO*	L2	n/a*	-	L3
mp.if.7	Registro de entrada y salida de equipamiento	MEDIO	L0	MEDIO	L0	L3
mp.per.1	Caracterización del puesto de trabajo	MEDIO	L1	MEDIO	L1	L3
mp.per.2	Deberes y obligaciones	MEDIO	L1	MEDIO	L1	L3
mp.per.3	Concienciación	MEDIO	L0	MEDIO	L0	L3
mp.per.4	Formación	MEDIO	L0	MEDIO	L0	L3
mp.per.9	Personal alternativo	n/a	-	n/a	-	
mp.eq.1	Puesto de trabajo despejado	MEDIO	L0	MEDIO	L0	L3
mp.eq.2	Bloqueo de puesto de trabajo	MEDIO	L0	MEDIO	L0	L3
mp.eq.3	Protección de dispositivos portátiles	MEDIO	L1	MEDIO	L1	L3
mp.eq.9	Medios alternativos	n/a	-	n/a	-	
mp.com.1	Perímetro seguro	MEDIO	L2	MEDIO	L2	L3
mp.com.2	Protección de la confidencialidad	MEDIO	L1	MEDIO	L1	L3
mp.com.3	Protección de la autenticidad y de la integridad	MEDIO	L1	MEDIO	L1	L3
mp.com.4	Separación de redes	ALTO*	L1	ALTO*	L1	L3-L4
mp.com.9	Medios alternativos	n/a	-	n/a	-	
mp.si.1	Etiquetado	MEDIO*	L0	MEDIO*	L0	L3
mp.si.2	Criptografía	MEDIO*	L0	MEDIO*	L0	L3
mp.si.3	Custodia	MEDIO*	L0	MEDIO*	L0	L3
mp.si.4	Transporte	MEDIO*	L0	MEDIO*	L0	L3
mp.si.5	Borrado y destrucción	MEDIO*	L0	MEDIO*	L0	L3
mp.sw.1	Desarrollo de aplicaciones	MEDIO*	L0	n/a*	-	L3
mp.sw.2	Aceptación y puesta en servicio	MEDIO*	L1	n/a*	-	L3
mp.info.1	Datos de carácter personal	MEDIO	L1	MEDIO	L1	L3
mp.info.2	Calificación de la información	MEDIO	L0	MEDIO	L0	L3
mp.info.3	Cifrado	n/a	-	n/a	-	
mp.info.4	Firma electrónica	(n/a, BAJO, MEDIO)*	L1	(n/a, BAJO, MEDIO)*	L1	L3

Medidas de Seguridad		SERVICIO AYUNTAMIENTO		SERVICIO DEL AYUNTAMIENTO EXTERNALIZADO		
		APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	SISTEMA EXTERNALIZADO NIVEL DE MADUREZ ALCANZADO
mp.info.5	Sellos de tiempo	ALTO*	L2	ALTO*	L2	L3
mp.info.6	Limpieza de documentos	MEDIO	L0	MEDIO	L0	L3
mp.info.9	Copias de seguridad	MEDIO	L2	MEDIO*	L2	L3
mp.s.1	Protección del correo electrónico	MEDIO*	L2	MEDIO*	L2	L3
mp.s.2	Protección de servicios y aplicaciones web	MEDIO*	L1	n/a*	-	L3
mp.s.8	Protección frente a denegación de servicio	MEDIO*	L2	n/a*	-	L3
mp.s.9	Medios alternativos	n/a	-	n/a	-	

2. PLAN DE MEJORA DE LA SEGURIDAD

2.1. OBJETO DEL DOCUMENTO

El propósito de este documento es proponer un plan de medidas de seguridad ("Plan de Mejora de la Seguridad) a llevar a cabo para subsanar las desviaciones de cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad.

La responsabilidad de su ejecución y la provisión de recursos recaen sobre el Ayuntamiento de _____, ya sean propios o mediante externalización. El RSEG se encargará de la supervisión de su ejecución. Las tareas realizar se organizan en tres grupos:

- **Tareas priorizadas:** tareas que se deben abordar inicialmente, ya sea fruto del análisis de riesgos, o porque presentan un cumplimiento muy bajo, o por tratarse de un incumplimiento normativo.
- **Tareas de implantación ENS:** resto de tareas que es necesario llevar a cabo para realizar la implantación efectiva del ENS. Para ello, se irán revisando/implantando y documentando, las medidas de seguridad, siguiendo el orden establecido en el anexo II del Real Decreto ENS. De esta manera, se va implantado el Sistema de Gestión que dará cumplimiento a estas medidas.
- **Tareas periódicas:** tareas para llevar a cabo aquellas medidas de seguridad que se deben realizar de forma periódica.

