Esquema Nacional de Seguridad (ENS)

POLÍTICA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN

Julio 2023

Clasificación: Público

Código	Versión	Fecha	Modificación
POL-001P	0.9	12-2017	Creación NEXTEL
POL-001P	1.0	05-2018	Modificaciones y validaciones Ayto
POL-001P	2.0	11-2019	Aprueba Comité TICS
POL-001P	3.0	07-2023	Actualización nuevo RD

Elaborado por:	Revisado por	Aprobado por	Responsable Documento
RSIS	Comité de Seguridad; Comité TICS	Junta de Gobierno Local	Responsable de Seguridad

CONTENIDOS

0 Introducción

El "Ayuntamiento de Pamplona-Iruñeko Udala" -en adelante Ayuntamiento de Pamplona- asume que la información que maneja para ejercitar sus competencias es un activo de gran valor. La gestión de dicha información tiene importantes implicaciones tanto para la efectividad y eficiencia de la organización como para las libertades y derechos de las personas físicas y jurídicas con las que se relaciona. El objetivo de esta política consiste por tanto en regular los agentes y mecanismos que permitan realizar dicha gestión de manera operativa, coherente y segura.

De acuerdo con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica y que establece en su artículo 12 y en la medida org.1 del Anexo II que "*las Administraciones Públicas deberán disponer formalmente de una Política de Seguridad, que será aprobada por el titular del órgano superior competente*", ésta deberá presentar al menos estos contenidos:

- los objetivos o misión de la organización,
- el marco regulatorio en el que se desarrollarán las actividades,
- Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación,
- la estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización,
- las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso,

- la Política de Seguridad de la Información identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

Es el instrumento en el que se apoya "Ayuntamiento de Pamplona-Iruñeko Udala" -en adelante Ayuntamiento de Pamplona- para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad, concebida como proceso integral, comprende todos los activos o elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en el Ayuntamiento de Pamplona.

1 Principios de Seguridad

La presente política integra conceptos esenciales de seguridad de la información que se fundamentan en los principios básicos de protección descritos en la Tabla 1. Dichos principios conforman los pilares sobre los que se sustentan y sustentarán las actuaciones en materia de seguridad que realice el Ayuntamiento de Pamplona en el desarrollo de su actividad:

Tabla 1: Principios de Seguridad

#	Principio	Descripción
1	**La Seguridad como proceso integral**	La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, excluyendo 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 fuentes de riesgo para la seguridad. Los requerimientos de la seguridad de la información se atenderán durante todo el ciclo de vida de los activos, desde su planificación hasta su retirada.

2	**Gestión del riesgo**	El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado. Gestionar la seguridad de la información consistirá en analizar los riesgos, estableciéndose medidas de seguridad adecuadas, eficaces y proporcionadas que permitan el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Se deberán contemplar medidas de prevención, detección y corrección para evitar amenazas y que éstas, si se producen, no afecten gravemente a la información y servicios prestados.
3	**Disponibilidad, continuidad y conservación**	Se deberá procurar que los activos estén disponibles cuando lo requieran las personas autorizadas para acceder a ellos. Para ello, se garantizará la prestación continuada de los servicios y la rápida recuperación ante posibles contingencias, mediante medidas de continuidad orientadas a la restauración de los servicios y de la información asociada. Así mismo se garantizará la conservación de los datos e informaciones en soporte electrónico.
4	**Integridad**	Se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.
5	**Confidencialidad**	Se deberá garantizar que los activos sean accesibles únicamente para aquellas personas expresamente autorizadas para ello.
6	**Autenticidad**	Se deberá garantizar que la información se intercambie con

		los interlocutores idóneos y que los servicios se acrediten correctamente.
7	**Trazabilidad**	Se deberá garantizar el seguimiento de las operaciones efectuadas sobre la información y los servicios que lo requieran.
8	**Prevención, reacción y recuperación**	Se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad. La seguridad del sistema deberá contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o a los servicios que se prestan. Las medidas de prevención deberán eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema, contemplando, entre otras, la disuasión y la reducción de la exposición. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.
9	**Múltiples líneas de defensa**	Los sistemas deberán disponer de una estrategia de protección en líneas de defensa, constituida por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas falle, permita:

		a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto c) Minimizar el impacto final sobre el mismo Las líneas de defensa deberán estar constituidas por medidas de naturaleza organizativa, física y lógica.
10	**Mejora continua y reevaluación periódica**	Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.
11	**Proporcionalidad en coste**	La implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.
12	**Concienciación y formación**	Se articularán programas de formación, sensibilización y concienciación para las personas usuarias en materia de seguridad de la información, debidamente apoyados en las políticas corporativas y con un adecuado proceso de seguimiento y actualización.
13	**Función diferenciada**	Conforme a la exigencia legal de considerar la seguridad como una función diferenciada, la responsabilidad sobre la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios. La política de seguridad detallará las atribuciones de cada responsable y los mecanismos de coordinación y

		resolución de conflictos.
14	**Cumplimiento normativo**	Todos los sistemas de información, así como cualquier proceso relacionado, se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquella relacionada con la intimidad y la protección de datos de carácter personal y con la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos, que permita a la ciudadanía y a las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de la tecnología.

2 Directrices

La Política de Gestión y Seguridad de la Información del Ayuntamiento de Pamplona se desarrolla en base a las directrices recogidas en los siguientes apartados.

2.1 Objetivos del Ayuntamiento de Pamplona

La misión del Ayuntamiento de Pamplona es construir un municipio innovador y abierto que ofrezca a la sociedad servicios de calidad, eficientes, eficaces y seguros, en colaboración con su entorno y con la participación activa de la ciudadanía, contando con las personas como protagonistas del cambio, y todo ello basado en los nuevos valores de gobernanza: apertura, orientación a resultados, transparencia e innovación.

Para conseguir este objetivo, apoya su actividad en los sistemas de información (SSII), en soportes tanto digitales como físicos, que deben ser administrados con diligencia tomando las medidas de seguridad adecuadas para protegerlos frente a los daños accidentales o deliberados que pueden afectar a las garantías de autenticidad, integridad, confidencialidad, disponibilidad, trazabilidad y conservación de la información.

De forma estrechamente relacionada con el cumplimiento de esta misión, es importante resaltar la necesidad de una infraestructura de tecnologías de la información y las comunicaciones —en adelante, TIC— que prime y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio a las personas usuarias, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales.

