III.-ADMINISTRACIÓN LOCAL

AYUNTAMIENTO DE VALLADOLID

ÁREA DE HACIENDA, PERSONAL Y MODERNIZACIÓN ADMINISTRATIVA

Secretaria Ejecutiva del Área de Hacienda, Personal y Modernización Administrativa

La Junta de Gobierno Local, en sesión de fecha 26 de mayo de 2026, adoptó, entre otros, el siguiente acuerdo:

Vistas las actuaciones contenidas en el expediente 2026/DIR_01/000002 (Pieza separada nº1 del expte HPMA-SE 43/2024)., relativo a la Aprobación de la actualización de la Política de Seguridad de la Información del Ayuntamiento de Valladolid, se formula la siguiente propuesta:

ANTECEDENTES DE HECHO

Primero: El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, persigue reforzar la confianza en el adecuado funcionamiento de los sistemas de información, estableciendo medidas para garantizar la seguridad de los datos, las comunicaciones y los servicios electrónicos, de forma que se facilite a la ciudadanía y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos.

Segundo: Mediante Decreto de Alcaldía núm. 2024/3007, de fecha 30 de abril, se crea el “Comité Municipal de Seguridad de la Información”, al que se atribuyen funciones de apoyo y propuesta para la elaboración, modificación y actualización de la Política de Seguridad de la Información; su difusión y seguimiento; así como velar por el cumplimiento de la normativa en materia de seguridad de la información, proponiendo, en su caso, estrategias oportunas para la evolución de la organización municipal en la materia.

Tercero: Mediante acuerdo de la Junta de Gobierno Local de fecha 20 de mayo de 2024, fue aprobada la Política de Seguridad de la Información del Ayuntamiento de Valladolid, que se configura como el instrumento en el que se apoyará el Ayuntamiento para alcanzar su objetivo de garantizar 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, estableciendo, dicha política, responsabilidades, principios y directrices de seguridad alineados con los establecidos por el Esquema Nacional de Seguridad.

Cuarto: Según el plan de transformación digital 2024-2027 del Ayuntamiento de Valladolid, el Departamento de Tecnologías de la Información y las Comunicaciones, está llevando a cabo la consecución de la medida “31 de avances en la certificación en el Esquema Nacional de Seguridad” definida dentro del eje de actuación “7. Renovación de infraestructuras y refuerzo de la ciberseguridad”, dando así cumplimiento a la obligación de las Administraciones Públicas de encontrarse certificadas en el Esquema Nacional de Seguridad, esquema regulado a través del Real Decreto 311/2002 de 3 de mayo (en adelante, ENS) y cuyo alcance propuesto es la Sede Electrónica y el tramitador AVANTE del Ayuntamiento.

Quinto: Consta en el expediente memoria justificativa de modificación de la Política de Seguridad de la Información, en la que se pone de manifiesto que, como consecuencia de las actuaciones desarrolladas para la adecuación y certificación en el Esquema Nacional de Seguridad, la implantación de medidas técnicas, organizativas y documentales, así como la realización de auditorías internas, se han identificado oportunidades de mejora y necesidades de adaptación de la Política de Seguridad de la Información a las circunstancias organizativas actuales del Ayuntamiento.

Es por esto que se plantea la necesidad de adaptar la Política de Seguridad de la Información en los siguientes términos:

-Definición del identificador y adaptación del formato del documento al resto de documentación del Cuerpo Normativo de Seguridad del ENS.
-Extracción del marco normativo a un anexo para facilitar la modificación y actualización de la legislación de aplicación sin necesidad de elevar a la Junta de Gobierno Local su modificación.
-Correcciones tipográficas y de léxico identificadas durante la revisión, así como la eliminación de contenido no aplicable.
-Redefinición de la relación del Ayuntamiento de Valladolid con los terceros implicados en materia de cumplimiento de la PSI, así como la concreción en la periodicidad con la que el Comité Municipal de Seguridad de la Información se reúne.
-Revisión de la asignación de los roles definidos por e l E NS al personal del Ayuntamiento, incluyendo la concreción del puesto del Responsable de Seguridad de la Información.
-Cambios en la asignación de las responsabilidades de realizar la aprobación de los planes de tratamiento de riesgos, aceptación de los niveles de riesgo asumibles y la Declaración de Aplicabilidad, así como en la elaboración de la Declaración de Aplicabilidad dentro del marco del ENS con el objeto de dar respuesta a la realidad del contexto organizativo del Ayuntamiento y a su vez aumentar la operatividad de la gestión de la seguridad dentro de las posibilidades existentes en el marco legislativo vigente.