2.2. PLAN DE MEJORA DE LA SEGURIDAD

Tareas prioritarias

Leyenda: RINF (Responsable/s de Información); RSER (Responsable del/de los Servicio/s); RSEG (Responsable de Seguridad); RSIS (Responsable del Sistema); CSI (Comité de Seguridad de la Información); T (Trimestre); RESPONSABLE (Responsable de que la tarea se lleve a cabo)

Las siguientes tareas se abordarán de forma prioritaria, son las que se exponen a continuación.

TAREAS PRIORITARIAS	CONTROL/CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Desarrollar la Política de seguridad (pertenece al plan de adecuación): designación de roles de seguridad y constituir el CSI. Publicar en el Boletín Oficial de la Provincia, sede electrónica/portales internos vinculados con la difusión de iniciativas de seguridad.	Política de seguridad de la Información [org.1]	CSI	X			
Categorizar el sistema (pertenece al plan de adecuación): realizar y aprobar la valoración de los Servicios y la Información. Determinar la categoría del sistema	Artículo 43. Categorías y 44. Facultades del Real Decreto ENS	RINF, RSER/RSIS	X			
Realizar el Análisis de Riesgos (pertenece al plan de adecuación) informes asociados y aceptar los riesgos residuales	Análisis de riesgos [op.pl.1]	RSINF, RSER,RSEG,RSIS	X			
Realizar la Declaración de aplicabilidad (pertenece al plan de adecuación)	Artículo 27. Cumplimiento de requisitos mínimos. 2. Selección de medidas de seguridad - ANEXO II Medidas de seguridad	RSEG	X			
Realizar al Informe de Insuficiencias (pertenece al plan de adecuación) y el Plan de mejora de la seguridad	Disposición transitoria. *Adecuación de sistemas*	RSEG,RSIS/CSI	X			

TAREAS PRIORITARIAS	CONTROL/CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Desarrollar y aprobar la normativa de seguridad de los recursos TIC (correo, internet, etc.) puestos a disposición del personal que regule también, entre otros, el uso de dispositivos portátiles, soportes extraíbles, la necesidad de que los usuarios bloqueen su puesto de trabajo ante las ausencias, la necesidad de limpiar los documentos de metadatos no necesarios, etc. Aprobar formalmente y difundir a todo personal: publicación en el portal del empleado. Elaborar de plan anual de difusión/sensibilización y de formación.	Normativa de seguridad [org.2] Puesto de trabajo despejado [mp.eq.1] Bloqueo de puesto de trabajo [mp.eq.2] Protección de dispositivos portátiles [mp.eq.3] Protección de los soportes [mp.si] Limpieza de metadatos [mp.info.6] Concienciación [mp.per.3] Formación [mp.per.4]	RSEG/CSI	X	X		
Desarrollar e implantar un procedimiento de gestión de la seguridad con terceros: antes, durante y después de la contratación: Requisitos de solvencia técnica. Exigencia de declaración/certificación de conformidad con el ENS, contratos de encargado del tratamiento de datos personales y/o confidencialidad, acuerdos de nivel de servicio, etc. Inventariar terceros y regular su situación. En caso de servicios externalizados: completar con certificados de Conformidad ENS de los servicios subcontratados por el proveedor. Para la gestión diaria completar con los Informes/herramientas seguimiento SLA proporcionadas por el proveedor	Contratación y acuerdos de nivel de servicio [op.ext.1] Gestión diaria [op.ext.2]	CSI	X	X		
Revisar las medidas de protección frente a código dañino, en todo el equipamiento incluido: el de las sedes, portátiles, etc. Se recomienda implementar soluciones medidas EDR (Endpoint Defense and Response) Desarrollar un procedimiento que describa la forma en cual se gestiona y se mantiene la solución de protección frente a código dañino	Protección frente a código dañino [op.exp.6]	RSIS	X			
Segmentar las redes de tal forma que el tráfico de la red se segregue por medio de redes virtutales (VLAN) para que cada equipo solamente tenga acceso a la información que necesita, se compartimenten los diferentes grupos de usuarios para evitar la propagación de malware y las redes inalámbricas disponga de su propio segmento de red. Desarrollar los procedimientos asociados.	Segregación de redes [mp.com.4]	RSIS	X	X		

