Política de Seguridad

AJUNTAMENT DE PATERNA

28/11/2023

Control de Cambios

Versión	Fecha	Autor	Descripción del Cambio
1.0	28/02/2023	Ajuntament de Paterna	Versión inicial adaptación al ENS, RD 311/2022 de 3 de mayo
1.1	28/11/2023	Ajuntament de Paterna	Adaptación logos PRTR

ÍNDICE

1. INTRODUCCIÓN

1.1 JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El "AJUNTAMENT DE PATERNA" 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. Es por ello que el Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, “ENS” en adelante), en su artículo 12 establece que *“Cada Administración Pública contará con una política de seguridad formalmente aprobada por el órgano competente”.*

Esto implica que las diferentes áreas del "AJUNTAMENT DE PATERNA" 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.

Todas las áreas deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC. Los departamentos deben estar preparados para la prevención, detección, respuesta y conservación en caso de incidentes, de acuerdo con el artículo 8 del ENS.

1.2 MISIÓN Y SERVICIOS PRESTADOS

El "AJUNTAMENT DE PATERNA" para la gestión de sus intereses, y en el ámbito de sus competencias y como Administración pública, sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de los habitantes del municipio.

La presente Política de Seguridad aplica a las diferentes actividades en las que participa el "AJUNTAMENT DE PATERNA" a través de medios electrónicos, en concreto:

a) Las relaciones de carácter jurídico-económico entre los ciudadanos y el ayuntamiento.

b) La consulta por parte de los ciudadanos de la información pública administrativa y de los datos administrativos que estén en poder del ayuntamiento.

c) La realización de los trámites y procedimientos administrativos incorporados para su tramitación en la Sede Electrónica del AJUNTAMENT DE PATERNA.

d) El tratamiento de la información obtenida por el "AJUNTAMENT DE PATERNA" en el ejercicio de sus potestades.

2. MARCO NORMATIVO

Como base normativa para realizar la presente guía de seguridad, se ha analizado la legislación vigente, que afecta al desarrollo de las actividades de la Administración Local 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. El marco legal en materia de seguridad de la información viene establecido principalmente por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que señala en su art. 17.3 que los medios o soportes en que se almacenen documentos , deberán contar con las medidas de seguridad que establece el Esquema Nacional de Seguridad, que garanticen una serie de principios (como integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados); y, establece también, en su art. 27.3 que las Administraciones Públicas deberán cumplir con el Esquema Nacional de Seguridad para garantizar la identidad y contenido de las copias electrónicas o en papel, es decir, el carácter de copias auténticas. Por último, dispone en su Disposición Adicional segunda que, tanto las Comunidades Autónomas, como las Entidades

Locales, deberán garantizar su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes registros y plataformas mediante el cumplimiento, igualmente, del Esquema Nacional de Seguridad. Y que, además, deroga la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

- El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.

- 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, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

- 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 (en adelante RGPD).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. ORGANIZACIÓN DE LA SEGURIDAD

3.1 DEFINICIÓN DE ROLES

Tal como indica el artículo 13 del ENS, la seguridad de los sistemas de información deberá comprometer a **todos los miembros** de la Organización. La Política de Seguridad, según detalla el Anexo II del ENS, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa. Se establecen los siguientes roles en la Organización relacionados con la Seguridad de la Información:

3.1.1 Responsable de la Información

Se ha designado Responsable de la Información a la **Junta de Gobierno Local (en adelante, "JGL")** a quien le corresponden las siguientes funciones:

- Adoptar las **medidas de índole técnica y organizativas** necesarias que garanticen la seguridad de los tratamientos de datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

- Tiene la responsabilidad última del **uso** que se haga de una cierta información y, por tanto, de su **protección**.

- El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un **incidente** de **confidencialidad** o de **integridad**.

- Establece los **requisitos de la información** en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

- Determinará los **niveles de seguridad en cada dimensión** dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, este podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

3.1.2 Responsables del Servicio

Se ha designado responsables del Servicio **a cada uno de los responsables que constan en el presente apartado**, a quienes les corresponde las siguientes funciones:

- En cuanto al RGPD, por delegación del Responsable del tratamiento, se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la **gestión de los tratamientos** de datos personales que se realizan en su **Área** en concreto.