En este sentido, las TIC se constituyen como un instrumento de alto nivel

estratégico, debido a su potencial para impulsar la modernización municipal, así como a su capacidad para estimular y sustentar el desarrollo social y económico del propio Ayuntamiento. Por tanto, es imprescindible que los sistemas TIC sean administrados con diligencia, y que se tomen las medidas adecuadas para protegerlos de amenazas de rápida evolución que puedan incidir en la confidencialidad, integridad, disponibilidad, trazabilidad, autenticidad, conservación y valor de la información y de los servicios.

2.2 Marco Normativo

El marco normativo de las actividades del Ayuntamiento de Pamplona en el ámbito de esta Política de Gestión y Seguridad de la Información está integrado por la legislación definida en un registro al efecto, el cual se mantiene actualizado según señala el correspondiente procedimiento de gestión de requisitos legales.

Igualmente, se deberán tener en cuenta las posibles modificaciones normativas y avances técnicos que puedan afectar al ámbito de esta Política de Seguridad.

Se advierte que el RGPD requiere implícitamente, pero no provee, de lo que en el entorno tecnológico y legal se conoce como Sistema de Gestión de Seguridad de la Información (SGSI). La LOPDP/GDD establece en relación a las medidas de seguridad del sector público, que deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad por lo que dicha norma servirá como referencia de cara a introducir los controles organizativos, operacionales y técnicos (o de protección) para la garantizar que se están gestionando los principales aspectos de la seguridad de la

información.

Igualmente, en lo que se refiere a la Protección de Datos Personales, será necesario establecer las medidas que garanticen que el foco de las decisiones está en la salvaguarda de la intimidad, el honor y la dignidad de las personas físicas. Este hecho tiene importantes implicaciones en:

- El grado de independencia de cara a la toma de decisiones.
- La aproximación que se realice para valorar el riesgo o el impacto de determinadas situaciones y las acciones a llevar a cabo.
- Los modelos de relación entre el Ayuntamiento de Pamplona y terceras partes.

3 El Comité TICS

El Comité de Tecnologías de la Información, Comunicaciones y su Seguridad (Comité TICS) se encarga de la elaboración y ejecución de líneas directrices, objetivos y planificaciones de carácter estratégico o a medio plazo, en materia de Sistemas de Información y Sistemas de Telecomunicaciones para el Ayuntamiento de Pamplona, considerando sus aspectos tecnológicos, jurídicos, organizativos, de repercusión ciudadana y económico presupuestarios.

El Comité TICS estará compuesto por:

- **Presidencia**, que realizará las funciones de presidente/a del Comité TICS y que se asumirá por la persona que lleve a cabo las funciones de Gerencia Municipal.
- Un **cuerpo de vocales** entre los que deberán quedar representados los siguientes roles u órganos colegiados:
    - Responsable municipal de Sistemas Informáticos[1],
    - Representante de ANIMSA,
    - Representante del Comité Delegado de Protección de Datos (DPD),
    - Representante de la Asesoría Jurídica[2].
- Adicionalmente, se podrá convocar puntualmente a las reuniones del comité a las personas Responsables de los Servicios (RSERV) o Responsables Funcionales del Tratamiento (RFTRAT), Direcciones de las Áreas Municipales, la Gerencia de ANIMSA o del Sector Público

[1] Cargo según la Estructura Municipal, no relacionado directamente con los roles ENS o LOPDP/GDD.
[2] Ídem.

Institucional o personas en quienes ellos deleguen, en función del asunto tratado.

Todos los servicios y direcciones del Ayuntamiento de Pamplona, por tanto, están obligados a informar y prestar apoyo al Comité TICS cuando éste así lo requiera.

Para hacer efectivas las decisiones tomadas, el Comité TICS podrá proponer, a las personas responsables municipales correspondientes en cada caso[3], la publicación de normas para su revisión y aprobación por el organismo competente.

Puesto que el Comité TICS no es un comité técnico, deberá recabar regularmente de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas:

- Grupos de trabajo especializados, internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de eventos formativos o de intercambio de experiencias.

Sus funciones y responsabilidades en materia de Seguridad de la Información aparecen detalladas en la sección 4, "Organización de la Seguridad", apartado 4.3.

Por otra parte, el Comité TICS podrá apoyarse en diversos grupos

[3] Como puedan ser Concejalías, Gerencia, Direcciones de Área o Dirección de la Asesoría Jurídica o cualquier otro organismo municipal con competencias.

interdisciplinares para la elaboración de trabajos específicos que requieran un enfoque interdisciplinar según se detalla en la sección 4.10.

4 Organización de la Seguridad

Para promover la aplicación de esta Política de Seguridad del Ayuntamiento de Pamplona y demás normativas e instrucciones de seguridad de la información, se establece una estructura organizativa y se definen las funciones y responsabilidades de cada una de las personas y órganos que forman parte de la misma.

Dicha estructura organizativa integra la establecida para la materia de Protección de Datos Personales del Ayuntamiento de Pamplona y el Esquema Nacional de Seguridad. Esto es, la articulación de los roles definidos es compatible y está integrada con la articulación de roles y responsabilidades existente en relación a la protección de datos de carácter personal y el cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDP/GDD), y de toda la regulación asociada a ella, como el Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de Abril de 2016. Para ello se han tomado como guía las recomendaciones de la Agencia Española de Protección de Datos (AEPD)[4] y el Centro Criptológico Nacional (CCN)[5].