TAREAS PRIORITARIAS	CONTROL/CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Asegurarse de que todos los usuarios o procesos disponen de un identificador único. Establecer un "periodo de retención" de las cuentas. Desarrollar un procedimiento de control de acceso detallando los mecanismos de identificación implementados En caso de servicios externalizados: completar con los procedimientos documentados proporcionados por el proveedor de configuración de roles/perfiles de acceso a los servicios	Identificación [op.acc.1]	RSIS	X	X		
Desarrollar e implementar una Política de acceso desarrollando un procedimiento de gestión de los derechos de acceso cumpliendo el requisito de "mínimo privilegio". Realizar controles aleatorios de cumplimiento. Registrar estas acciones y sus resultados. Desarrollar un procedimiento de gestión de los derechos de acceso, que garantice que se asignan los mínimos privilegios y que son acordes a los establecidos para el control Requisitos de acceso [op.acc.2] y establecer tareas periódicas de revisión de los permisos otorgados. En caso de servicios externalizados: completar con los procedimientos documentados proporcionados por el proveedor de configuración de roles/perfiles de acceso a los servicios	Requisitos de acceso [op.acc.2] Proceso de gestión de los derechos de acceso [op.acc.4]	RSIS, CSI	X	X		
Desarrollar Instrucciones Técnicas de configuración segura (bastionado) de los principales componentes del sistema: equipamiento (seguridad perimetral, electrónica de red, servidores (físicos, virtuales), bases de datos), equipos de usuarios (PC, portátiles, Smartphone, tabletas), dispositivos conectados a la red (impresoras, etc.) Migrar los sistemas obsoletos (Windows XP, 2003 Server, etc.) a sistemas que dispongan de soporte de seguridad	op.exp.2 Configuración de Seguridad op.exp.3 Gestión de la configuración Protección de equipos portátiles [mp.eq.3]	RSIS		X	X	
Revisar el procedimiento de copias y asegurarse que las políticas implementadas respaldan toda la información, aplicaciones, logs, etc. En caso de servicios externalizados: completar con procedimientos documentados proporcionados por el proveedor de la política de copias de seguridad y de restauración	mp.info.9 Copias de seguridad (back up)	RSIS	X			

TAREAS PRIORITARIAS	CONTROL/CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Instalar la herramienta Lucia herramienta desarrollada por el CCN-CERT para la Gestión de Ciberincidentes. Completar la instalación con las sondas que ofrece (Internet y Red SARA). Instalar un IDS de red Desarrollar un procedimiento integral de gestión de incidentes de seguridad con las obligaciones establecidas por el ENS y RGPD En caso de servicios externalizados: completar con los procedimientos documentados de coordinación con el Ayuntamiento para la gestión incidentes y de comunicación de los mismos a las autoridades de control	Gestión de incidentes [op.exp.7] Registro de la gestión de incidentes [op.exp.9] mp.mon.1 Detección de Intrusión	RSEG	X	X		
Implementar un mecanismo de acceso al CPD que permita identificar a las personas (incluido el acceso de terceros). Desarrollar el procedimiento asociado Revisar las medidas de acondicionamiento del CPD. Implantar un registro de entrada/salida de equipamiento al CPD. Desarrollar el procedimiento asociado.	Identificación de las personas [mp.inf.2] Acondicionamiento de los locales [mp.if.3] Registro de entrada y salida de equipamiento [mp.if.7]	RSIS		X		
Habilitar registros de las actividades de los usuarios realizadas sobre el Sistema, de forma que Indique quién las realiza, cuándo y sobre qué información. Desarrollar procedimiento asociado. Especialmente los de los administradores del sistema para monitorizar su actividad como medida compensatoria de op.acc.3. En caso de servicios externalizados: completar con procedimientos documentados de configuración de los registros de actividad de los usuarios a los servicios Información/plataforma de visualización proporcionada por el proveedor de los accesos de los administradores del sistema que soporta los servicios (en caso de que se hayan requerido) Implantar un sistema automático de recolección de eventos de seguridad. Valorar que permita la correlación de los mismos. (herramienta GLORIA CCN)	Registros de la actividad de los usuarios [op.exp.8] Segregación de funciones y tareas [op.acc.3]	RSIS		X	X	