Sexto: Consta en el expediente acta del Comité Municipal de Seguridad de la Información en la que se informa favorablemente la modificación de la Política de Seguridad de la Información del Ayuntamiento de Valladolid.

FUNDAMENTOS DE DERECHO

Primero: Resulta de aplicación el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, singularmente sus artículos 12 y siguientes.

Segundo: Resulta igualmente de aplicación el Decreto de Alcaldía núm. 2024/3007, de fecha 30 de abril, por el que se crea el "Comité Municipal de Seguridad de la Información" del Ayuntamiento de Valladolid.

Tercero: Resulta de aplicación la Política de Seguridad de la Información del Ayuntamiento de Valladolid, aprobada por acuerdo de la Junta de Gobierno Local de fecha 20 de mayo de 2024.

Cuarto: El órgano competente para la aprobación de la modificación y actualización de la Política de Seguridad de la Información es la Junta de Gobierno Local, de conformidad con lo dispuesto en el apartado 7.3.1 b) de la propia Política de Seguridad de la Información del Ayuntamiento de Valladolid, que atribuye a dicho órgano la competencia para aprobar la Política de Seguridad de la Información del Ayuntamiento de Valladolid y cualquier otra política sectorial complementaria, así como todas aquellas modificaciones o actualizaciones de las mismas que sean propuestas por el Comité Municipal de Seguridad de la Información y permitan el cumplimiento de la normativa aplicable en materia de seguridad de la información.

Por todo ello, considerados los argumentos anteriores y su adecuación a la legalidad
SE PROPONE LA ADOPCIÓN DEL SIGUIENTE ACUERDO

PRIMERO: Aprobar la modificación de la Política de Seguridad de la Información del Ayuntamiento de Valladolid, en los términos que constan en el Anexo al presente acuerdo, incorporando las modificaciones necesarias para su adaptación a la situación organizativa actual del Ayuntamiento y al proceso de adecuación y certificación en el Esquema Nacional de Seguridad.

SEGUNDO: La presente Política de Seguridad de la Información modificada será de aplicación y obligado cumplimiento para todos los Departamentos Municipales del Ayuntamiento de Valladolid, así como para todos los servicios, sistemas de información y procesos afectados por el Esquema Nacional de Seguridad que sean desarrollados con recursos internos o externos vinculados a la entidad mediante contratos, convenios o acuerdos con terceros.

En Valladolid, a 28 de mayo de 2026.- El Concejal delegado general del Área de Hacienda, Personal y Modernización Administrativa.- Fdo.: Francisco de Paula Blanco Alonso.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE VALLADOLID

Versión 2.0

Documento aprobado por el Comité Municipal de Seguridad de la Información

ÍNDICE

ÍNDICE DE ILUSTRACIONES

No se encuentran elementos de tabla de ilustraciones.

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

1.1. Objetivo

El Ayuntamiento de Valladolid ha definido un marco de gestión de la Seguridad de la Información conforme a los requerimientos establecidos por el por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), así como por toda la normativa que lo desarrolle y complemente en este ámbito.

La Política de Seguridad de la Información (en adelante, PSI) es el instrumento en el que se apoya el Ayuntamiento de Valladolid para alcanzar su objetivo de garantizar 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 (en adelante, TIC). Para tal fin, la PSI identifica responsabilidades y establece principios y directrices de seguridad alineados con los establecidos por el ENS.