Dado que ambas normativas requieren la definición de diferentes roles, a menudo mutuamente incompatibles pero que exigen profunda coordinación,

[4] Agencia Española de Protección de Datos, sobre la posible compatibilidad entre la figura del delegado de protección de datos del Reglamento general de protección de datos y el responsable de seguridad de la información del Esquema Nacional de Seguridad: https://www.aepd.es/documento/2018-0170.pdf

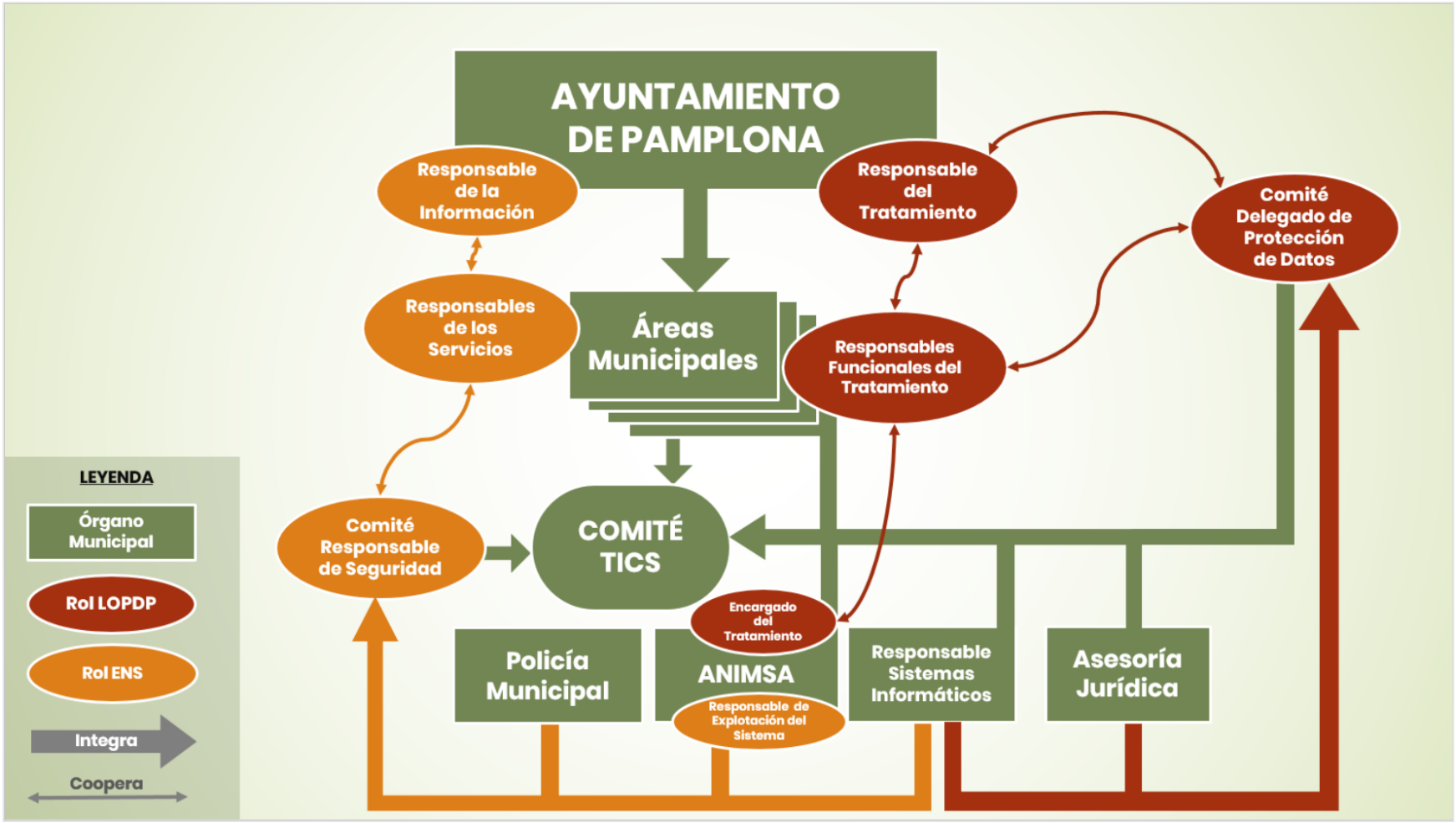
[5] CCN-STIC 801: ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

se constituirán órganos colegiados con responsabilidades diferenciadas, como es visiblemente el caso del Comité de Tecnologías de la Información, las Comunicaciones y su Seguridad (Comité TICS), el Comité Responsable de Seguridad de la Información y el Comité Delegado de Protección de Datos. Está previsto que dichos órganos colegiados puedan incorporar algunos miembros en común, para garantizar la coherencia entre sus actuaciones, si bien *en ningún caso* podrán estar formados por un conjunto idéntico de miembros para cumplir con el criterio de Función Diferenciada[6].

La relación entre los diferentes organismos municipales en lo que compete a la Política de Seguridad de la Información, sus roles según el Esquema Nacional de Seguridad y la normativa de protección de datos de carácter personal aparece recogida en la Figura 1. La descripción pormenorizada de todas las funciones se detalla en el resto de la presente sección, mientras que la relación de miembros nominales se recoge en el "ANEXO B Roles y miembros de comités nominales". De esta manera, cualquier cambio nominal de miembros y roles de los definidos en la política podrá actualizarse cambiando esta relación y aprobando una nueva versión de la misma por Decreto de Alcaldía.

[6] Tal y como se describe en la Tabla 1: Principios de Seguridad.

Figura 1: Organización de la Seguridad de la Información – Estructura municipal, Roles ENS, LOPDP/GDD y relaciones.



Los **organismos y roles propios del Ayuntamiento de Pamplona** con funciones y responsabilidades asociadas a la Política de Seguridad de la Información y a la Protección de Datos de Carácter Personal son las siguientes:

4.1 Ayuntamiento de Pamplona

El Ayuntamiento de Pamplona figura, necesariamente, como **Responsable del Tratamiento (RTRAT)** de todos los datos personales en lo que respecta a la LOPDP/GDD y, dado que la información disponible en la organización podrá reutilizarse por diferentes áreas y servicios, se hace necesario diferenciar la función de **Responsable de la Información (RINFO)** y asimilarla al más alto nivel, si bien se delegarán las tareas efectivas de dicha función en el Comité de Tecnologías de la Información, Comunicaciones y su Seguridad.

En el ámbito de Seguridad de la Información y Protección de datos personales, tanto el Pleno Municipal como la Junta de Gobierno deben garantizar que los órganos competentes[7] han realizado:

- una Política de Seguridad de la Información, como la presente,
- una definición, para la **información** bajo su responsabilidad, de las dimensiones de la seguridad relevantes (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente,
- las tareas de más alto nivel de gestión del riesgo, como notablemente

[7] Según el caso podrán delegar estas tareas en el Comité TICS o en los Responsables de los Servicios y Responsables Funcionales del Tratamiento.

son el "Análisis de Riesgos", establecer los niveles de seguridad requeridos por la información y la "Aceptación del riego residual".

