Guía de Seguridad de las TIC
CCN-STIC 883

Anexo III. Plan de Adecuación al ENS
Diputaciones, Cabildos, Consejos Insulares y órganos competentes equivalentes

Mayo 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO :083-19-183-2

Fecha de Edición: mayo de 2020

ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Nota: sustituir "órgano competente" por Diputación, Cabildo, Consejo Insular u órgano competente equivalente.

Texto aprobado el día __ de _____ de ____ por resolución de [indicar órgano] del "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 Diputaciones, Consejos Insulares y órganos competentes equivalentes.

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 "órgano competente" de_____, conforme a lo establecido en

el Perfil de Cumplimiento Específico de aplicación a las Diputaciones, Cabildos, Consejos Insulares y órganos competentes equivalentes.

7. PLAN DE MEJORA DE LA SEGURIDAD

En el **Anexo V**, del presente documento, se adjunta el **Plan de Mejora de la Seguridad** del "órgano competente" 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. PROPUESTA DE DECRETO DE CREACIÓN DE ORGANO Y DESIGNACIÓN DE ROLES DE SEGURIDAD DE LA INFORMACIÓN

Nota: modelo de Decreto para una Diputación

PROPUESTA DE DECRETO DE PRESIDENCIA DE LA DIPUTACIÓN DE_____ POR EL QUE SE ASIGNAN FUNCIONES AL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, SE REGULA SU COMPOSICIÓN Y FUNCIONAMIENTO Y SE DESIGNAN LOS ROLES Y FUNCIONES EN SEGURIDAD DE LA INFORMACIÓN EN LA DIPUTACIÓN, EN CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD

El Diputado/a con competencias en administración electrónica y/o Seguridad de la información de la Diputación de_____, de acuerdo a las competencias que le han sido delegadas por Decreto de la Presidencia de fecha_____, eleva a la Ilma. Presidencia de la Diputación de _____ la propuesta de decreto por el que se asignan funciones al Comité de Seguridad de la Información, se regula su composición y funcionamiento y se designan las funciones en seguridad de la información, en el cumplimiento 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, 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 3/2010 que regula el Esquema Nacional de Seguridad, la Diputación 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:

Cuarto. - En aplicación del Real Decreto que regula el Esquema Nacional de Seguridad, la Diputación 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 Presidencia por el que se asignan las funciones el Comité de Seguridad de la Información, se regula su composición y funcionamiento y se designan las funciones en seguridad de la información en la Diputación de _____, en los términos que a continuación se detallan**.**

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

A la vista de la propuesta presentada por el Diputado/a con competencias en materia de administración electrónica y/o seguridad de la información, según las competencias atribuidas por Decreto de _____

Según las competencias de auto-organización de la Diputación, reconocidas en el artículo 4 y con la capacidad reconocida en el artículo 31 de la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, teniendo en cuenta lo establecido en el Real Decreto_3/2010 por el que se regula el Esquema Nacional de Seguridad; Esta Presidencia considerando las competencias atribuidas en el artículo 34.1 h y ñ) de la Ley 7/1985, de 2 de abril, reguladora de la Ley de Bases de Régimen Local.

RESUELVE

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 de la Diputación denominado Comité de Seguridad de la Información, incluyendo la regulación de sus composición y funciones.

2.- En el presente Decreto se designan también la composición y 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 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 de la Diputación 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 Presidencia o Diputado en quien delegue.

Artículo 6.- Régimen de funcionamiento y convocatorias

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias de la Diputación 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. Con carácter excepcional, las reuniones podrán realizarse a distancia, debiendo reunir los mismos requisitos que si fuese presencial, dejando constancia en todo caso de los asistentes, las opiniones y sentido de la votación, así como la posibilidad de realizar la grabación de las sesiones para la configuración de las actas o videoactas. Se deberá prever que las conexiones se realicen de forma segura y que los integrantes cuenten con los medios adecuados para su participación.

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 a 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 Presidencia o Diputado delegado.

El Responsable de Información será un puesto de nivel directivo, al ser el responsable último de la información municipal, estableciendo los niveles de seguridad de la información.

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.

El Responsable del Sistema se establece a nivel operativo. Se pueden designar Delegados de dicho responsable.

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 de la Diputación, 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, pudiendo contar con una 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, pudiendo contar con una 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 Presidencia o Diputado 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 Presidencia o Diputado delegado, 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 validez 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

1 APROBACIÓN Y ENTRADA EN VIGOR

Nota: sustituir "órgano competente" por Diputación, Cabildo, Consejo Insular u órgano competente equivalente.

Texto aprobado el día __ de _____ de ____ por resolución de la _____ del "órgano competente" 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 "órgano competente" 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 [ÓRGANO COMPETENTE]

Nota: Describir los objetivos de servicio del órgano competente.

4. ALCANCE

Esta Política se aplicará a los sistemas de información del "órgano competente" 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 "órgano competente" 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- 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 "órgano competente" de_____.
- Reglamento por el que se establece la Sede Electrónica del "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 [indicar rol/órgano] 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 del "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 "órgano competente" 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 el "órgano competente" 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 "órgano competente" de _____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) 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 "órgano competente" de_____.