1.2. Ámbito del documento

La presente PSI será de aplicación y obligado cumplimiento para todos los Departamentos Municipales del Ayuntamiento de Valladolid; considerando todos los servicios, sistemas de información, procesos afectados por el ENS que son desarrollados con recursos internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

1.3. Marco normativo y estándares de referencia

El marco normativo se compone de las normas de ámbito local, autonómico, estatal y europeo que afecten a la Seguridad de la Información. Dicha normativa aplicable se encuentra recogida en un documento anexo de esta política (POL-001.ANE-001) en su versión más reciente.

1.4. Vigencia

El Responsable de Seguridad mantendrá el documento organizado, actualizado y publicado en una ubicación accesible para todos los miembros incluidos en su ámbito de aplicación, en coordinación, en caso necesario, con el DTIC y la Oficina Técnica de Seguridad.

La validez de este documento perdurará hasta que se apruebe uno nuevo que sustituya al presente, ya sea por las revisiones periódicas establecidas, por necesidades de cambios del propio contenido o por cambios sustanciales en la estructura y organización de los sistemas, o por revocación del documento.

Aquellos aspectos que puedan ser actualizables automáticamente serán incluidos en anexos incorporados al presente documento, sin necesidad de que sea sustituido por una nueva versión.

1.5. Revisión y actualización

La gestión del presente documento corresponde al Comité Municipal de Seguridad de la Información, a través de los medios y capacidades del Responsable de Seguridad, de la Oficina de Seguridad y el DTIC para:

- Interpretar y aclarar las dudas que puedan surgir en su aplicación.
- Evaluar la eficacia y eficiencia de las pautas descritas, en términos de mejora de la seguridad de los sistemas de información, en su ámbito de aplicación.
- Su revisión, cuando sea necesario para mejorar la eficacia o eficiencia, actualizar su contenido o se cumplan los plazos máximos establecidos para ello, proponiendo a los órganos competentes para su deliberación y aprobación las modificaciones necesarias.

Los puntos mínimos a considerar en las revisiones serán los siguientes:

- Identificación de acciones de mejora en la gestión de la seguridad de la información.
- Adaptación a los posibles cambios normativos, de infraestructuras tecnológicas, organizativas, etc.
- Identificación de oportunidades de mejora en la gestión de la seguridad de la información.

La revisión se orientará a la identificación y propuesta de oportunidades para la mejora de la seguridad de los sistemas de información, en su ámbito de aplicación, así como a la adaptación a cambios, ya sean legales, tecnológicos, organizativos, etc.

Cualquier deficiencia y/o inconsistencia en este documento deberá ser puesta en conocimiento del responsable de su definición.

1.6. Responsabilidades

Participan en la gestión de este documento:

Tabla 1. Participantes

Modifica y actualiza	Revisa	Aprueba	Responsable definición
• Responsable del Sistema • Responsable de Seguridad de la Información	Comité Municipal de Seguridad de la Información	Junta de Gobierno del Ayuntamiento de Valladolid	DTIC

2. MISIÓN DEL AYUNTAMIENTO DE VALLADOLID

El Ayuntamiento de Valladolid, con personalidad jurídica plena, ejerce sus competencias en régimen de autonomía y, en uso de la potestad de autoorganización, desarrolla sus funciones de acuerdo con los principios de eficacia, eficiencia, transparencia, descentralización, desconcentración, coordinación y servicio al ciudadano, con sometimiento pleno a la ley y al derecho.

En sus relaciones con los ciudadanos, la Administración Municipal actuará de acuerdo con los principios de máxima transparencia y participación, debiendo asegurar la plena efectividad de sus derechos y la mejora continua de la calidad de los servicios que les presta, así como impulsar la utilización de las tecnologías de la información y la comunicación para alcanzar estos fines.