En este sentido:

- los miembros de la Junta de Gobierno (JOB) deben asimilar dicho conocimiento de cara a desempeñar sus labores estratégicas. Además, deberán garantizar que sus responsables ejecutivos como las Direcciones de Áreas y Secretarías Generales Técnicas operen de acuerdo a los mismos;

- por su parte, los miembros del Pleno Municipal, deben de conocerlos para poder llevar a cabo de manera efectiva y segura sus responsabilidades de control y supervisión de la gestión.

4.2 Alcaldía y Nombramientos

En el ámbito de seguridad de la información, corresponde a Alcaldía:

- la asignación, a través de las concejalías delegadas y sus respectivos equipos, las funciones correspondientes en materia de seguridad de la información y protección de datos personales. Dichas personas asumirán los roles de **Responsables de los Servicios (RSERV)** y **Responsables Funcionales del Tratamiento de Datos Personales (RFTRAT)**.

- la constitución y modificación del Comité de Tecnologías de la Información, Comunicaciones y su Seguridad (Comité TICS) y la designación de sus integrantes por el órgano municipal competente.

- el nombramiento de los miembros del Comité Delegado de Protección

de Datos.

- Aprobar la presente Política de seguridad de la Información así como la Normativa de Seguridad del Ayuntamiento de Pamplona y sus posteriores modificaciones a propuesta del Comité de Tecnologías de la Información, las Comunicaciones y su Seguridad (Comité TICS).

La designación nominal de dichos nombramientos aparece recogida en el Anexo B del presente documento.

4.3 Comité de Tecnologías de la Información, Comunicaciones y su Seguridad (Comité TICS)

El Comité de Tecnologías de la Información, Comunicaciones y su Seguridad (Comité TICS) dirige, gestiona, coordina, establece y aprueba las actuaciones en materia de tecnologías de la información, incluyendo todos los aspectos de seguridad de las mismas.

Las **funciones y responsabilidades** concretas del Comité TICS en lo que respecta a la seguridad de la información y la protección de datos de carácter personal son las siguientes:

- Elaborar e impulsar la estrategia y nuevas líneas de trabajo en lo que respecta a la seguridad de la información.

- Atender las inquietudes de las Áreas en materia de Seguridad de la Información.

- Establecer directrices de actuación relacionadas con 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, que están alineados con la estrategia decidida en la materia, evitando duplicidades.

- Promover la mejora continua del sistema de gestión de la 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.
- Proponer a Alcaldía la aprobación de las políticas y normativas de seguridad relacionadas con el ENS.
- Elaborar, revisar y hacer el seguimiento de la Política de Seguridad de la Información proponiendo a Alcaldía las modificaciones que considere oportunas.
- Proponer las medidas oportunas para divulgar la Política de Seguridad de la Información aprobada por el Ayuntamiento de Pamplona.
- Comunicar a los órganos competentes el incumplimiento de la Política de Seguridad de la Información e instar, en su caso, la adopción de las medidas disciplinarias correspondientes.
- Supervisar y aprobar las tareas de seguimiento del ENS.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos 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.

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

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

- Elevar a Alcaldía su informe anual sobre la gestión de la Política de Seguridad de la Información en el que podrá incluir una exposición detallada de los incidentes habidos en materia de seguridad de la información y los resultados de las auditorías realizadas.

4.4 Responsables de los Servicios y Responsables Funcionales del Tratamiento de Datos Personales

Las personas **Responsables de los Servicios (RSERV)** son los titulares de los órganos directivos de cada una de las áreas de gobierno municipal, o personas en quienes deleguen, y son, a su vez, responsables de los tratamientos de datos, incluyendo los de carácter personal, definidos en su ámbito competencial. Aunque se ha establecido al Ayuntamiento de Pamplona como Responsable del Tratamiento en lo que respecta a los Datos de Carácter Personal, dichos responsables serán considerados **Responsables Funcionales del Tratamiento (RFTRAT)**.

Tienen las siguientes funciones y responsabilidades:

- Determinar, en su ámbito de responsabilidad, los requisitos de seguridad de la información que sean de aplicación a sus sistemas de

información necesarios para proteger apropiadamente la información de las aplicaciones, y concretar los intereses a salvaguardar, así como las necesidades a cubrir. Estas consideraciones han de incluir, necesariamente, aquellas que se deriven de la protección de datos de carácter personal.

- Realizar, para los **servicios** bajo su responsabilidad, un análisis de las dimensiones de la seguridad relevantes (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente,

- Definir las necesidades de seguridad de los **servicios** contemplados en el análisis de riesgos para cada una de las diferentes dimensiones de seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente.

- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y por su cumplimiento.

- Determinar, para los servicios electrónicos bajo su responsabilidad, la evolución del impacto de una indisponibilidad en función del tiempo.

- Colaborar en el análisis de impacto de los incidentes que se puedan producir y plantear las estrategias y salvaguardas ante los mismos.

- Colaborar en la creación de las políticas y normativas de Seguridad de la Información.

- Cualquier otra función que se entienda pertinente en el ámbito de las funciones generales que les corresponden o que sea encomendada

por los órganos competentes.

4.5 Comité Responsable de Seguridad de la Información

Un órgano colegiado ejercerá las funciones de Responsable de Seguridad de la Información según el Esquema Nacional de Seguridad. Dicho comité ejercerá sus funciones para satisfacer los requisitos de seguridad de la información que la organización establezca, especialmente a través de su Comité TICS.

Dicho comité contará, al menos, con los siguientes **miembros permanentes**:

- Responsable de Sistemas Informáticos del Ayuntamiento de Pamplona,
- Representante de ANIMSA.
- Responsable del Sistema, según el rol ENS.

Adicionalmente, y según el tema a tratar, se **podrá convocar** a:

- representante de la Policía Municipal o el Área Municipal de la que dependa la seguridad física de las instalaciones.
- representantes de la Asesoría Jurídica o Personal
- Otros roles de los establecidos según el ENS o el RGPD.

Dicho comité tiene definidas las siguientes funciones y responsabilidades:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información.

- Involucrar y asesorar a las personas Responsables de los Servicios de las diferentes áreas en tareas de protección de la información.

- Determinar las medidas de seguridad necesarias para la protección de la información manejada y los servicios prestados por el Ayuntamiento

de Pamplona y verificar que las establecidas son adecuadas en todo momento.