- Establece los **requisitos de los servicios** en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

- Tiene la responsabilidad última del **uso** que se haga de determinados servicios y, por tanto, de su **protección**.

- El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un **incidente de disponibilidad** de los servicios.

- Determinará los **niveles de seguridad en cada dimensión** del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, este podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

- La prestación de un **servicio** siempre debe atender a los **requisitos de seguridad** de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de esta, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

En el **Anexo II** de la presente política se incorpora la relación de servicios y los responsables de los mismos.

3.1.3 Responsable de Seguridad de la Información

Se ha designado como Responsable de Seguridad de la Información al **Teniente de Alcalde** que tenga delegadas las **competencias** en materia de **Tecnologías de la Información y Comunicaciones**, a quien le corresponderán las siguientes funciones:

- **Coordinará** y **controlará** las medidas definidas en el Registro de Actividades del Tratamiento y, en general, se encargará de la **aplicación** de las medidas de seguridad que detalla el informe de evaluación de impacto en la protección de datos.

- **Mantendrá** la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la **Política de Seguridad** de la Organización.

- Promoverá la **formación** y **concienciación** en materia de seguridad de la información dentro de su ámbito de responsabilidad.

- Recopilará los **requisitos de seguridad** de los Responsables de Información y Servicio y determinará la **categoría del Sistema**.

- Realizará y aprobará el **Análisis de Riesgos**.

- Elaborará y aprobará una **Declaración de Aplicabilidad** a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.

- Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones

de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.

- Coordinará la elaboración de la **Documentación** de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la **Política de Seguridad** de la Información para su aprobación por Dirección.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la **normativa de Seguridad** de la Información.

3.1.4 Responsable del Sistema

Se ha designado como Responsable del Sistema a la **Directora Técnica de Organización y Modernización-TIC (en adelante, "D-OMTIC")**, a quien le corresponden las siguientes funciones:

- Desarrollar, operar y mantener el **Sistema de Información** durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la **topología** y **sistema de 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.
- El Responsable del Sistema puede **acordar la suspensión** del manejo de una cierta información o la prestación de un cierto servicio si es informado de **deficiencias graves de seguridad** que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Aplicar los **procedimientos operativos de seguridad** elaborados y aprobados por el Responsable de Seguridad.
- Monitorizar el **estado de la seguridad** del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.

- Elaborar los **Planes de Continuidad** del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.

- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos **actualizados** y verificar que son **efectivos**.

- Elaborará las **directrices** para garantizar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

- Elaborará y aprobará los **Procedimientos Operativos** de Seguridad de la Información.

- Facilitará periódicamente al Comité de Seguridad un **resumen de actuaciones** en materia de seguridad, de **incidentes** relativos a seguridad de la información y del **estado** de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).

- **Reportará** el estado de situación y acciones llevadas a cabo en ejercicio de las anteriores funciones al Comité de Seguridad de la Información.

3.1.5 Responsable de la explotación del Sistema

Se ha designado como Responsable de la explotación del sistema al **Jefe del Servicio de Seguridad, Sistemas y Comunicaciones (en adelante, "JSSC")** al que, como tal, le corresponden las siguientes funciones:

- La implementación, gestión y mantenimiento de las **medidas de seguridad** aplicables al Sistema de Información.

- Asegurar que los **controles de seguridad** establecidos son cumplidos estrictamente.

- Asegurar que la **trazabilidad**, **pistas de auditoría** y otros **registros de seguridad** requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la Política de Seguridad establecida por la Organización.

- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los **Procedimientos Operativos** de Seguridad y los mecanismos y servicios de seguridad requeridos.

- Asegurar que son aplicados los **procedimientos aprobados** para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.

- La gestión, **configuración** y **actualización**, en su caso, del **hardware** y **software** en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.

- Supervisar las **instalaciones** de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.

- Aprobar los **cambios** en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.

- Informar a los Responsables de la Seguridad y del Sistema de cualquier **anomalía**, **compromiso** o **vulnerabilidad** relacionada con la seguridad.