TAREAS PRIORITARIAS	CONTROL/CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Para servicios proporcionados directamente por el Ayuntamiento: • En caso de realizar desarrollo de Software utilizar metodologías de desarrollo reconocido y seguro. Desarrollar los procedimientos asociados. Realizar acciones formativas. • En caso de que se encargue a terceros desarrollo de software, solicitar que se utilicen metodologías de desarrollo seguro y que satisfagan los requisitos necesarios para cumplir con el ENS. • En caso de adquirir software para instalación en modo local solicitad la conformidad con el ENS, en categoría MEDIA, y los requisitos adicionales requeridos por el "Abstract- Requisitos de Seguridad Adicionales para Soluciones en la Nube (SaaS) implementadas en Modo Local"	Desarrollo [mp.sw.1] Formación [mp.per.4]	CSI			X	X
Para servicios proporcionados directamente por el Ayuntamiento: • Desarrollar e implantar un procedimiento donde se definan las pruebas, a realizar antes de la puesta en producción de las aplicaciones o bien solicitar a los proveedores en caso de que estos proporcionen este servicio. • Se recomienda realizar test de intrusión y análisis de vulnerabilidades, para todas las aplicaciones que ya están puestas en producción. • Para los servicios y las aplicaciones web, además realizar pruebas de las amenazas que son propias de este entorno, realizar test de intrusión. • Para los servicios web y aplicaciones web emplear "certificados de autenticación de sitio web" acordes a la normativa europea en la materia. En caso de servicios externalizados: recopilar los procedimientos documentados proporcionados por el proveedor de coordinación con el Ayuntamiento para la realización de pruebas de aceptación y puesta en servicio. Informes resultados pruebas y plan de acción y los Informes proporcionados por el proveedor con resultados de las inspecciones periódicas realizadas y plan de acción	Aceptación y puesta en servicio [mp.sw.2] Protección de los servicios y aplicaciones web [mp.s.2]	RSIS			X	X

TAREAS PRIORITARIAS	CONTROL/CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Identificar los mecanismos de autenticación de cada recurso y documentar como se encuentra implementado el doble factor de autenticación. Desarrollar el procedimiento asociado. Si se utilizan contraseñas: utilizar contraseñas seguras, definir una política de caducidad. Inventariar los accesos remotos. Realizar un procedimiento que permita mantener este inventario, cómo se autorizan, etc. Realizar unas normas para los accesos remotos que regulen las condiciones en las cuales debe realizare este acceso. Revisar que los accesos remotos, se realizan, implementando doble factor de autenticación En caso de servicios externalizados: completar con pprocedimientos documentados proporcionados por el proveedor de los mecanismos de autenticación de acceso a los servicios	Mecanismo de autenticación [op.acc.5] Acceso remoto (remote login) [op.acc.7]	RSIS	X	X		
Configurar las directivas de acceso al dominio de forma que: • Se establezca una limitación de intentos de acceso. • Solo se muestre información, una vez validado en el dominio, por tanto, no se guardará la información del último usuario validado. • Se informe al usuario de sus obligaciones. • Se muestre la información sobre el último acceso con éxito y los posibles intentos de acceso. En caso de servicios externalizados: completar con procedimientos documentados proporcionados por el proveedor de configuración de los requisitos del control: limitación de intentos de acceso, aviso de obligaciones, información sobre el último acceso	Acceso local (local logon) [op.acc.6]	RSIS	X	X		

Tareas implantación ENS

Durante el año se procederá a implantar y documentar el resto de medidas. La descripción detallada de la tarea.