2.10. TERCERAS PARTES

Cuando el "órgano competente" de _____ preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. El "órgano competente" 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 "órgano competente" de_____ lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el "órgano competente" 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, propuesto como modelo a utilizar para una Diputación.

1.1. Identificación e Inventario de Servicios e Información

Competencias de las Diputaciones

Para la identificación de servicios que se encuentran dentro del alcance de ENS, se ha tomado como base en análisis de las competencias recogidas en los artículos 27 y 36 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL). También se tienen en cuenta los artículos 25 y siguientes del Texto Refundido de las Disposiciones Legales vigentes en materia de régimen local (R.D. Leg. 781/1986, de 18 de abril).

COMPETENCIAS	DESCRIPCIÓN
BOLETÍN OFICIAL DE LA PROVINCIA	Gestión del Servicio del Boletín Oficial de la Provincia
GESTIÓN TRIBUTARIA DE LOS MUNICIPIOS	Gestión del servicio de recaudación y cooperación con municipios
ATENCIÓN AL CIUDADANO	Gestión de la atención ciudadana, actividades de participación y página web
ASESORAMIENTO TÉCNICO Y JURÍDICO A MUNICIPIOS	Servicio de asistencia técnica y jurídica a municipios mediante el asesoramiento y elaboración de informes Selección y formación de personal municipal
ADMINISTRACIÓN ELECTRÓNICA EN MUNICIPIOS	Servicio relacionado con la implantación de la administración electrónica proporcionado a Ayuntamientos de menor tamaño
CULTURA	Gestión del servicio de servicios culturales y bibliotecas en cooperación con los Ayuntamientos
JUVENTUD	Gestión de servicios de juventud municipales
PRESTACIONES SOCIALES	Gestión de las prestaciones sociales del servicio de Derechos Sociales en cooperación con otras administraciones
DEPORTES	Gestión de las actividades e infraestructuras deportivas en colaboración con los municipios de la provincia
PROMOCIÓN Y APOYO AL TURISMO	Gestión y promoción del turismo en la Diputación
PROMOCIÓN DE ACTIVIDADES ECONÓMICAS Y DEL EMPLEO	Gestión del servicio de promoción y actividades económicas de la provincia

COMPETENCIAS	DESCRIPCIÓN
OBRAS PÚBLICAS Y MANTENIMIENTO DE INFRAESTRUCTURAS y EQUIPAMIENTOS	Gestión de las obras públicas en los municipios de la provincia, apoyo a los municipios en el mantenimiento de diversas infraestructuras y equipamientos municipales
GESTIÓN DEL CICLO DEL AGUA. SANEAMIENTO	Servicio de gestión del ciclo del agua: abastecimiento y saneamiento
RECOGIDA DE RESIDUOS	Servicio de recogida selectiva de residuos en el territorio de la Diputación
DESARROLLO RURAL	Gestión de la promoción del desarrollo rural en la provincia
EXTINCIÓN DE INCENDIOS Y PROTECCIÓN CIVIL	Servicio de prevención de incendios y protección civil
MEDIOAMBIENTE	Gestión de la protección medioambiental en la provincia. Apoyo a los municipios en la materia, control plagas, saneamiento ganadero y recogida de animales

En esta identificación se han tratado de abarcar otros servicios que presta la Diputación, así como otras competencias y potestades propias de estas entidades locales que se regulan tanto en la Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local, como en otra normativa sectorial, como la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común; la Ley 40/2015, de 1 de octubre de régimen jurídico del sector público o la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno. También otras materias específicas, como las prestaciones sociales, las políticas de igualdad o violencia de género o la materia de consumo, que pueden venir de un reparto competencial de normativa estatal o autonómica, pero vista siempre desde una perspectiva general, sin entrar a valorar la normativa propia y específica de las diferentes comunidades autónomas.

Identificación e inventario de Servicios

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

ID	SERVICIOS	DESCRIPCIÓN	COMPETENCIA*
S 01	ARCHIVO	Gestión del Servicio de archivo	LRJSP
S 02	BOLETÍN OFICIAL DE LA PROVINCIA	Gestión del Servicio del Boletín Oficial de la Provincia	Ley 5/2002, de 4 de abril, reguladora de los Boletines Oficiales de Provincias