- Monitorizar el **estado** de la seguridad del sistema.

En caso de ocurrencia de incidentes de seguridad de la información:

- Llevar a cabo el **registro**, **contabilidad** y **gestión** de los incidentes de seguridad en los Sistemas bajo su responsabilidad.

- Ejecutar el **plan de seguridad** aprobado.

- **Aislar el incidente** para evitar la propagación a elementos ajenos a la situación de riesgo.

- Tomar **decisiones** a **corto plazo** si la información se ha visto comprometida de tal forma que pudiera tener **consecuencias graves** (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).

- Asegurar la **integridad** de los **elementos críticos** del Sistema si se ha visto afectada la **disponibilidad** de los mismos (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).

- **Mantener** y **recuperar** la información almacenada por el Sistema y sus servicios asociados.

- **Investigar** el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.

3.1.6 Responsable de Seguridad Física

Se ha designado como responsable de Seguridad Física a la **Jefatura de la Policía Local**, al que le corresponderá implantar las medidas de seguridad que le competan dentro de las determinadas por el responsable de la Seguridad de la Información e informará a éste de su grado de implantación, eficacia e incidentes.

3.1.7 Responsable de Gestión de Personal

Se ha designado como responsable de Gestión de Personal al **Jefe de Personal**, al que le corresponde implantar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

3.2 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Se crea el **Comité de Seguridad de la Información** compuesto por los siguientes miembros:

- **Presidencia:** Alcaldía o concejal en quien delegue.
- **Secretario:** Jefe de Área de atención a la ciudadanía.
- **Vocales:**
    - Responsable de Seguridad de la Información.
    - Secretaria General.
    - Delegado de Protección de Datos (DPD).
    - Responsable del Sistema.
    - Responsable de la explotación del Sistema.

Podrán acudir a requerimiento del Comité el Responsable de la Seguridad Física y Responsable de Gestión de Personal o cualquier otro Responsable de Servicio cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad y por el RGPD.

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

- Atender las **inquietudes** de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del **estado de la seguridad** de la información a la Alta Dirección.
- Promover la **mejora continua** del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la **estrategia de evolución** del "AJUNTAMENT DE PATERNA" en lo que respecta a la seguridad de la información.
- Coordinar los **esfuerzos** de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son **consistentes**, **alineados** con la estrategia decidida en la materia, y **evitar duplicidades**.

- Elaborar (y revisar regularmente) la **Política de Seguridad** de la información para que sea aprobada por la Dirección.

- Aprobar la **normativa de seguridad** de la información.

- Elaborar y aprobar los **requisitos de formación** y **calificación** de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

- Monitorizar los principales **riesgos residuales** asumidos por el "AJUNTAMENT DE PATERNA" y recomendar posibles **actuaciones** respecto de ellos.Monitorizar el desempeño de los **procesos de gestión de incidentes** de seguridad y recomendar posibles **actuaciones** respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

- Promover la realización de las **auditorías periódicas** que permitan verificar el **cumplimiento** de las obligaciones del organismo en materia de seguridad.

- Elaborar y aprobar **planes de mejora** de la seguridad de la información del AJUNTAMENT con su do. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

- Velar para que la seguridad de la información se tenga en cuenta en todos los **proyectos** que directa o indirectamente tengan algún componente TIC 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.

- Resolver los **conflictos de responsabilidad** que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

- Recabará regularmente del personal técnico propio o externo, la **información pertinente** para tomar **decisiones**.

- Se asesorará de los temas que tenga que decidir o emitir una opinión. Este **asesoramiento** se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

    - Grupos de trabajo especializados internos, externos o mixtos.

    - Asesoría interna y/o externa.

- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

- Elaborará y aprobará los **Planes de Formación y Concienciación** del personal en Seguridad de la Información.

- Validará y aprobará los **Planes de Continuidad** de Sistemas que elabore el Responsable de Sistemas, y que deberán ser probados periódicamente por éste.

- Aprobará las **directrices** propuestas por los **Responsables de Sistemas** para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

3.3 JERARQUÍA EN EL PROCESO DE DECISIONES Y MECANISMOS DE COORDINACIÓN

1. El **Comité de Seguridad de la Información**:

   - toma las decisiones para coordinar la seguridad de la información en el Ayuntamiento.