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
MARCO ORGANIZATIVO						
POLÍTICA DE SEGURIDAD-(incluido en medidas priorizadas)	org.1					
NORMATIVA DE SEGURIDAD-(incluido en medidas priorizadas)	org.2					
PROCEDIMIENTOS DE SEGURIDAD- Desarrollar procedimientos operativos que recojan las principales tareas sobre el sistema. Indicando los responsables de su realización y cómo identificar y reportar comportamientos anómalos. Integrar en un Sistema de Gestión de Seguridad de la Información que de soporte al cumplimiento del ENS. (SGSIENS)	org.3	RSEG RSIS	X	X	X	X
PROCESOS DE AUTORIZACIÓN- Implantar y documentar un proceso de autorización para la introducción de elementos en el sistema: instalaciones, equipos, aplicaciones, medios de comunicación, utilización de soportes, portátiles, móviles, etc. y servicios de terceros.	org.4	RSIS		X		
MARCO OPERACIONAL - PLANIFICACIÓN						
ANÁLISIS DE RIESGOS ENS – (incluido en medidas priorizadas). Desarrollar el procedimiento de análisis de riesgos	op.pl.1	RSEG RSIS				X
ARQUITECTURA DE SEGURIDAD- Recopilar, organizar, completar y mantener actualizada documentación sobre: áreas y puntos de acceso, del sistema, líneas de defensa, identificación y autenticación, controles técnicos, relaciones con terceros, para que formen parte del SGSENS. En caso de servicios externalizados: completar con la documentación proporcionada por el proveedor sobre las comunicaciones con el Ayuntamiento, y con otros sistemas interconectados comunicaciones con el Ayuntamiento, y con otros sistemas interconectados	op.pl.2	RSIS		X	X	
ADQUISICIÓN DE NUEVOS COMPONENTES- Implantar un procedimiento que analice los riesgos, evalúe la necesidad de requisitos antes de la adquisición de nuevos componentes. Registrar estas acciones y sus resultados.	op.pl.3	RSIS		X		
DIMENSIONAMIENTO Y GESTIÓN DE LA CAPACIDAD - (en caso que aplique) - Implantar un procedimiento para la realización de un estudio de estos parámetros antes de la entrada en producción de nuevos elementos. En caso de servicios externalizados: completar con la documentación regular proporcionada por el proveedor sobre los recursos disponibles y consumidos	op.pl.4	RSIS		X		
MARCO OPERACIONAL – CONTROL DE ACCESO						
IDENTIFICACIÓN- (incluido en medidas priorizadas)	op.acc.1					

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
REQUISITOS DE ACCESO- (incluido en medidas priorizadas)	op.acc.2					
SEGREGACIÓN DE FUNCIONES Y TAREAS- Elaborar un procedimiento documento de asignación de tareas con indicación de las tareas críticas y la incompatibilidad entre estas. – Medida compensatoria en caso de que sea necesario incluido en incluido en medidas priorizadas	op.acc.3	RSIS				X
PROCESO DE GESTIÓN DE LOS DERECHOS DE ACCESO-(incluido en medidas priorizadas).	op.acc.4					
MECANISMOS DE AUTENTICACIÓN- (incluido en medidas priorizadas).	op.acc.5					
ACCESO LOCAL (local logon)- (incluido en medidas priorizadas).	op.acc.6					
ACCESO REMOTO (remote login)- (incluido en medidas priorizadas).	op.acc.7					
MARCO OPERACIONAL – EXPLOTACIÓN						
INVENTARIO DE ACTIVOS- Desarrollar un procedimiento que describa la forma en la que se gestionan los activos. Realizar un inventario de software (se recomienda utilizar una herramienta que realice un inventario de activos hardware, software de forma automática).	op.exp.1	RSIS			X	
CONFIGURACIÓN DE SEGURIDAD)- (incluido en medidas priorizadas). Elaborar un procedimiento de bastionado que recoja la configuración básica de seguridad del equipamiento (seguridad perimetral, electrónica de red, servidores (físicos, virtuales), bases de datos), equipos de usuarios (PC, portátiles, Smartphone, tabletas), dispositivos conectados a la red (impresoras, etc.), antes de entrar en operación.	op.exp.2	RSIS		X	X	X
GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD- (incluido en medidas priorizadas). Establecer revisiones periódicas de la configuración de la seguridad: identificar vulnerabilidades, incidencias, etc. Registrar estas acciones y sus resultados.	op.exp.3	RSIS			X	
MANTENIMIENTO - Documentar todas las acciones de mantenimiento (físico y lógico). Registrar estas acciones y sus resultados. Desarrollar un procedimiento para analizar, prioridad la aplicación de actualizaciones de seguridad, parches, mejoras, etc. En caso de servicios externalizados: completar con procedimientos documentados de coordinación con el Ayuntamiento para realizar acciones de mantenimiento sobre el sistema que	op.exp.4	RSIS			X	
GESTIÓN DE CAMBIOS – Desarrollar un procedimiento de Gestión de cambios. En caso de servicios externalizados: completar con procedimientos documentados de coordinación con el Ayuntamiento para realizar cambios sobre el sistema que soporta los servicios	op.exp.5	RSIS			X	
PROTECCIÓN FRENTE A CÓDIGO DAÑINO- (incluido en medidas priorizadas).	op.exp.6					
GESTIÓN DE INCIDENTES- (incluido en medidas priorizadas).	op.exp.7					
REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS – [Incluido en medidas priorizadas}	op.exp.8					
REGISTRO DE LA GESTIÓN DE INCIDENCIAS- (incluido en medidas priorizadas).	op.exp.9					