ID	SERVICIOS	DESCRIPCIÓN	COMPETENCIA*
S 03	CONTRATACIÓN	Gestión del Servicio de contratación de la Diputación y compras centralizadas para municipios	LCSP ASESORAMIENTO TÉCNICO Y JURÍDICO A MUNICIPIOS
S 04	GESTIÓN ECONÓMICA, TRIBUTARIA Y CONTABLE	Gestión de los ingresos de la Diputación y la contabilidad, fiscalización. Control financiero y gestión de la caja de crédito local	LBRL y LHL Caja de crédito local Texto Refundido en materia de disposiciones legales vigentes en materia de régimen local (R.D. Legislativo 781/1986, de 18 de abril)
S 05	TESORERÍA	Gestión de tesorería	LBRL LHL
S 06	PERSONAL	Gestión de las personas empleadas en la Diputación, así como la prevención de los riesgos laborales	LBRL EBEP Texto Refundido en materia de disposiciones legales vigentes en materia de régimen local
S 07	GESTIÓN TRIBUTARIA DE LOS MUNICIPIOS	Gestión del servicio de recaudación y cooperación con municipios	GESTIÓN TRIBUTARIA DE LOS MUNICIPIOS
S 08	SECRETARÍA	Gestión, seguimiento y control sobre los actos municipales y los miembros de la corporación local. Gestión de expedientes relacionados con la actividad municipal. Gestión de las obligaciones en materia de protección de datos.	Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local (LBRL)
S 09	SERVICIOS JURÍDICOS	Gestión de expedientes judiciales y de responsabilidad patrimonial.	LBRL LRJSP
S 10	REGISTRO GENERAL	Gestión del registro de entrada y salida de documentos	LBRL. ROF LPAC

ID	SERVICIOS	DESCRIPCIÓN	COMPETENCIA*
S 11	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 la Diputación.	LBRL LPAC LTAIBG
S 12	ASESORAMIENTO TÉCNICO Y JURÍDICO A MUNICIPIOS	Servicio de asistencia técnica y jurídica a municipios mediante el asesoramiento y elaboración de informes Selección y formación de personal municipal	ASESORAMIENTO TÉCNICO Y JURÍDICO A MUNICIPIOS
S 13	ADMINISTRACIÓN ELECTRÓNICA EN MUNICIPIOS	Servicio relacionados con la implantación de la administración electrónica proporcionado a Ayuntamientos de menor tamaño	ADMINISTRACIÓN ELECTRÓNICA EN MUNICIPIOS
S 14	SEGURIDAD DE EDIFICIOS Y ACCESOS	Gestión del Servicio de la seguridad de edificios y accesos, incluyendo los sistemas de videovigilancia en edificios	LBRL
S 15	INFORMÁTICA Y COMUNICACIONES	Gestión y control de los sistemas informáticos y de comunicaciones de la Diputación, así como la gestión del cumplimiento de las obligaciones en materia de protección de datos y ENS.	LRJSP
S 16	CULTURA	Gestión del servicio de servicios culturales y bibliotecas en cooperación con los Ayuntamientos	CULTURA
S 17	JUVENTUD	Gestión de servicios de juventud municipales	JUVENTUD

ID	SERVICIOS	DESCRIPCIÓN	COMPETENCIA*
S 18	PRESTACIONES SOCIALES	Gestión de las prestaciones sociales del servicio de Derechos Sociales en cooperación con otras administraciones	PRESTACIONES SOCIALES Legislación sectorial (Leyes servicios sociales autonómicas, Ley Dependencia, etc.)
S 19	IGUALDAD Y VIOLENCIA DE GENERO	Cooperación municipal en las actuaciones de igualdad y violencia de género	Ley de igualdad Ley contra la Violencia de Género
S 20	DEPORTES	Gestión de las actividades e infraestructuras deportivas en colaboración con los municipios de la provincia	DEPORTES
S 21	PROMOCIÓN Y APOYO AL TURISMO	Gestión y promoción del turismo en la Diputación	PROMOCIÓN Y APOYO AL turismo
S 22	PROMOCIÓN DE ACTIVIDADES ECONÓMICAS Y DEL EMPLEO	Gestión del servicio de promoción y actividades económicas de la provincia	PROMOCIÓN DE ACTIVIDADES ECONÓMICAS Y DEL EMPLEO
S 23	CONSUMO	Cooperación con los municipios de la provincia en la prestación de servicios de consumo	Ley General de Defensa de los Consumidores y usuarios (R.D. Legislativo 1/2007, de 16 de noviembre) Legislación autonómica
S 24	OBRAS PÚBLICAS Y MANTENIMIENTO DE INFRAESTRUCTURAS y EQUIPAMIENTOS	Gestión de las obras públicas en los municipios de la provincia, apoyo a los municipios en el mantenimiento de diversas infraestructuras y equipamientos municipales	OBRAS PÚBLICAS Y MANTENIMIENTO DE INFRAESTRUCTURAS y EQUIPAMIENTOS
S 25	GESTIÓN DEL CICLO DEL AGUA. SANEAMIENTO	Servicio de gestión del ciclo del agua: abastecimiento y saneamiento	GESTIÓN DEL CICLO DEL AGUA. SANEAMIENTO
S 26	RECOGIDA DE RESIDUOS	Servicio de recogida selectiva de residuos en el territorio de la Diputación	RECOGIDA DE RESIDUOS
S 27	DESARROLLO RURAL	Gestión de la promoción del desarrollo rural en la provincia	DESARROLLO RURAL