- Proponer la implantación de medidas de seguridad de índole técnico y organizativo al Comité TICS para su aprobación.
- Determinar la clasificación de la categoría del sistema y las medidas de seguridad que deben aplicarse en el Ayuntamiento de Pamplona.
- Reportar el estado de la seguridad al Comité TICS.
- Coordinar las tareas periódicas derivadas de la revisión y mantenimiento del Análisis de Riesgos y del Análisis de Impacto definido en el Ayuntamiento de Pamplona.
- Impulsar o instar junto con el Comité TICS la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Informar al Comité TICS de los incidentes de seguridad de carácter grave.
- Elaborar el documento de Declaración de Aplicabilidad.
- Elaborar un informe periódico de seguridad, que incluya los incidentes más relevantes del periodo.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como

lógicos.

- Proponer al Comité TICS la modificación de aquella normativa, instrucciones y directrices técnicas que considere necesarias y que afecten directamente al Ayuntamiento de Pamplona en materia de seguridad de la información.

- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.

- Decidir transitoriamente la aprobación de los procedimientos de seguridad elaborados por el Responsable de Explotación de los Sistemas y procurar su implementación.

Cualquier otra función que se entienda pertinente en materia de seguridad, no atribuida específicamente a cualquier otro órgano contemplado en el presente documento.

4.6 Comité Delegado de Protección de Datos

Dadas las particulares necesidades que la normativa establece para el perfil de Delegado de Protección de Datos, con capacidades tecnológicas y jurídicas, se establece un órgano colegiado que asuma las funciones de Comité Delegado de Protección de Datos. Todas sus funciones en materia de seguridad quedarán asociadas al tratamiento de los datos personales y según la aproximación de la LOPDP/GDD.

Dicho comité está conformado, al menos, por:

- Responsable de Sistemas Informáticos del Ayuntamiento de Pamplona,

- Dirección de la Asesoría Jurídica o persona en quien delegue,

Y podrá apoyarse para su operativa diaria en técnicos informáticos y jurídicos especializados a través de personal municipal y/o ANIMSA.

El DPD tiene definidas las funciones y responsabilidades que se recogen en el artículo 39 del RGPD[8]:

> *1.- 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;*

[8] Tal y como aparece en https://www.boe.es/doue/2016/119/L00001-00088.pdf

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.

2.- 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."

4.7 Responsable del Sistema

Es la persona encargada de determinar las medidas de seguridad de índole tecnológica determinadas por el Responsable de la Seguridad de la Información. Este rol lo ostentará un Responsable Técnico de ANIMSA, por asignación del Comité TICS, asumiendo, dentro de su ámbito de competencia, las siguientes funciones y responsabilidades específicas:

- Garantizar que las tareas propias de la administración de la seguridad de los sistemas bajo su responsabilidad se llevan a cabo de manera correcta.
- Garantizar que los sistemas de información de los que es responsable permanecen bajo control.
- Llevar a cabo los procesos de seguridad en el ámbito de su área.
- Garantizar que se implementa la seguridad física y lógica de la organización municipal.
- Colaborar en las auditorias de seguridad, de Protección de Datos de

Carácter Personal y en la gestión de riesgos.

- Cualquier otra función que se entienda pertinente en el ámbito de las funciones generales que les corresponden.

4.8 Administrador de Seguridad

El personal que realice funciones de Administrador de Seguridad (AS) será personal de ANIMSA y, por tanto, dependerá jerárquicamente del Responsable de Seguridad, en el que se encuentra la persona Representante de ANIMSA.

Sus funciones más significativas serán las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- 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.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad (POS).
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

4.9 Otros roles y responsabilidades

4.9.1 Seguridad Física

Como quiera que el ENS contempla preceptos y medidas de seguridad específicos para la seguridad física, las entidades afectadas deberán desarrollar un marco conjunto capaz de dar respuesta a ambas exigencias: físicas y lógicas.

La Policía Municipal es quien tiene las competencias de custodia de los edificios. En los casos en los que proceda, en el Comité de Responsable de Seguridad de la Información solicitará que se realicen las aportaciones necesarias por un representante de la misma.

Así, el Responsable de la Seguridad Física adoptará 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.

4.9.2 Personal – Recursos Humanos

Como quiera que el ENS también contempla preceptos y medidas de seguridad relativas al personal, los responsables de RR.HH. ajustarán sus acciones a lo establecido por el ENS en materia de seguridad ligada al personal, de forma análoga a lo establecido en los puntos anteriores.

El departamento de RR.HH. de la entidad adoptará las medidas de seguridad que le competan, dentro de las determinadas por el Responsable de la Seguridad de la Información, e informarán a éste de su grado de implantación, eficacia e incidentes.

4.9.3 Personas usuarias

Toda persona o sistema que acceda a la información tratada, gestionada o propiedad del Ayuntamiento de Pamplona se considerará un usuario. Los usuarios son responsables de su conducta cuando acceden a la información o utilicen los sistemas informáticos del Ayuntamiento de Pamplona. El usuario es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los usuarios tienen la obligación de:

- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de políticas, normas, procedimientos y medidas de seguridad aplicables.

- Proteger y custodiar la información de Ayuntamiento de Pamplona, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.

4.10 Tareas relacionadas con la Seguridad - Matriz RACI[9]

Tabla 2: Relación de tareas y responsabilidades relacionadas con las Seguridad de la Información.

Tarea	Ayunta-miento (RTRAT)	Comité TICS (RINFO)	Direcciones de Área (RSERV / RFTRAT)	Comité Responsable de Seguridad de la Información (RSEG)	Responsable del Sistema (RSIS)	Administrador de la Seguridad (AS)	Comité Delegado de Protección de Datos (DPD)[10]
Niveles de seguridad requeridos por la información		**A**	**I**	**R**	**C**		**C**
Niveles de seguridad requeridos por el servicio		**I**	**A**	**R**	**C**		**C**
Determinación de la categoría del sistema				**A**	**R**		**C**
Análisis de riesgos		**A**	**I**	**R**	**C**		**A***
Declaración de aplicabilidad ENS		**I**	**I**	**A/R**	**C**		
Medidas de seguridad adicionales		**I**	**I**	**A/R**	**C**		**C**
Configuración de seguridad		**I**	**I**	**A**	**C**	**R**	
Aceptación del riesgo residual		**A**	**C**	**R**	**I**		**A***

[9] Una Matriz de Asignación de las Responsabilidades (RACI, por las iniciales en inglés de cada responsabilidad) relaciona las actividades a realizar con los roles implicados en ellas y su grado de responsabilidad según este criterio:

A-Administrador**:** Es quien debe garantizar que la tarea se ejecute y quien debe aprobar su versión final.