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
PROTECCIÓN DE LAS CLAVES CRIPTOGRÁFICAS- Documentar las medias de seguridad implementadas para garantizar la protección de las claves criptográficas durante todo su ciclo de vida. Para sistemas de categoría media asegurará la utilización de programas evaluados o dispositivos criptográficos evaluados que empleen algoritmos acreditados por el CCN. En caso de servicios externalizados: completar con procedimientos documentados de protección de las claves criptográficas del Ayuntamiento que se encuentren alojadas en el sistema que soporta los servicios	op.exp.11	RSIS				X
MARCO OPERACIONAL – SERVICIOS EXTERNOS						
CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO - (incluido en medidas priorizadas)	op.ext.1					
GESTIÓN DIARIA - (incluido en medidas priorizadas)	op.ext.2					
MARCO OPERACIONAL – MONITORIZACIÓN DEL SISTEMA						
DETECCIÓN DE INTRUSIÓN – (incluido en medidas priorizadas)	op.mon.1					
MARCO OPERACIONAL – SITEMA DE MÉTRICAS						
SISTEMA DE MÉTRICAS – Realizar un procedimiento que establezca los indicadores, métrica asociada y designación de responsables para su recopilación de los elementos para dar respuesta a la encuesta INES (re-querido por el artículo 35).	op.mon.2	RSIS				X
MARCO OPERACIONAL-CONTINUIDAD						
ANÁLISIS DE IMPACTO – Desarrollar un análisis de impacto que permita determinar los requisitos de disponibilidad y los elementos críticos de cada servicio. Realizar el procedimiento asociado	op.cont.1	CSI		X		
MARCO DE PROTECCIÓN – PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS						
ÁREAS SEPARADAS Y CONTROL DE ACCESO- Realizar un procedimiento que contengan un inventario de todas las áreas donde se concentra el sistema de información y que detalle los mecanismos implementados en cada caso para controlar el acceso a las mismas y las autorizaciones pertinentes en caso de que sea necesario	mp.if.1	RSIS				X
IDENTIFICACIÓN DE LAS PERSONAS- (incluido en medidas priorizadas).	mp.if.2					
ACONDICIONAMIENTO DE LOS LOCALES- Documentar las medidas implementadas para asegurar el acondicionamiento del CPD: sensores de temperatura, humedad, protección del cableado, etc. Cómo se monitorizan y responsables. -(incluido en medidas priorizadas).	mp.if.3	RSIS				X
ENERGÍA ELÉCTRICA- Documentar las medidas implementadas para garantizar el suministro eléctrico en el CPD. En caso de que sea de aplicación describir las medidas adicionales implementadas (SAI, grupo electrónico, la forma y cuando entran en funcionamiento, pruebas de contingencia realizadas para determinar los cálculos de tiempo.)	mp.if.4	RSIS				X