ID	SERVICIOS	DESCRIPCIÓN	COMPETENCIA*
S 28	EXTINCIÓN DE INCENDIOS Y PROTECCIÓN CIVIL	Servicio de prevención de incendios y protección civil.	EXTINCIÓN DE INCENDIOS Y PROTECCIÓN CIVIL
S 29	MEDIOAMBIENTE	Gestión de la protección medioambiental en la provincia. Apoyo a los municipios en la materia, control plagas, saneamiento ganadero y recogida de animales	MEDIOAMBIENTE

(*) 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);
- Texto Refundido en materia de disposiciones legales vigentes en materia de régimen local (R.D. Legislativo 781/1986, de 18 de abril)
- 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);
- L.O 3/2007, de 22 de marzo, para la igualdad efectiva de hombres y mujeres (Ley igualdad)
- LO 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género (Ley violencia de género)
- Ley 39/2016, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las Personas en situación de Dependencia (Ley Dependencia);
- Ley 5/2002, de 4 de abril, reguladora de los Boletines Oficiales de Provincias;
- 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 DEL ARCHIVO DE LA DIPUTACIÓN	Organización, archivo de expedientes, documentos, contenidos audiovisuales, fondos o registros de la Diputación que han pasado al Archivo. Gestión de las peticiones de acceso, consultas, copias y extracciones de documentos.

ID	INFORMACIÓN	DESCRIPCIÓN
I 02	ATENCIÓN A LA CIUDADANÍA	Tramitación y gestión de solicitudes de información, quejas, reclamaciones e iniciativas recibidas por la Diputación. Gestión de las solicitudes de acceso a la información pública y de la publicidad activa (transparencia) de la Diputación
I 03	GESTIÓN DE LAS OBRAS PÚBLICAS	Gestión y control de los procedimientos y actividades realizados por el Ayuntamiento obras públicas de la Diputación, mantenimiento y limpieza de otras infraestructuras.
I 04	GESTIÓN DE LA INFORMACIÓN SOBRE EL CICLO DEL AGUA	Gestión y control de la coordinación de los servicios municipales de aguas, saneamiento y recogida de basuras. Control de residuos y puntos limpios.
I 05	ATENCIONES Y PRESTACIONES SOCIALES	Coordinación y apoyo en la gestión de las prestaciones sociales de los municipios de menor tamaño de la Diputación, incluyendo las actuaciones de coordinación, la gestión y tramitación de ayudas y prestaciones
I 06	AYUDAS Y SUBVENCIONES	Tramitación y gestión de las ayudas, becas y subvenciones existentes en los diferentes programas o líneas de subvención de la Diputación
I 07	GESTIÓN DEL SERVICIO DE EXTINCIÓN DE INCENDIOS	Gestión de las actuaciones e intervenciones de los servicios de bomberos de la Diputación.
I 08	PROTECCIÓN CIVIL	Gestión de las actuaciones e intervenciones de Protección Civil.
I 09	PROCEDIMIENTOS SANCIONADORES	Gestión y control de toda clase de procedimientos sancionadores abiertos por la Diputación
I 10	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.
I 11	PROCEDIMIENTOS TRIBUTARIOS	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.

ID	INFORMACIÓN	DESCRIPCIÓN
I 12	PROMOCIÓN DEL DEPORTE	Gestión de las instalaciones deportivas y actividades deportivas desarrolladas en las mismas, así como el fomento, promoción del deporte en la Diputación. Colaboración con los municipios de menor entidad.
I 13	PROMOCIÓN CULTURAL	Gestión de las actividades culturales organizadas o promocionadas en cooperación de los Ayuntamientos de la Diputación, incluida la gestión de las bibliotecas municipales. Colaboración con los municipios de menor entidad.
I 14	FORMACIÓN	Gestión de los servicios, actividades y eventos formativos organizados y promovidos por la Diputación y coordinación con los municipios.
I 15	PROCEDIMIENTOS DE CONTRATACIÓN PÚBLICA	Gestión del proceso de contratación municipal y seguimiento de los licitadores para el cumplimiento del servicio contratado.
I 16	GESTIÓN DEL PERSONAL	Gestión de la nómina del personal funcionario y laboral de la Diputación, así como la obtención de todos los productos derivados de la misma. Gestión del personal de la Diputación: Control de incompatibilidades; situación laboral. Cumplimento de las obligaciones en materia de prevención de riesgos laborales. [categorías especiales de datos]
I 17	PRESUPUESTOS, CONTABILIDAD, PAGOS Y FISCALIZACIÓN	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.
I 18	ORGANOS DE GOBIERNO, DIPUTADOS Y REGISTRO DE BIENES E INTERESES	Gestión de los datos de los miembros de la corporación de la Diputación 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 19	REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS	Gestión de la información relacionada registro de entrada y salida de documentos en los términos y condiciones establecidas en la Ley de procedimiento administrativo común y la Ley de Bases de Régimen Local y su normativa de desarrollo.
I 20	PARTICIPACIÓN CIUDADANA	Gestión de los procesos de participación ciudadana