2. El **Responsable de la Seguridad** (Teniente de Alcalde):

   - informa al Responsable de la Información (JGL) de las decisiones e incidentes en materia de seguridad que afecten a la **información** que le compete, en particular de la estimación de **riesgo residual** y de las **desviaciones** significativas de riesgo respecto de los márgenes aprobados.

   - informa al Responsable del Servicio (Anexo II) de las decisiones e incidentes en materia de seguridad que afecten al **servicio** que le compete, en particular de la estimación de **riesgo residual** y de las **desviaciones** significativas de riesgo respecto de los márgenes aprobados.

   - Es responsable de la **ejecución** directa o delegada de las **decisiones** del Comité.

3. El **Responsable del Sistema** (D-OMTIC):

   - Informa al Responsable de la Información (JGL) de las **incidencias funcionales** relativas a la **información** que le compete.

- Informa al Responsable del Servicio (Anexo II) de las **incidencias funcionales** relativas al **servicio** que le compete.

- Reporta al Responsable de la Seguridad (Teniente de Alcalde):

  ✓ actuaciones en materia de seguridad, en particular en lo relativo a **decisiones de arquitectura** del sistema.

  ✓ Resumen consolidado de los **incidentes** de seguridad.

  ✓ Medidas de la eficacia de las **medidas de protección** que se deben implantar.

- Reporta al Comité de Seguridad de la Información:

  ✓ Resumen consolidado de **actuaciones** en materia de seguridad.

  ✓ Resumen consolidado de **incidentes** relativos a la seguridad de la información.

  ✓ El estado de la seguridad del sistema, en particular del **riesgo residual** al que el sistema está expuesto.

- Reporta al Delegado de Protección de Datos (DPD):

  ✓ Resumen consolidado de **incidentes** relativos a protección de datos personales.

4. El **Responsable de Explotación del Sistema** (JSSC):

   - reporta al Responsable del Sistema (D-OMTIC):

     ✓ **Incidentes** relativos a la seguridad del sistema.

     ✓ **Acciones** de configuración, actualización o corrección.

5. El **Secretario del Comité de Seguridad**:

   - **Informa** a la Junta de Gobierno como Responsable de la Información de lo acordado en el Comité de Seguridad.

   - **Convocará** al Comité de Seguridad de la Información, recopilando la información pertinente.

- Preparará los **temas a tratar** en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el **acta** de las reuniones.

Procedimientos de designación de personas

La Alcaldía/Presidencia nombrará formalmente:

- Al Responsable de la Información.
- A los Responsables del Servicio.
- Al Responsable de la Seguridad.
- Al Responsable de Explotación del Sistema.
- Al Responsable del Sistema.

3.4 REQUISITOS MÍNIMOS DE SEGURIDAD

Atendiendo al cumplimiento del Esquema Nacional de Seguridad, se garantizará el cumplimiento de los siguientes requisitos mínimos:

a) Organización e implantación de la organización de la seguridad: detallada en el apartado 3 de la presente política.

b) Análisis y gestión de los riesgos: detallado en el apartado 5 de la presente política.

c) Obligaciones de personal: detallado en el apartado 7 de la presente política.

d) Profesionalidad: la seguridad de los sistemas estará atendida revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidentes y desmantelamiento. El personal del "AJUNTAMENT DE PATERNA" recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.

El "AJUNTAMENT DE PATERNA" exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

e) Autorización y control de los accesos: el acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

f) Protección de las instalaciones: los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas permanecerán cerradas y dispondrán de un control de llaves.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad: en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por el "AJUNTAMENT DE PATERNA" se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que 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.

La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

Para la contratación de servicios de seguridad se estará a lo dispuesto en el Esquema Nacional de Seguridad.

h) Mínimo privilegio: los sistemas se diseñarán y configurarán de manera que garanticen la seguridad por defecto:

- El sistema proporcionará la **mínima funcionalidad** requerida para que la organización alcance sus objetivos.

- 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.