R-Responsable: Es el responsable de realizar de facto la documentación.

C-Consultado: Aquellos roles que deben de ser tenido en cuenta de cara a realizar la documentación para garantizar la coherencia con el resto de decisiones tomadas por la organización.

I-Informado: Son aquellos perfiles que deben de tener conocimiento de la existencia de dicha documentación bien sea como afectados directos o indirectos.

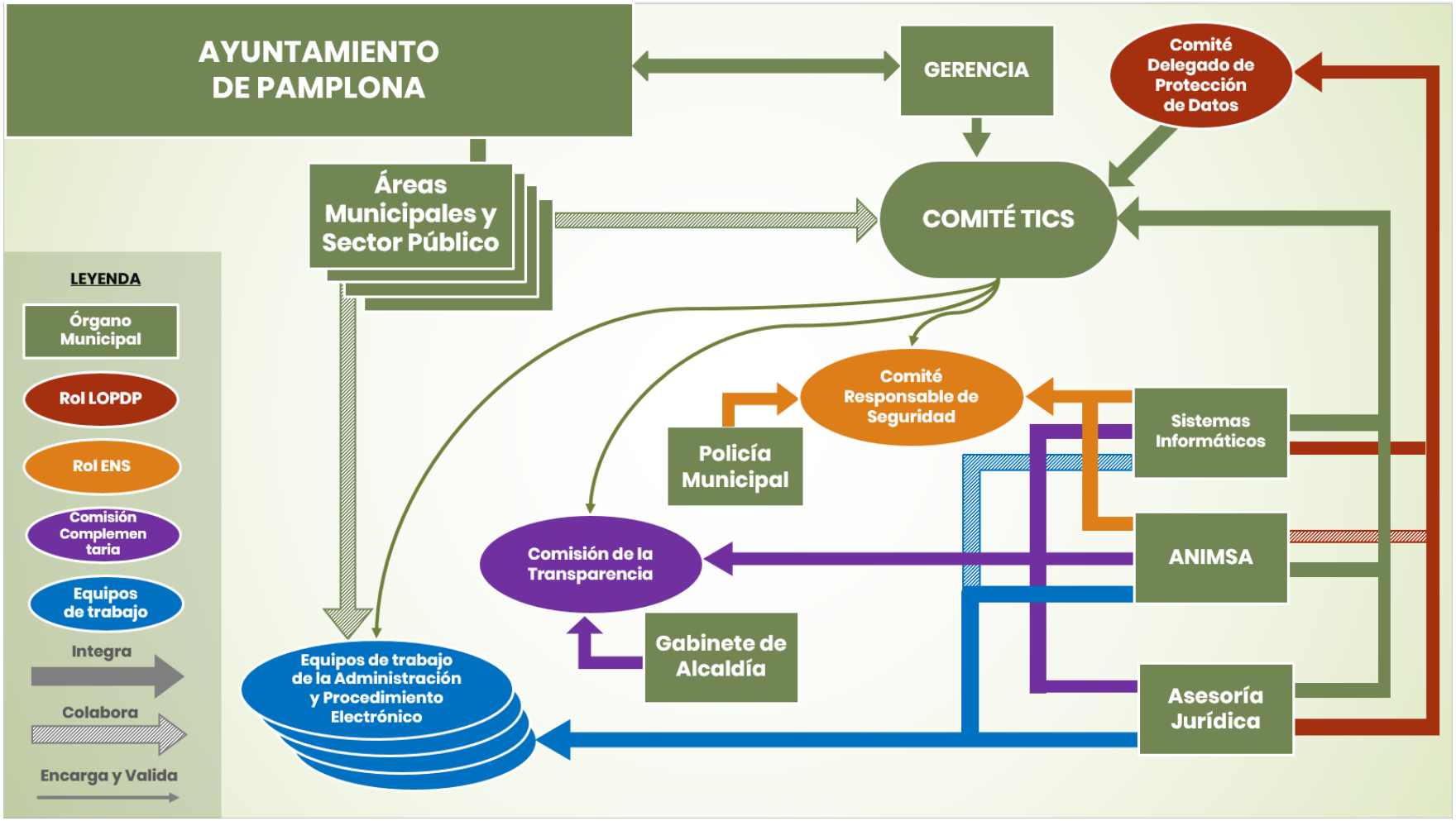
[10] Todas las funciones del DPD aplican en el ámbito de Protección de Datos Personales.

Tarea	Ayunta-miento (RTRAT)	Comité TICS (RINFO)	Direcciones de Área (RSERV / RFTRAT)	Comité Responsable de Seguridad de la Información (RSEG)	Responsable del Sistema (RSIS)	Administrador de la Seguridad (AS)	Comité Delegado de Protección de Datos (DPD)[10]
Documentación de seguridad				A	C	I	
Política de seguridad	A	C	C	R	C		
Normativa de seguridad	A	C	C	R	C	I	
Procedimientos de seguridad		I	I	C	A/R	I	R*
Implantación de las medidas de seguridad		I	I	C	A	R	
Supervisión de las medidas de seguridad				A	I	R	C*
Estado de seguridad del sistema	I	I	I	A	I	R	
Planes de mejora de la seguridad		I	I	A/R	C		
Planes de concienciación y formación		I	I	A/R	C		A*
Planes de continuidad		I	I	C	A		
Suspensión cautelar del servicio	I	I	I	A	R		
Seguridad en el ciclo de vida				C	A		

5 Equipos multidisciplinares en la Gestión de la Información Municipal

Como se ha descrito previamente, el Comité TICS en el ejercicio de sus funciones deberá recabar regularmente de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento. En esta sección se describen aquellos cuyo objeto principal no consiste en la seguridad de la información, sino que se deben a cuestiones normativas u organizativas que requieren un enfoque multidisciplinar. Los principales aparecen recogidos en la Figura 2.