ID	INFORMACIÓN	DESCRIPCIÓN
I 21	SEGURIDAD DE INSTALACIONES	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 22	PROMOCIÓN DE ACTIVIDADES JUVENILES	Gestión y control de los servicios, programas, actividades y recursos dirigidos a la población juvenil del municipio y de los participantes.
I 23	CONTROL FINANCIERO	Concesión de préstamos a los municipios de la Diputación y apoyo a los Planes Económico Financieros
I 24	PLANES DE COOPERACIÓN LOCAL	Gestión de los planes de cooperación local.
I 25	MANTENIMIENTO DE ESPACIOS PÚBLICOS	Gestión de mantenimiento de espacios públicos de la Diputación vinculados al medio ambiente.
I 26	GESTIÓN DE RESIDUOS MUNICIPALES	Coordinación para el tratamiento y gestión de los residuos de los Ayuntamientos de la Diputación.
I 27	ACTIVIDADES DE TURISMO	Gestión de las actividades vinculadas a la promoción del turismo en la Diputación y coordinación con los Ayuntamientos en apoyo al sector turístico.
I 28	GESTIÓN DE ACTIVIDADES EN TRANSPARENCIA	Gestión del Cumplimiento de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno en la entidad local. Portal de transparencia y datos abiertos
I 29	SERVICIOS DE CONSUMO	Gestión de la información relacionada con la prestación de los servicios para la defensa de consumidores.
I 30	GESTIÓN DEL ENTORNO RURAL	Información relacionada con las actuaciones de promoción y coordinación del ámbito rural en la Diputación
I 31	PROCESOS SELECTIVOS	Gestión de los procesos selectivos propios y en apoyo a los municipios de menor entidad
I 32	INFORMES JURÍDICOS Y TÉCNICOS EN ASESORAMIENTO A MUNICIPIOS	Gestión de informes jurídicos y técnico en diversas materias de competencia municipal en apoyo a los municipios que así la requieran.

ID	INFORMACIÓN	DESCRIPCIÓN
I 33	MEDIDAS DE PROMOCIÓN ECONÓMICA Y DEL EMPLEO	Gestión de diversas actuaciones relacionadas con la promoción económica de la Diputación y promoción de políticas de empleo.
I 34	PUBLICACIONES OFICIALES	Gestión de actividades relacionadas con la publicación en el Boletín de la Provincia
I 35	SISTEMAS DE INFORMACIÓN	Gestión interna de los sistemas de información y comunicaciones del Diputación para garantizar su correcto funcionamiento y el cumplimiento de las obligaciones de seguridad y protección de datos legalmente establecidas.
I 36	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 37	VOLUNTARIADO	Gestión y control de las personas que realizan algún tipo de actividad de voluntariado en la Diputación y de las actividades realizadas.
I 38	DEFENSA JURÍDICA Y RESPONSABILIDAD PATRIMONIAL	Gestión de los expedientes de responsabilidad patrimonial de la Diputación. Gestión y seguimiento de los expedientes administrativos.

Relación entre Servicios e información

A continuación, se establece la relación entre Servicios e Información

SERVICIOS	INFORMACIÓN
ARCHIVO	GESTIÓN DEL ARCHIVO DE LA DIPUTACIÓN
BOLETÍN OFICIAL DE LA PROVINCIA	PUBLICACIONES OFICIALES
CONTRATACIÓN	PROCEDIMIENTOS DE CONTRATACIÓN PÚBLICA
GESTIÓN ECONÓMICA, TRIBUTARIA Y CONTABLE	PRESUPUESTOS, CONTABILIDAD, PAGOS Y FISCALIZACIÓN CONTROL FINANCIERO PROCEDIMIENTOS TRIBUTARIOS

SERVICIOS	INFORMACIÓN
TESORERÍA	AYUDAS Y SUBVENCIONES PROCEDIMIENTOS TRIBUTARIOS PRESUPUESTOS, CONTABILIDAD, PAGOS Y FISCALIZACIÓN CONTROL FINANCIERO
PERSONAL	GESTIÓN DEL PERSONAL FORMACIÓN PROCESOS SELECTIVOS
GESTIÓN TRIBUTARIA DE LOS MUNICIPIOS	PROCEDIMIENTOS TRIBUTARIOS
SECRETARÍA	ORGANOS DE GOBIERNO, DIPUTADOS Y REGISTRO DE BIENES E INTERESES PROCEDIMIENTOS SANCIONADORES
SERVICIOS JURÍDICOS	DEFENSA JURÍDICA Y RESPONSABILIDAD PATRIMONIAL PROCEDIMIENTOS SANCIONADORES
REGISTRO GENERAL	REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS
PARTICIPACIÓN CIUDADANA	ATENCIÓN A LA CIUDADANÍA VOLUNTARIADO GESTIÓN DE ACTIVIDADES EN TRANSPARENCIA
ASESORAMIENTO TÉCNICO Y JURÍDICO A MUNICIPIOS	AYUDAS Y SUBVENCIONES INFORMES JURÍDICOS Y TÉCNICOS EN ASESORAMIENTO A MUNICIPIOS FORMACIÓN PROCESOS SELECTIVOS CONTROL FINANCIERO
ADMINISTRACIÓN ELECTRÓNICA EN MUNICIPIOS	INFORMES JURÍDICOS Y TÉCNICOS EN ASESORAMIENTO A MUNICIPIOS SERVICIOS TELEMÁTICOS Y COMUNICACIONES
SEGURIDAD DE EDIFICIOS Y ACCESOS	SEGURIDAD DE INSTALACIONES
INFORMÁTICA Y COMUNICACIONES	SISTEMAS DE INFORMACIÓN SERVICIOS TELEMÁTICOS Y COMUNICACIONES
CULTURA	AYUDAS Y SUBVENCIONES PROMOCIÓN CULTURAL
JUVENTUD	AYUDAS Y SUBVENCIONES PROMOCIÓN DE ACTIVIDADES JUVENILES
PRESTACIONES SOCIALES	ATENCIONES Y PRESTACIONES SOCIALES GESTIÓN DE LOS SISTEMAS DE ATENCIÓN A LA DEPENDENCIA Y OTRAS PRESTACIONES AYUDAS Y SUBVENCIONES
DEPORTES	AYUDAS Y SUBVENCIONES PROMOCIÓN DEL DEPORTE