- 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.

- Se garantizará que el **uso ordinario** del sistema sea sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

i) Integridad y actualización del sistema: Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se conocerá en todo momento el estado de 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.

j) Protección de la información almacenada y en tránsito: En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

k) Prevención ante otros sistemas de información interconectados: El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas.

Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

l) Registro de actividad y detección de código dañino: Con la finalidad exclusiva de lograr el cumplimiento del objeto del Esquema Nacional de Seguridad con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

m) Incidentes de seguridad: se desarrolla en el apartado 6 de la presente Política.

n) Continuidad de la actividad: Los sistemas del "AJUNTAMENT DE PATERNA" 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.

o) Mejora continua del proceso de seguridad. El proceso integral de seguridad implantado será actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

4. DATOS DE CARÁCTER PERSONAL

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. El Registro de Actividades del Tratamiento detalla los tratamientos que se llevan a cabo en el Ayuntamiento y los responsables correspondientes. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades del Tratamiento.

4.1 FIGURAS VINCULADAS A PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

4.1.1 Responsable del Tratamiento

El Responsable del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento.

A efectos de la entidad local se ha atribuido la condición de Responsable de Tratamiento a la persona jurídico-pública, es decir, al propio **"AJUNTAMENT DE PATERNA"**. De manera que, se ha entendido que el "AJUNTAMENT DE PATERNA" es Responsable del Tratamiento de los datos de carácter personal, que obran en sus sistemas de información, y que derivan de la prestación de los servicios públicos atribuidos a nivel de competencias.

A su vez, cabe decir que la consideración de Responsable de Tratamiento no debe ser asociada a persona física representante del AJUNTAMENT, en calidad del cargo o puesto (como por ejemplo, el Alcalde o Secretario).

Las funciones y obligaciones del Responsable del tratamiento son:

- Adoptar las **medidas de índole técnica y organizativas** necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

- Deberá informar a los **titulares de los datos** los **derechos** que les asisten y en los **términos** en los que pueden ejercerlos.

- Deberá **excluir** del tratamiento los datos relativos al afectado que se oponga al tratamiento de los mismos.

- Cumplir con **la prohibición de la recogida de datos personales de fuentes ilegítimas**, de fuentes que no garanticen suficientemente su legítima procedencia o de fuentes cuyos datos hayan sido recabados o cedidos incumpliendo la ley. Facilitar a los interesados el ejercicio de los derechos de acceso, rectificación, supresión y portabilidad de los datos, de oposición y limitación del tratamiento. Deberá **cesar** cualquier utilización o cesión ilícita de los datos.

- Obligación de hacer efectivo **todos los derechos en materia de protección de datos** del interesado en el plazo máximo de 1 mes.

- Notificar las **rectificaciones** o **cancelaciones** efectuadas en los datos personales a quien se haya comunicado dichos datos, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

- Mantener un **registro de actividades de tratamiento** como Responsable y/o Encargado de Tratamiento.

- **Colaborar** con las Autoridades de Control pertinentes.

4.1.2 Delegado de Protección de Datos (DPD).

El DPD puede ser una persona física o un órgano colegiado, cuyas funciones se señalan en el artículo 39 del Reglamento (UE) 679/2016, así como los artículos 36 y 37 de la Ley

Orgánica 3/2018, y se ocupa de la aplicación de la legislación sobre privacidad y protección de datos en la entidad en la que desarrolla sus funciones.

El "AJUNTAMENT DE PATERNA" ha nombrado Delegado de Protección de Datos a la empresa SOTHIS TECNOLOGÍAS DE LA INFORMACIÓN SLU.

El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Para ello deberá **ser capaz de**:

a) Recabar información para determinar las actividades de tratamiento,

b) analizar y comprobar la conformidad de las actividades de tratamiento, e

c) informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.

d) Recabar información para supervisar el registro de las operaciones de tratamiento.

e) Asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.

f) Asesorar sobre:

- Si se debe llevar a cabo o no una evaluación de impacto de la protección de datos.
- Qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos.
- Si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
- Qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos de intereses de los afectados.
- Si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y
- Si sus conclusiones son conformes al Reglamento (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar).

g) Priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.

h) Asesorar al responsable del tratamiento sobre:

- Qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos.
- Qué áreas deben someterse a auditoría de protección de datos interna o externa.
- Qué actividades de formación internas proporcionar al personal o a los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de los datos. Se han identificado, en consecuencia, aquellos **conocimientos, habilidades o destrezas necesarias** que tiene que saber o poseer el Delegado de Protección de Datos para llevar a cabo una de las funciones propias de su puesto.