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
PROTECCIÓN FRENTE A INCENDIOS- Desarrollar un procedimiento que recoja la forma en la cual se protegen los locales conforme a la normativa industrial, la ubicación de los carteles, extintores, materiales no inflamables, etc. Los controles periódicos realizados, etc. Mantener de forma centralizada toda la documentación relacionada Mantener de forma centralizada toda la documentación relacionada)	mp.if.5	RSIS				X
PROTECCIÓN FRENTE A INUNDACIONES- (en caso que aplique) Desarrollar un procedimiento que recoja la forma en la cual se protegen los locales frente a inundaciones	mp.if.6	RSIS				X
REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO- (incluido en medidas priorizadas)	mp.if.7					
MARCO DE PROTECCIÓN – GESTIÓN DE PERSONAL						
CARACTERIZACIÓN DEL PUESTO DE TRABAJO- Realizar fichas de perfiles de puestos de trabajo, que contemplen la definición de responsabilidades en materia de seguridad.	mp.per.1	CSI		X		X
DEBERES Y OBLIGACIONES- Desarrollar un procedimiento de gestión de personal que describa la forma en la cual se trasladan los deberes al personal propio o de terceros.	mp.per.2	CSI				X
CONCIENCIACIÓN- (incluido en medidas priorizadas) Desarrollar un procedimiento que describa la cómo se desarrollará el Plan Concienciación en materia de seguridad de la información para todo el personal, con periodicidad anual. (Incluido también en medidas periodicidad anual)	mp.per.3	RSEG CSI				
FORMACIÓN– (incluido en medidas priorizadas) Desarrollar un procedimiento que describa la cómo se desarrollará el Plan de Formación específica en seguridad de la información para el personal con responsabilidad en la operación del sistema, con periodicidad anual. (Incluido también en medidas periodicidad anual)	mp.per.4	RSEG CSI				
MARCO DE PROTECCIÓN – PROTECCIÓN DE LOS EQUIPOS						
PUESTO DE TRABAJO DESPEJADO – (incluido en medidas priorizadas) Obligación recogida en la Normativa de seguridad [org.2]	mp.eq.1					
BLOQUEO DE PUESTO DE TRABAJO– (incluido en medidas priorizadas) Obligación recogida en la Normativa de seguridad [org.2]	mp.eq.2					
PROTECCIÓN DE LOS EQUIPOS PORTÁTILES-– (incluido en medidas priorizadas) Desarrollar un procedimiento que describa la forma en la que realizar el inventario de los equipos portátiles (incluido Smartphone, tabletas, etc.)	mp.eq.3	RSIS			X	
MARCO DE PROTECCIÓN – PROTECCIÓN DE LAS COMUNICACIONES						
PERÍMETRO SEGURO- Documentar la seguridad perimetral y las excepciones implementadas en los firewalls. Proceso de autorización y que describa la separación de flujos implementada.	mp.com.1	RSIS				X

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
PROTECCIÓN DE LA CONFIDENCIALIDAD- Realizar un procedimiento que describa la forma en la cual se protege la confidencialidad de la información cuanto esta discurre por redes fuera del propio dominio de seguridad. En caso de servicios externalizados: completar con documentos proporcionados por el proveedor con información sobre los mecanismos de cifrado implementados en las comunicaciones.	mp.com.2	RSIS				X
PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD - Realizar un procedimiento/norma que establezca la necesidad de utilizar redes privadas virtuales para garantizar la autenticidad y la integridad de la información antes de su intercambio. En caso de servicios externalizados: completar con documentos proporcionados por el proveedor con información sobre los mecanismos implementados para proteger la autenticidad y de la integridad	mp.com.3	RSIS				X
SEGREGACIÓN DE REDES – (incluido en medidas priorizadas)	mp.com.4					
MARCO DE PROTECCIÓN – PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN						
ETIQUETADO–- (en caso que aplique). Desarrollar un procedimiento para el etiquetado de soportes extraíbles conforme a la calificación de la información que contienen. Difundir al personal afectado.	mp.si.1	RSIS		X		
CRIPTOGRAFÍA-- (en caso que aplique). Desarrollar un procedimiento que describa la forma en la que se aplicarán mecanismos de cifrado a los soportes de información. Difundir al personal afectado.	mp.si.2	RSIS		X		
CUSTODIA- - (en caso que aplique). Desarrollar un procedimiento para la custodia de soportes de información. Difundir al personal afectado.	mp.si.3	RSIS		X		
TRANSPORTE- - (en caso que aplique) Desarrollar un procedimiento que describa las medidas de seguridad a aplicar durante el transporte a los soportes de información. Difundir al personal afectado.	mp.si.4	RSIS		X		
BORRADO Y DESTRUCCIÓN- Desarrollar un procedimiento que describa el procedimiento a seguir para el borrado y destrucción en función del soporte. Elaborar instrucción técnica de borrado y de destrucción	mp.si.5	RSIS		X		
MARCO OPERACIONAL – PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS						
DESARROLLO- - (en caso que aplique) (incluido en medidas priorizadas)	mp.sw.1					
ACEPTACIÓN Y PUESTA EN SERVICIO-- (en caso que aplique) (incluido en medidas priorizadas)	mp.sw.2					
MARCO OPERACIONAL – PROTECCIÓN DE LA INFORMACIÓN						
DATOS DE CARÁCTER PERSONAL – Desarrollar las acciones de seguridad necesarias para llevar a cabo la implantación de la normativa de protección de datos (RAT, designación DPD, Análisis de Riegos RGPD, Evaluación de Impacto, contratos de encargado del tratamiento, alinear medidas de seguridad con las del ENS). En caso de servicios externalizados: recopilar documentos /plataformas online, proporcionados por el proveedor, con evidencias de cumplimiento de la normativa de protección de datos	mp.info.1	CSI	X	X	X	X
CALIFICACIÓN DE LA INFORMACIÓN - Desarrollar e implantar un procedimiento de calificación de la información. Elaborar procedimientos que definan la forma que hay que tratar la documentación en consideración al nivel de seguridad requerido	mp.info.2	CSI				X