SERVICIOS	INFORMACIÓN
PROMOCIÓN Y APOYO AL turismo	ACTIVIDADES DE TURISMO AYUDAS Y SUBVENCIONES
PROMOCIÓN DE ACTIVIDADES ECONÓMICAS Y DEL EMPLEO	AYUDAS Y SUBVENCIONES MEDIDAS DE PROMOCIÓN ECONÓMICA Y DEL EMPLEO
CONSUMO	SERVICIOS DE CONSUMO AYUDAS Y SUBVENCIONES
OBRAS PÚBLICAS Y MANTENIMIENTO DE INFRAESTRUCTURAS y EQUIPAMIENTOS	PLANES DE COOPERACIÓN LOCAL GESTIÓN DE LAS OBRAS PÚBLICAS MANTENIMIENTO DE ESPACIOS PÚBLICOS
GESTIÓN DEL CICLO DEL AGUA. SANEAMIENTO	PLANES DE COOPERACIÓN LOCAL GESTIÓN DE LA INFORMACIÓN SOBRE EL CICLO DEL AGUA
RECOGIDA DE RESIDUOS	PLANES DE COOPERACIÓN LOCAL GESTIÓN DE RESIDUOS MUNICIPALES
DESARROLLO RURAL	PLANES DE COOPERACIÓN LOCAL GESTIÓN DEL ENTORNO RURAL AYUDAS Y SUBVENCIONES
EXTINCIÓN DE INCENDIOS Y PROTECCIÓN CIVIL	GESTIÓN DEL SERVICIO DE EXTINCIÓN DE INCENDIOS PROTECCION CIVIL
MEDIOAMBIENTE	PLANES DE COOPERACIÓN LOCAL GESTIÓN DE LAS OBRAS PÚBLICAS MANTENIMIENTO DE ESPACIOS PÚBLICOS