Figura 2: Organización de los Equipos de Trabajo dependientes del Comité TICS



5.1 Comisión Técnica de la Transparencia

La Comisión Técnica de la Transparencia se encargará de promover y garantizar que se cumplen con todas las obligaciones legales en materia de transparencia, como son la "Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno" y la "Ley Foral 5/2018, de 17 de mayo, de transparencia, acceso a la información pública y buen gobierno".

Dicho órgano estará conformado al menos por:

- Un representante de la Asesoría Jurídica
- Un técnico de ANIMSA con conocimiento en explotación de datos
- Personal del Gabinete de Alcaldía y Comunicación
- Persona Responsable de Sistemas Informáticos

Todas las áreas municipales deberán facilitar a dicho grupo de trabajo la información pertinente para la elaboración de los indicadores necesarios.

5.2 Comisión Técnica de la Administración y Procedimiento Electrónico

Dicho Comité se encargará de trabajar de manera coordinada en la gestión y evolución de la administración electrónica,

Serán miembros **permanentes** de dicho comité:

- Al menos un representante de la Asesoría Jurídica,
- Persona Responsable de Sistemas Informáticos

- Representante dirección de ANIMSA
- Al menos un técnico de ANIMSA especializado en la Gestión de Expedientes electrónicos.

Adicionalmente, y en función de la cuestión a tratar, otros empleados municipales podrán ser requerido a participar en las reuniones o en el desarrollo de determinadas tareas. Este será notablemente el caso de personal del Archivo Municipal, Secretarías Técnicas o Gerencia Municipal.

5.3 Comisión Técnica de Gestión de los Documentos Electrónicos

La Comisión Técnica de Gestión de los Documentos Electrónicos Ayuntamiento de Pamplona se coordinará con el Comité TICS, asumiendo tareas y elevándole las propuestas que considere pertinentes. Sus funciones serán las siguientes:

- Garantizar la continuidad del proyecto de gestión documental en el Ayuntamiento de Pamplona, su despliegue eficiente y la formalización de un calendario que permita asegurar una efectiva aplicación de los requerimientos del proyecto de manera secuencial y acumulativa.
- Supervisar la formulación e implementación del Plan Director del Documento Electrónico.
- Coordinar las acciones emprendidas durante el proceso de implementación.
- Acordar las directrices y la normativa técnica necesaria para hacer efectiva la implementación.

- Evaluar los recursos económicos y humanos necesarios.
- Proceder a la valoración de la actualización tecnológica: decisión sobre formatos, sobre su obsolescencia, sobre su migración y verificar su cumplimiento.
- Proponer las medidas que estime oportunas para garantizar el correcto funcionamiento de los circuitos documentales, y la colaboración de las unidades administrativas.

5.4 Otros equipos de trabajo

Otros equipos de trabajo podrán recibir encargos por parte del Comité TICS, siempre que su enfoque requiera un enfoque multidisciplinar que pueda conllevar cambios en la forma en la que el Ayuntamiento de Pamplona se organiza y gestiona su información. Dicho de otra manera, en aquellos casos en los que un enfoque meramente tecnológico no sea suficiente.

6 Normativa de Seguridad de la información

El Ayuntamiento de Pamplona establece un marco documental estructurado en diferentes niveles, de forma que las directrices marcadas por el presente documento tengan un desarrollo específico. En cualquier caso, las diferentes políticas, normativas y regulaciones específicas que se desarrollen deben estar alineadas con la presente política de seguridad y derivarse de la misma. La composición del citado marco documental aparece definido en la Tabla 3:

Tabla 3: Marco documental de la Normativa de Seguridad

#	Nivel	Descripción
1	**Política** de Gestión y	Está constituido por el presente documento y la

	seguridad de la información y **Normativa** del Ayuntamiento de Pamplona	Normativa de Seguridad de la Información, que emana de la Política de Seguridad y soporta diferentes ámbitos de la seguridad.
2	**Procedimientos** de seguridad de alto nivel	Emana de la Política de seguridad de la información y soporta los diferentes ámbitos de la seguridad.
3	**Procedimientos, Guías específicas de TI o Instrucciones técnicas** de seguridad	Conjunto de documentos que describen las pautas especificas a seguir a la hora de realizar una determinada actividad técnica relacionada con la seguridad de la información.
4	**Otros** documentos	Además de los documentos citados, la documentación de seguridad podrá contar con otros adicionales, como son: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, presentaciones, etc.

La Política de Seguridad de la Información y la Normativa de Seguridad de la Información (primer nivel) son aprobadas por la Junta de Gobierno del Ayuntamiento de Pamplona. Su incumplimiento puede dar lugar a la correspondiente responsabilidad disciplinaria.

Los procedimientos de seguridad de más alto nivel (segundo nivel) son aprobadas por el Comité de Tecnologías de la Información, cómo por ejemplo de gestión de personal o gestión de servicios externos, así como el análisis de riesgos y la aceptación del riesgo.

Los procedimientos y guías de seguridad o instrucciones de seguridad (tercer

y cuarto nivel) son aprobadas por el Responsable de Seguridad de la Información en colaboración con las y los Responsables Explotación de los Servicios y de los Sistemas.

La presente Política de Seguridad de la Información, las normativas y el resto de documentación específica que se apruebe deben ser comunicadas a todas las personas responsables de los servicios afectados, debiendo quedar publicadas al menos en la intranet del Ayuntamiento de Pamplona, o en la página web pública, siempre que su aplicabilidad pueda afectar a todas las personas usuarias.

Los responsabilidades anteriormente descritas pueden visualizarse en la matriz RACI[11] mostrada en la Tabla 4:

[11] Una Matriz de Asignación de las Responsabilidades (RACI, por las iniciales en inglés de cada responsabilidad) relaciona las actividades a realizar con los roles implicados en ellas y su grado de responsabilidad según este criterio:

A-Administrador**:** Es quien debe garantizar que la tarea se ejecute y quien debe aprobar su versión final.

R-Responsable: Es el responsable de realizar de facto la documentación.

C-Consultado: Aquellos roles que deben de ser tenido en cuenta de cara a realizar la documentación para garantizar la coherencia con el resto de decisiones tomadas por la organización.

I-Informado: Son aquellos perfiles que deben de tener conocimiento de la existencia de dicha documentación bien sea como afectados directos o indirectos.