3. PRINCIPIOS FUNDAMENTALES

Toda actividad del Ayuntamiento de Valladolid se regirá por los siguientes principios:

a) **Gestión como proceso integral:** La gestión de la seguridad se entenderá como un proceso integral y planificado, considerando todos los elementos que constituyen un sistema de gestión, y evitando las actuaciones puntuales o tratamientos coyunturales.

b) **Gestión basada en los riesgos:** El análisis y la gestión de los riesgos serán parte esencial y permanente del proceso de gestión de la seguridad de la información. Mediante este proceso se analizan y tratan los riesgos de seguridad, en aras a reducirlos a un nivel aceptable mediante la selección e implantación de las medidas de que correspondan.

c) **Proporcionalidad:** El establecimiento de medidas será proporcional en sus costes económicos y operativos, a los potenciales riesgos y a la criticidad, así como el valor de la información y sus servicios.

d) **Prevención, detección, respuesta y recuperación:** Se establecerán medidas para reducir la probabilidad de que las amenazas que afectan a los activos de información materialicen un impacto negativo, y en caso de ocurrir, gestionarlo en tiempo y forma adecuados para que se mantenga la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de dichos activos.

e) **Líneas de defensa:** La estrategia de protección estará constituida por múltiples capas de seguridad organizativa, lógica y física, para facilitar la respuesta en caso de incidente.

f) **Vigilancia continua y reevaluación periódica:** Se desarrollarán actividades de supervisión y evaluación para asegurar la correcta protección de los activos de información, la operativa establecida, el cumplimiento de obligaciones en el ámbito de aplicación de la presente PSI y el tratamiento de los riesgos derivados; todo con el objetivo de promover una mejora continua.

g) **Responsabilidad diferenciada:** Se establecerán las responsabilidades para los diferentes roles clave en el ámbito de aplicación de esta PSI, como son el Responsable de la Información, Responsable del Servicio, Responsable de Seguridad y Responsable del Sistema. En su designación se tendrán en cuenta las disposiciones de las autoridades competentes en cuanto a incompatibilidades entre los citados roles y sus funciones.

h) **Secreto profesional:** Quienes intervengan en los tratamientos de datos personales o tengan acceso a información que no esté catalogada oficialmente como de difusión pública, estarán obligados a guardar el deber de secreto, incluso después de haber finalizado las actividades relacionadas.

4. DIRECTRICES DE SEGURIDAD

Se adoptarán las medidas organizativas, técnicas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información. La PSI se ejecutará aplicando las siguientes directrices:

a) Organización e implantación del proceso de seguridad:

i. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización, internos y externos, que participen en las actividades que entran dentro del alcance de la PSI.

ii. Se identificarán de forma inequívoca a las figuras de Responsable de la Información, Responsable del Servicio, Responsable de Seguridad y Responsable del Sistema, con una asignación clara de responsabilidades, segregación de funciones y ubicación jerárquica, de conformidad con las disposiciones del ENS.

iii. Se comunicarán las designaciones a todos los miembros de la organización.

iv. Las organizaciones externas que presten servicios al Ayuntamiento designarán puntos de contacto para el ámbito de seguridad de la información, los cuales deberá ser asumido por la figura del Responsable de Seguridad de la organización externa o estar vinculado a esta.

v. Cuando se identifique la exigencia legal o disposición del Ayuntamiento, se requerirá la certificación de las figuras de Responsable de Seguridad.

b) Control de activos y registro de actividades de tratamiento:

i. Los activos de información y de servicio se inventariarán y categorizarán de acuerdo a sus características y nivel de seguridad requerido.

ii. Las medidas de seguridad aplicadas a los activos tendrán en cuenta su categorización.

c) Análisis y gestión de riesgos:

i. Todos los sistemas de información en el ámbito de la presente PSI están sujetos a un proceso de gestión de riesgos, que deberá seguir una metodología reconocida internacionalmente y adecuada a cada ámbito.

ii. El proceso de gestión de riesgos de seguridad de la información deberá realizarse conforme a las disposiciones del ENS.

iii. Las medidas aplicadas como consecuencia de los análisis deberán estar justificadas, y ser proporcionales a los riesgos. Los planes de tratamiento de riesgos deberán ser aprobados por el Comité Municipal de Seguridad de la Información del Ayuntamiento de Valladolid.