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	ARCHIVO	-	-	[M]	-	-
S 02	BOLETÍN OFICIAL DE LA PROVINCIA	-	-	[M]	-	-
S 03	CONTRATACIÓN			[M]		
S 04	GESTIÓN ECONÓMICA, TRIBUTARIA Y CONTABLE	-	-	[M]	-	-
S 05	TESORERÍA	-	-	[M]	-	-
S 06	PERSONAL			[M]		
S 07	GESTIÓN TRIBUTARIA DE LOS MUNICIPIOS	-	-	[M]	-	-
S 08	SECRETARÍA			[M]		
S 09	SERVICIOS JURÍDICOS			[M]		
S 10	REGISTRO GENERAL	-	-	[M]	-	-
S 11	PARTICIPACIÓN CIUDADANA	-	-	[B]	-	-
S 12	ASESORAMIENTO TÉCNICO Y JURÍDICO A MUNICIPIOS	-	-	[M]	-	-
S 13	ADMINISTRACIÓN ELECTRÓNICA EN MUNICIPIOS	-	-	[M]	-	-
S 14	SEGURIDAD DE EDIFICIOS Y ACCESOS	-	-	[M]	-	-
S 15	INFORMÁTICA Y COMUNICACIONES	-	-	[M]	-	-
S 16	CULTURA			[B]		
S 17	JUVENTUD	-	-	[B]	-	-
S 18	PRESTACIONES SOCIALES	-	-	[M]	-	-
S 19	IGUALDAD Y VIOLENCIA DE GENERO	-	-	[M]	-	-
S 20	DEPORTES	-	-	[B]	-	-
S 21	PROMOCIÓN Y APOYO AL TURISMO	-	-	[B]	-	-
S 22	PROMOCIÓN DE ACTIVIDADES ECONÓMICAS Y DEL EMPLEO	-	-	[M]	-	-
S 23	CONSUMO	-	-	[B]	-	-
S 24	OBRAS PÚBLICAS Y MANTENIMIENTO DE INFRAESTRUCTURAS y EQUIPAMIENTOS	-	-	[B]	-	-
S 25	GESTIÓN DEL CICLO DEL AGUA. SANEAMIENTO	-	-	[B]	-	-
S 26	RECOGIDA DE RESIDUOS	-	-	[B]	-	-
S 27	DESARROLLO RURAL	-	-	[B]	-	-
S 28	EXTINCIÓN DE INCENDIOS Y PROTECCIÓN CIVIL	-	-	[M]	-	-
S 29	MEDIOAMBIENTE	-	-	[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] 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 LOS SERVICIOS		[D]
(Legislación vigente)	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
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 DEL ARCHIVO DE LA DIPUTACIÓN	[M]	[M]	-	[M]	[M]
I 02	ATENCIÓN A LA CIUDADANÍA	[B]	[M]	-	[M]	[M]
I 03	GESTIÓN DE LAS OBRAS PÚBLICAS	[M]	[B]	-	[B]	[B]
I 04	GESTIÓN DE LA INFORMACIÓN SOBRE EL CICLO DEL AGUA	[B]	[M]	-	[M]	[M]
I 05	ATENCIONES Y PRESTACIONES SOCIALES	[M]	[M]	-	[M]	[M]
I 06	AYUDAS Y SUBVENCIONES	[M]	[M]		[M]	[M]
I 07	GESTIÓN DEL SERVICIO DE EXTINCIÓN DE INCENDIOS	[M]	[M]	-	[M]	[M]
I 08	PROTECCIÓN CIVIL	[M]	[M]	-	[M]	[M]
I 09	PROCEDIMIENTOS SANCIONADORES	[M]	[M]	-	[M]	[M]
I 10	SERVICIOS TELEMÁTICOS Y COMUNICACIONES	[M]	[M]	-	[M]	[M]
I 11	PROCEDIMIENTOS TRIBUTARIOS	[M]	[M]	-	[M]	[M]
I 12	PROMOCIÓN DEL DEPORTE	[B]	[B]	-	[B]	[B]
I 13	PROMOCIÓN CULTURAL	[B]	[B]	-	[B]	[B]
I 14	FORMACIÓN	[B]	[B]	-	[B]	[B]
I 15	PROCEDIMIENTOS DE CONTRATACIÓN PÚBLICA	[B]	[M]	-	[M]	[M]
I 16	GESTIÓN DEL PERSONAL	[M]	[M]	-	[M]	[M]
I 17	PRESUPUESTOS, CONTABILIDAD, PAGOS Y FISCALIZACIÓN	[M]	[M]	-	[M]	[M]
I 18	ORGANOS DE GOBIERNO, DIPUTADOS Y REGISTRO DE BIENES E INTERESES	[M]	[M]	-	[M]	[M]
I 19	REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS	[M]	[M]	-	[M]	[M]
I 20	PARTICIPACIÓN CIUDADANA	[B]	[B]	-	[B]	[B]
I 21	SEGURIDAD DE INSTALACIONES	[M]	[B]	-	[B]	[B]
I 22	PROMOCIÓN DE ACTIVIDADES JUVENILES	[B]	[B]	-	[B]	[B]
I 23	CONTROL FINANCIERO	[M]	[M]	-	[M]	[M]
I 24	PLANES DE COOPERACIÓN LOCAL	[B]	[B]	-	[B]	[B]
I 25	MANTENIMIENTO DE ESPACIOS PÚBLICOS	[B]	[B]	-	[B]	[B]
I 26	GESTIÓN DE RESIDUOS MUNICIPALES	[B]	[B]	-	[B]	[B]
I 27	ACTIVIDADES DE TURISMO	[B]	[B]	-	[B]	[B]
I 28	GESTIÓN DE ACTIVIDADES EN TRANSPARENCIA	[S]	[B]	-	[B]	[B]
I 29	SERVICIOS DE CONSUMO	[B]	[B]	-	[B]	[B]

ID	INFORMACIÓN	[C]	[I]	[D]	[A]	[T]
I 30	GESTIÓN DEL ENTORNO RURAL	[B]	[B]	-	[B]	[B]
I 31	PROCESOS SELECTIVOS	[M]	[M]	-	[M]	[M]
I 32	INFORMES JURÍDICOS Y TÉCNICOS EN ASESORAMIENTO A MUNICIPIOS	[M]	[M]	-	[M]	[M]
I 33	MEDIDAS DE PROMOCIÓN ECONÓMICA Y DEL EMPLEO	[M]	[M]	-	[M]	[M]
I 34	PUBLICACIONES OFICIALES	[B]	[B]	-	[B]	[B]
I 35	SISTEMAS DE INFORMACIÓN	[M]	[M]	-	[M]	[M]
I 36	GESTIÓN DE LOS SISTEMAS DE ATENCIÓN A LA DEPENDENCIA Y OTRAS PRESTACIONES	[M]	[M]	-	[M]	[M]
I 37	VOLUNTARIADO	[M]	[M]	-	[M]	[M]
I 38	DEFENSA JURÍDICA Y RESPONSABILIDAD PATRIMONIAL	[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

VALORACIÓN DE LA INFORMACIÓN		[C]
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)[1]	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