Estas funciones genéricas del DPD se pueden concretar en tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.

2. Identificación de las bases jurídicas de los tratamientos.

3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

4. Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.

5. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.

6. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.

7. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.

8. Asesoramiento y supervisión de la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.

9. Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.

10. Diseño e implantación de políticas de protección de datos.

11. Auditoría de protección de datos.

12. Establecimiento y gestión de los registros de actividades de tratamiento.

13. Análisis de riesgos de los tratamientos realizados.

14. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.

15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

16. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.

17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.

18. Realización de evaluaciones de impacto sobre la protección de datos.

19. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida las consultas previas.

20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

4.1.3 Usuarios con acceso a datos personales

Todos los empleados de la entidad están sujetos a funciones y obligaciones. Todo el personal de la entidad que disponga de **acceso a los datos de carácter personal** debe cumplir con las siguientes obligaciones:

- No se permite la difusión de datos de carácter personal ni confidencial perteneciente a la entidad. Estando obligado a guardar **secreto de la información** incluso terminada la relación laboral.

- El usuario se responsabilizará de **notificar toda incidencia** según el procedimiento de gestión de incidencias, no notificar una incidencia será considerada una omisión del deber del trabajador.

- El usuario se responsabilizará de todos los accesos que se realicen bajo su identificador y contraseña, por tanto, **no deberá revelar la contraseña**.

- El usuario se responsabilizará siempre que abandone el puesto de trabajo de **cerrar su sesión o bloquear el equipo** con contraseña.

- No se permite la **copia de datos** de carácter personal, en soportes, sin la **autorización** expresa del Responsable de seguridad y/o del Responsable del Sistema.

4.1.4 Encargado del Tratamiento

Los encargados del tratamiento tienen como misión realizar las tareas ordinarias para el desarrollo efectivo de las funciones para las que ha sido creado el tratamiento por cuenta del Responsable del tratamiento.

En este sentido, el **apartado 8 del artículo 4 del RGPD** define al Encargado de Tratamiento como <<la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento>>.

El Encargado del Tratamiento deberá aplicar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Igualmente deberá implementar las **medidas de seguridad** a que se refiere el párrafo anterior y que aparecerán estipuladas en el **contrato** con el Responsable del Tratamiento.

En concreto, sus funciones son las de:

- Tratar los datos del tratamiento por cuenta y en nombre del Responsable.
- Realizar el **control de tratamiento**, calidad y seguridad de los datos.
- Controlar la forma y requisitos para proceder a las **adiciones** y **cancelaciones**.
- Controlar los **soportes de seguridad**.
- Control y acceso de **contraseñas**.
- Mantenimiento del **registro de incidencias**.
- Crear una lista para las situaciones en la que un **afectado** no desee que sus datos personales se almacenen en el tratamiento.
- Dar traslado al responsable del tratamiento de aquellas **solicitudes** de **ejercicio de derecho** que se reciban por parte de los interesados.

5. GESTIÓN DE RIESGOS

5.1 JUSTIFICACIÓN

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el artículo 7 del ENS.

5.2 CRITERIOS DE EVALUACIÓN DE RIESGOS

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

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

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

5.3 DIRECTRICES DE TRATAMIENTO

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

5.4 PROCESO DE ACEPTACIÓN DEL RIESGO RESIDUAL

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

Los niveles de Riesgo residuales esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de esa Información.

Los niveles de Riesgo residuales esperados sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de ese Servicio.