d) Gestión del personal:

i. El personal, interno o externo, que haga uso de los sistemas de información que soportan los servicios del ayuntamiento o participe en los tratamientos de datos personales derivados de éstos, deberá ser formado e informado de sus deberes, obligaciones, y responsabilidades en materia de seguridad de la información.

ii. Las obligaciones y responsabilidades en estos ámbitos quedarán recogidas en una normativa interna aprobada por la Junta de Gobierno Local. El cumplimiento de la normativa será supervisado.

iii. Se desarrollarán actividades orientadas a la formación y concienciación del personal en los ámbitos de aplicación de la presente PSI.

e) Profesionalidad:

i. La seguridad de los sistemas estará implantada, atendida, revisada y auditada por personal cualificado y formado, que participará en todas las fases del ciclo de vida de los sistemas.

f) Autorización y control de los accesos:

i. El acceso a los activos de información comprendidos en el ámbito de aplicación de la PSI deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

g) Protección de las instalaciones:

i. Los activos de información deberán permanecer en áreas con un nivel de control y los mecanismos de acceso adecuados y proporcionales a los riesgos identificados.

h) Adquisición de productos de seguridad y contratación de servicios de seguridad:

i. Se seleccionarán los productos y servicios que, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición o que en su defecto cumplan con los criterios preestablecidos de calidad.

i) Mínimo privilegio:

i. Los sistemas se diseñarán y configurarán para ofrecer las funcionalidades imprescindibles para la consecución de los objetivos por los cuales se requieren, siendo especialmente restrictivo en el acceso a funcionalidades y recursos para la administración y monitorización.

j) Integridad y actualización del sistema:

i. El desarrollo y mantenimiento de los sistemas de información irán acompañados de las especificaciones de seguridad.

ii. Se implantarán procesos de gestión del cambio, configuración, y actualización de los sistemas, acordes a un proceso de autorización, para garantizar la integridad de éstos y la resolución de cualquier debilidad que les afecte.

k) Protección de la información almacenada y en tránsito:

i. Se aplicarán medidas para mantener el nivel de seguridad requerido para la información almacenada o en tránsito hacía dispositivos como equipos portátiles, dispositivos móviles, periféricos, y soportes de almacenamiento, considerando por supuesto las comunicaciones sobre redes abiertas.

ii. Igualmente se mantendrá el nivel de seguridad estipulado para la documentación física que provenga de información digital catalogada.

l) Prevención ante otros sistemas de información interconectados:

i. Se analizarán las interconexiones con sistemas ajenos al control del Ayuntamiento, especialmente si se conectan a través de redes públicas, y se mitigarán los riesgos aplicando las medidas que correspondan según las disposiciones de la normativa aplicable y las buenas prácticas.

m) Registro de la actividad y detección de código dañino:

i. Se registrará la actividad de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y, en general, gestionar situaciones ilícitas o de riesgo para la seguridad de los activos de la organización y de los derechos de los afectados. Para desarrollar correctamente esta labor se establecerán accesos unipersonales siempre que sea posible.

n) Incidentes de seguridad y brechas de seguridad de datos personales:

i. Se implantarán procedimientos de gestión integral de incidentes que afecten a la seguridad de la información y a los datos personales, considerando para ello los criterios de clasificación, los protocolos de notificación y comunicación a partes interesadas, un detalle de actividades a desarrollar en cada fase de gestión de un incidente, la aplicación de medidas de detección, respuesta y recuperación, así como el mantenimiento de un registro de los incidentes ocurridos que facilitará la mejora continua del proceso.

ii. Dichos procedimientos serán definidos, de manera no excluyente, de acuerdo con todas las disposiciones aplicables del ENS, la Instrucción Técnica de Seguridad del ENS de Notificación de Incidentes, la Guía Nacional de Notificación y Gestión de Ciberincidentes y la Guía CCN-STIC 817 de Gestión de Ciberincidentes.

iii. El proceso considerará una gestión de incidentes a través de soluciones de ventanilla única, la participación de los órganos y roles clave en seguridad, así como la notificación según corresponda (en base a la clasificación del incidente) a los equipos de respuesta a incidentes de seguridad informática (denominados por su acrónimo en inglés Computer Security Incident Response Team, en adelante, CSIRT), las autoridades de control competentes, y a los usuarios afectados.