[1] 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 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	
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		[I]
(Legislación vigente)[2]	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 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

[2] 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		[A]
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)[3]	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

[3] 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 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] 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		[T]
(Legislación vigente)[4]	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. CATEGORÍA DEL SISTEMA

El presente registro recoge la categorización del sistema de la Diputación de _____, 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 DE LA DIPUTACIÓN					
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]					

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

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 de la [DIPUTACIÓN/CABILDO/CONSEJO INSULAR/ÓRGANO COMPETENTE EQUIVALENTE] de _____

En adelante para referirnos a la Diputación, Cabildo, Consejo Insular u órgano competente equivalente, indicaremos órgano competente. Se establecen los siguientes supuestos:

- **Servicios alojados en el órgano competente**, donde el Perfil de Cumplimiento Específico será de aplicación al sistema de información del órgano competente.
- **Servicios del órgano competente 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 órgano competente desde el que se accede a los servicios.

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	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 sobre la normativa	MEDIO	Normativa de Uso de Recursos y Accesos a Sistemas de Información Curso la 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 ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	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 órgano competente, 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 órgano competente	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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 órgano competente	Cubierto por Conformidad ENS Documentación regular proporcionada por el proveedor sobre los recursos disponibles y consumidos
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 ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	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 mecanismos de autenticación de acceso a los servicios

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	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

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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
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 órgano competente 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 órgano competente para realizar cambios sobre el sistema que soporta los servicios

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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
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

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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)
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 órgano competente para la gestión incidentes y de comunicación de los mismos autoridades de control
op.exp.10	Protección de los registros 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

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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 órgano competente que se encuentren alojadas en el sistema que soporta los servicios
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

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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
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

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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
mp.if.3	Acondicionamiento de los locales	Todas	aplica	=	=	MEDIO	Procedimiento de Protección de las Instalaciones Herramientas sensores temperaturas y humedad Revisiones mantenimientos	MEDIO	Procedimiento de Protección de las Instalaciones Herramientas sensores temperaturas y 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	BAJO	Procedimiento de Protección de las Instalaciones Revisiones mantenimientos	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
							Informes pruebas de capacidad			
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 órgano competente	Cubierto por Conformidad ENS
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	

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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
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

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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
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

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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
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

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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
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	

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
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 ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	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 órgano competente	Cubierto por Conformidad ENS

Medidas de Seguridad		Dimensiones Afectadas	CATEGORÍA			SERVICIO ALOJADO ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	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 órgano competente	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el proveedor de coordinación con el órgano competente 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 ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	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 ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	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 órgano competente)	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 órgano competente	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 ÓRGANO COMPETENTE		SERVICIO EXTERNALIZADO		
			BÁSICA	MEDIA	ALTA	APLICA	JUSTIFICACIÓN	APLICA	JUSTIFICACIÓN	
							SISTEMA ÓRGANO COMPETENTE		SISTEMA ÓRGANO COMPETENTE	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 órgano competente	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%

En adelante para referirnos a la Diputación, Cabildo, Consejo Insular o órgano competente equivalente, indicaremos órgano competente. Se establecen los siguientes supuestos:

- **Servicios alojados en el órgano competente**, donde el Perfil de Cumplimiento Específico será de aplicación al sistema de información del órgano competente.
- **Servicios del órgano competente 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 órgano competente desde el que se accede a los servicios.

		SERVICIO ÓRGANO COMPETENTE		SERVICIO DEL ÓRGANO COMPETENTE EXTERNALIZADO		
Medidas de Seguridad		APLICA	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA ÓRGANO COMPETENTE 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

[5] Sistema que dispone de la conformidad ENS en categoría MEDIA

Medidas de Seguridad		SERVICIO ÓRGANO COMPETENTE		SERVICIO DEL ÓRGANO COMPETENTE EXTERNALIZADO		
		APLICA	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO	SISTEMA EXTERNALIZADO NIVEL DE MADUREZ ALCANZADO
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
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

Medidas de Seguridad		SERVICIO ÓRGANO COMPETENTE		SERVICIO DEL ÓRGANO COMPETENTE EXTERNALIZADO		
		APLICA	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO	SISTEMA EXTERNALIZADO NIVEL DE MADUREZ ALCANZADO
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
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

Medidas de Seguridad		SERVICIO ÓRGANO COMPETENTE		SERVICIO DEL ÓRGANO COMPETENTE EXTERNALIZADO		
		APLICA	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO	SISTEMA EXTERNALIZADO NIVEL DE MADUREZ ALCANZADO
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
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 la Diputación/Cabildo/Consejo Insular/ órgano competente equivalente 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.

Nota: en adelante para referirnos a la Diputación, Cabildo, Consejo Insular o órgano competente equivalente, indicaremos órgano competente.

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 virtuales (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 órgano competente 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 quiénn 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 órgano competente: • 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 órgano competente: • 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 órgano competente 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 órgano competente, y con otros sistemas interconectados comunicaciones con el órgano competente, 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 órgano competente 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 órgano competente 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 órgano competente 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 (requerido 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