Tabla 4: Matriz responsabilidades por roles para la Documentación de Seguridad

Rol	Política y Normativa	Procedimientos que se definan de más alto nivel	Procedimientos; Instrucciones y Guías Técnicas	Otros documentos
Ayuntamiento	**I**	**I**	**-**	**-**
Alcaldía	**A**	**I**	**-**	**-**
Comité TICS	**R/C**	**A**	**-**	**-**
Responsable de Seguridad de la Información	**R**	**R**	**R /A**	**R**
Delegado de Protección de Datos	**C**	**C**	**I**	**I**
Responsables de los Servicios y Responsables Funcionales del Tratamiento de Datos Personales	**C**	**C**	**A**	**A**
Responsable del Sistema	**C**	**C/R**	**R**	**C**
Usuarios	**I**	**I**	**I**	**I**
Ciudadanos y terceras partes	**I**	**-**	**-**	**I**

7 Obligaciones asociadas

7.1 Revisión de la política de seguridad

Se debe revisar y promover la actualización de la Política de seguridad de la información y normativa de seguridad definidas por el Ayuntamiento de Pamplona.

El Comité TICS revisará la Política de seguridad de la información regularmente o cuando exista un cambio significativo que obligue a ello.

La propuesta de revisión, en su caso, será aprobada y difundida para que la conozcan todas las partes afectadas.

7.2 Obligaciones generales de las personas usuarias

Todas las personas usuarias del Ayuntamiento de Pamplona tienen la obligación de conocer y cumplir esta Política de Gestión y Seguridad de la Información y la normativa e instrucciones de seguridad desarrolladas a partir de ella, siendo responsabilidad del Comité TICS disponer los medios necesarios para que la información llegue a todas ellas.

Todas las personas usuarias del Ayuntamiento de Pamplona deben ser conscientes de la necesidad de garantizar la seguridad de los sistemas de información, así como de que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad.

Se establece un programa de concienciación continua para atenderles, en particular a las de nueva incorporación. Se entiende conveniente que todas las personas con responsabilidad en el uso, operación o administración de sistemas TIC reciban la formación para el manejo seguro de los sistemas que necesiten para realizar su trabajo.

7.3 Responsabilidades en caso de incumplimiento

El Comité TICS podrá apreciar si por parte de las personas usuarias del Ayuntamiento de Pamplona ha podido existir algún tipo de incumplimiento en las obligaciones previstas en la Política de Seguridad de la Información o en su normativa e instrucciones de desarrollo.

En caso de que se aprecie un posible incumplimiento, se adoptarán medidas preventivas y correctoras encaminadas a salvaguardar y proteger las redes

y sistemas de información.

Igualmente, apreciado un posible incumplimiento de la Política de Seguridad de la Información del Ayuntamiento de Pamplona, el Comité de Tecnologías de la Información podrá instar, a los órganos correspondientes, la instrucción de los procedimientos disciplinarios que se consideren convenientes.

El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario del personal al servicio de las Administraciones Publicas o del propio Ayuntamiento de Pamplona.

8 Terceras partes

Cuando el Ayuntamiento de Pamplona utilice servicios o maneje información de terceros, les hará partícipes de esta Política de Gestión y Seguridad de la información. El Comité TICS establecerá canales para reporte y coordinación, así como procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Pamplona preste servicios a otros organismos, les hará partícipe de esta Política de Seguridad de la Información y de las Instrucciones y Procedimientos que atañan a dichos servicios o información.

Cuando el Ayuntamiento de Pamplona ceda información a terceros o encargue la prestación de servicios a otros organismos, les hará partícipe de esta Política de Seguridad de la Información y de las Instrucciones y Procedimientos que atañan a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la normativa mencionada, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y

resolución de incidencias. Asimismo, se exigirá que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al nivel establecido en esta Política.

ANEXO A: Glosario de Términos

En la Tabla 5 se definen una serie de términos y abreviaturas que han sido empleados a lo largo de todo el documento y que facilitan el entendimiento del mismo:

Tabla 5: Glosario de términos

Activo	Componente, funcionalidad o recurso que tenga valor para la organización —información, datos, servicios, aplicaciones, equipos, comunicaciones, recursos administrativos, físicos y humanos…—
Amenaza	Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización [UNE 71504:2008] Las amenazas siempre están presentes, pero se pueden intentar evitar o paliar los efectos de su materialización
Análisis de riesgos	Proceso para el análisis de las amenazas, vulnerabilidades, riesgos e impactos a los que está expuesto un sistema de información, teniendo en cuenta las medidas de seguridad ya presentes. Sirve como punto de partida para identificar las mejoras en las medidas de seguridad, tanto en lo que se refiere a la efectividad como a los costes
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos [ENS]
Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o

	procesos no autorizados [ENS]
Cuerpo normativo	Conjunto de normas que desarrollan de forma más concreta la manera de alcanzar los objetivos de una política
Dato de carácter personal	Cualquier información concerniente a personas físicas identificadas o identificables [LOPD]
Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren [ENS]
ENS	Esquema Nacional de Seguridad (RD 311/2022)
Gestión de la continuidad	Actividades que lleva a cabo una organización para asegurar que todos los procesos de negocio críticos estarán disponibles para sus usuarios, clientes, proveedores y otras entidades que deban utilizarlos
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respeto a los riesgos [ENS]
Incidente de seguridad	Suceso inesperado o no deseado con consecuencias negativas para la seguridad del sistema de información [ENS]
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada [ENS]
LOPDP/GDD	Ley Organica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.
Medidas de seguridad	Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de

	medidas de prevención, disuasión, protección, detección y reacción, o bien de recuperación [ENS]
Política de seguridad	Documento de alto nivel que especifica los objetivos en materia de seguridad de una organización y refleja el compromiso de la dirección para alcanzarlos
Proceso	Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y un fin delimitados, implica recursos y da lugar a un resultado [ENS]
RDLOPD	Reglamento de Desarrollo de la LOPD (RD 1720/2007)
RGPD	Reglamento General de Protección de Datos (Reglamento UE 2016/679)
Riesgo	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, con daños o perjuicios a la organización [ENS]
Riesgo residual	Riesgo remanente en el sistema tras la implantación de unas determinadas salvaguardas en el plan de tratamiento de riesgos
Seguridad de la información	Protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas
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 [ENS]

Soporte	Medio físico de cualquier tipo (DVD, discos portátiles, etc.) utilizado para almacenar información
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad [ENS]
Vulnerabilidad	Una debilidad en un activo que puede ser aprovechada por una amenaza [ENS]