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

5.5 NECESIDAD DE REALIZAR O ACTUALIZAR LAS EVALUACIONES DE RIESGOS

El análisis de los riesgos y su tratamiento deben ser una actividad continua y permanentemente actualizada, según lo establecido en el artículo 7 del ENS. Este análisis se repetirá:

- Regularmente, al menos **una vez al año**.
- Cuando se produzcan **cambios significativos** en la **información** manejada.
- Cuando se produzcan **cambios significativos** en los **servicios** prestados.
- Cuando se produzcan **cambios significativos** en los **sistemas** que tratan la información e intervienen en la prestación de los servicios.

- Cuando ocurra un **incidente grave de seguridad**.

- Cuando se reporten **vulnerabilidades graves**.

5.6 RIESGOS QUE SE DERIVAN DEL TRATAMIENTO DE DATOS PERSONALES

Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

6. GESTIÓN DE INCIDENTES DE SEGURIDAD

6.1 PREVENCIÓN DE INCIDENTES

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. El ENS a través de su artículo 20 establece la que los sistemas deben diseñarse y configurarse de forma que garanticen el principio de mínimo privilegio. De igual forma, el ENS establece que los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

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

Para garantizar el cumplimiento de la política, la Dirección Técnica de Organización y Modernización-TIC, debe:

- Establecer **áreas seguras** para los sistemas de información crítica o confidencial.

- Autorizar los sistemas antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

6.2 MONITORIZACIÓN Y DETECCIÓN DE INCIDENTES

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 8 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

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

Los sistemas de detección y monitorización de incidentes actuarán a nivel de red y sistema.

6.3 RESPUESTA ANTE INCIDENTES

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

6.4 RECUPERACIÓN ANTE INCIDENTES Y PLANES DE CONTINUIDAD

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

7. OBLIGACIONES DEL PERSONAL

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

Todos los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un **programa de concienciación continua** para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Atendiendo a los requisitos de profesionalidad, las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

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

8. TERCERAS PARTES

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Conforme a lo dispuesto en el artículo 13.5 ENS, en el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de

dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

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

9. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será **revisada** por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por Alcaldía/Presidencia.

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

10. DOCUMENTACIÓN COMPLEMENTARIA

La Política de Seguridad de la Información se complementará con documentos más precisos que ayudan a llevar a cabo lo propuesto. Para ello se utilizarán:

- **Normas de seguridad**
- **Guías de seguridad**.
- **Procedimientos de seguridad**.

Las **normas** uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter **obligatorio**.

Las **guías** tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los **procedimientos** [operativos] de seguridad afrontan **tareas concretas**, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

En relación a la **calificación de la información**, aquella documentación que contenga información confidencial, se etiquetará como tal mediante marcas de agua en el propio

documento, menciones al contenido confidencial en el pie de página o fórmulas alternativas que dejen constancia de la restricción de acceso en el documento o soporte.

ANEXO I. GLOSARIO DE TÉRMINOS

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables.

Gestión de incidentes

Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Información

Caso concreto de un cierto tipo de información.

Política de seguridad

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.

Principios básicos de seguridad

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información

Órgano o persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que por sí o a través de recursos propios o contratados, se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Responsable de la explotación del sistema

Persona que se encarga de la explotación del sistema de información.

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

ANEXO II. RELACIÓN DE SERVICIOS Y RESPONSABLES

Se relacionan a continuación los servicios prestados por el Ayuntamiento dentro del alcance del Esquema Nacional de Seguridad con los Responsables de cada uno de ellos:

Servicio	Responsable del Servicio
Urbanismo	Jefe de Área de Sostenibilidad y Vertebración Territorial
Medio Ambiente Urbano	Jefe de Área de Sostenibilidad y Vertebración Territorial
Medio Ambiente Rural	Jefe de Área de Servicios Municipales
Aguas, Saneamiento y recogida de residuos	Jefe de Área de Servicios Municipales
Mantenimiento e Infraestructuras	Jefe de la Oficina Técnica Municipal
Bienestar Social	Jefe de Área de Promoción Económica y Empleo
Actuaciones Sociales y Atención a la Dependencia	Jefe de Área de Promoción Económica y Empleo
Seguridad Ciudadana y Protección Civil	Jefe de Policía Local
Transporte Público	Jefe de Área de Servicios Municipales
Promoción de la Entidad Local	Coordinador del Servicio de Industria, Empresa y Universidad
Comercio y Mercados	Jefe de Área de Promoción Económica y Empleo
Servicios Funerarios	Jefe de Área de Servicios Municipales
Deportes	Jefe de Servicios Deportivos
Cultura	Jefa de área de Promoción y Dinamización
Educación y Formación	Técnico de Educación
Escuelas Infantiles	Técnico de Educación
Igualdad	Técnica de Igualdad
Registro General	Jefe de Área de Servicios Municipales
Archivo	Archivero Municipal
Contratación	Jefa de Área de Obras y Contratación
Participación Ciudadana	Jefa de área de Promoción y Dinamización
Intervención	Interventor Municipal
Gestión Tributaria	Jefa de Área de Gestión Municipal
Tesorería	Tesorera Municipal
Personal	Jefe de gestión de RRHH
Vivienda	Jefe de Área de Sostenibilidad y Vertebración Territorial
Informática y Comunicaciones	Directora Técnica de Organización y Modernización-TIC

Juventud	Técnica de Juventud
Secretaría Municipal	Secretaria General
Estadística	Jefa de Área de Gestión Municipal
Gestión Urbanismo Municipal	Jefe de Área de Sostenibilidad y Vertebración Territorial
Licencias, Autorizaciones y Concesiones	Jefe de Área de Sostenibilidad y Vertebración Territorial
Atención a la Ciudadanía	Jefa del Servicio de Información y Atención a la Ciudadanía
Gestión del Ciclo del Agua y Residuos	Jefe de Área de Servicios Municipales
Gestión de las Obras Mantenimiento e Infraestructuras	Jefe de la Oficina Técnica Municipal
Promoción de la Vivienda	Jefe de Área de Promoción Económica y Empleo
Atenciones y Prestaciones Sociales	Jefe de Área de Promoción Económica y Empleo
Gestión de los Sistemas de Atención a la Dependencia y otras Prestaciones	Jefe de Área de Promoción Económica y Empleo
Ayudas y Subvenciones	Jefa de área de Promoción y Dinamización
Policía Local	Jefe de Policía Local
Protección Civil	Jefe de Policía Local
Gestión de la Movilidad Urbana	Jefe de Área de Servicios Municipales
Procedimientos Sancionadores	Jefe de Área de Servicios Municipales
Servicios Telemáticos y Comunicaciones	Directora Técnica de Organización y Modernización-TIC
Gestión de Servicios Funerarios	Jefe de Área de Servicios Municipales
Gestión de Ingresos Públicos	Tesorera Municipal
Gestión de Servicios Deportivos	Jefa de Área de Gestión Municipal
Gestión de Servicios Culturales	Jefa de área de Promoción y Dinamización
Gestión de Servicios Educativos	Jefe de Área de Promoción Económica y Empleo
Gestión del Archivo Municipal	Archivero Municipal
Gestión de las Escuelas Infantiles	Jefe de Área de Promoción Económica y Empleo
Contratación Pública	Jefa de Área de Obras y Contratación
Gestión del Personal	Jefe de Gestión de RRHH
Gestión Presupuestaria Económica y Contable	Interventor Municipal
Gestión de los Órganos Municipales de Gobierno	Secretaria General
Padrón Municipal de Habitantes	Jefa de Área de Gestión Municipal
Registro de Entrada y Salida de Documentos	Jefe de Área de Servicios Municipales
Defensa Jurídica	Letrada Municipal

Responsabilidad Patrimonial	Jefe de Área de Servicios Municipales
Seguridad de Instalaciones Municipales	Jefe de Policía Local
Gestión de Servicios Juveniles Municipales	Jefa de área de Promoción y Dinamización
Gestión de la Participación Ciudadana	Jefa de área de Promoción y Dinamización
Voluntariado	Jefa de área de Promoción y Dinamización
Gestión de la Promoción Local y el Turismo	Jefa de área de Promoción y Dinamización
Promoción de la Administración Electrónica	Jefe de Área de Servicios Municipales
Sistemas de Información	Directora Técnica de Organización y Modernización-TIC

www.tech.telefonica.com/es