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
FIRMA ELECTRÓNICA – - (en caso que aplique) Desarrollar, aprobar y dar publicidad a la Política de Firma Electrónica. Realizar un procedimiento que recoja los requisitos que deben cumplir los mecanismos de firma electrónica En caso de servicios externalizados: completar con documentos proporcionados por el proveedor con información sobre las medidas de protección de la firma implementadas	mp.info.4	CSI			X	X
SELLOS DE TIEMPO –- (en caso que aplique) Realizar un procedimiento que recoja los requisitos que deben cumplir los mecanismos de sello electrónico En caso de servicios externalizados: recopilar documentos proporcionados por el proveedor con información sobre las medidas de seguridad implementadas para proteger el sello de tiempo	mp.info.6					
LIMPIEZA DE DOCUMENTOS- Desarrollar e Implantar un procedimiento donde se establezca la forma en la cual se ha de proceder para la limpieza de los documentos electrónicos.	mp.info.6	CSI			X	
COPIA DE SEGURIDAD- (incluido en medidas priorizadas)	mp.info.9					
MARCO OPERACIONAL – PROTECCIÓN DE LOS SERVICIOS						
PROTECCIÓN DEL CORREO ELECTRÓNICO- (en caso que aplique) Desarrollar un procedimiento que describa la forma en la cual se protege el correo.	mp.s.1	RSIS			X	
PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB - (en caso que aplique) - (incluido en medidas priorizadas)	mp.s.2	RSIS				X
PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO- (en caso que aplique) – Documentar las medidas de seguridad implementadas. Realizar el procedimiento asociado.	mp.s.8	RSIS				X

Tareas periódicas

TAREAS PERIODICIDAD ANUAL	CONTROL	PERIODICIDAD
Revisión de la Política de Seguridad de la Información	Política de Seguridad de la Información [org.1]	Anual
Elaboración del Plan de Concienciación y Plan de Formación	Concienciación [mp.per.3] Formación [mp.per.4]	Anual
Revisión de la Normativa de seguridad,	Normativa de seguridad [org.2]	Anual
Revisión de la Información y lo Servicios, su valoración y proceso de categorización del sistema	Artículo 43. Categorías y 44. Facultades del Real Decreto ENS	Permanente
Actualización del análisis de Riesgos	Análisis de riesgos [op.pl.1]	Anual/ cambios relevantes
Revisión de la Declaración de aplicabilidad o del Perfil de Cumplimiento	Artículo 27. Cumplimiento de requisitos mínimos. 2. Selección de medidas de seguridad -ANEXO II Medidas de seguridad	Anual
Realización de auditorías internas. Revisión de medidas de seguridad y procedimientos	Todos	Al menos anual
Revisión del Plan de Mejora de la Seguridad		Mensual/ Trimestral
Revisión del Estado de la Seguridad. INÉS	Artículo 35 Sistema de Métricas [op.mon.2]	Anual
Auditoría ENS (certificación conformidad ENS).	Artículo 34. Auditoría de la seguridad.	Bienal