o) Continuidad de la actividad:

i. Se implantarán medidas de recuperación y se definirán planes para garantizar la continuidad de las operaciones ante eventos disruptivos.

p) Auditoría y mejora continua de los procesos:

i. Los procesos de gestión de la seguridad serán actualizados y mejorados de forma continua, teniendo en consideración los cambios normativos y buenas prácticas en los citados ámbitos.

ii. Los sistemas de información certificados en el ENS serán objeto de una auditoría regular ordinaria, en función de la periodicidad marcada por la normativa de aplicación, que verifique el cumplimiento de los requisitos de la presente PSI, y de la normativa asociada.

iii. Con carácter extraordinario se realizarán auditorías cuando existan cambios sustanciales en los servicios prestados o en el conjunto de tratamientos de datos personales, o cuando ocurra un incidente de seguridad o incumplimiento grave.

iv. Las auditorías serán supervisadas por el Responsable de Seguridad de la Información.

5. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad del Ayuntamiento de Valladolid se establece partiendo de la identificación de diferentes funciones y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de la infraestructura que las soporte.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información del Ayuntamiento de Valladolid son responsables de la seguridad de la información, así como de los recursos y medios puestos a su disposición para el manejo de dicha información y uso de los servicios informáticos. En ellos recae la responsabilidad de un uso correcto, siempre de acuerdo a las atribuciones profesionales y competencias.

Como extensión a la estructura de seguridad del Ayuntamiento de Valladolid, se establecerán relaciones de cooperación en materia de seguridad con las autoridades competentes, autonómicas o estatales, proveedores de servicios informáticos o de comunicación, así como organismos públicos y privados dedicados a promover la seguridad de los sistemas de información.

5.1. Definición de roles de seguridad

A continuación, se identifican los roles que participan en la Seguridad de la Información del Ayuntamiento de Valladolid.

Tabla 2. Roles de seguridad

ROL	FUNCIONES
Junta de Gobierno	Es el órgano colegiado que establece la misión y los objetivos de la Organización. Se ocupa del nombramiento de los componentes del Comité Municipal de Seguridad de la Información.
Comité Municipal de Seguridad de la Información	Es el órgano colegiado encargado de tomar decisiones que concretan cómo alcanzar los objetivos marcados por los órganos de gobierno. Podrá nombrar Comités delegados o subcomités para la toma de decisiones diaria.
Responsable de la Información	Tiene la responsabilidad última sobre qué seguridad requiere la información manejada por el Ayuntamiento dentro del ámbito de sus competencias.
Responsable de Servicio	Tiene la responsabilidad última de determinar los niveles de servicio aceptables por el Ayuntamiento dentro del ámbito de sus competencias.

ROL	FUNCIONES
Responsable de Seguridad de la Información	Cumplirá las funciones como supervisor de la operación del sistema y vehículo de reporte y comunicación al Comité Municipal de Seguridad de la Información.
Responsable del Sistema	Es el responsable de la toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.
Administrador del Sistema	Es el encargado de la instalación y el mantenimiento del sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad.
Delegado de Protección de datos	Es la persona/as encargadas de asesorar a los Responsables en materia de seguridad (Dirección, Comité Municipal de Seguridad, Responsable de la Información, Responsable de Servicio, Responsable de Seguridad, Responsable del Sistema) acerca del cumplimiento de la normativa de protección de datos personales. Sus funciones vienen recogidas en el Reglamento General de Protección de datos (en adelante, RGPD).

En el Ayuntamiento de Valladolid, con el objetivo de buscar la eficacia y la eficiencia de las medidas de seguridad que se adopten en torno a la información, los sistemas de información y los procedimientos administrativos, el rol de Responsable de la Información y Responsable del Servicio estarán asumidos por la misma persona u órgano, en razón de la materia de su competencia.

5.2. Proceso de toma de decisiones y coordinación

Los diferentes roles de seguridad de la información se articularán mediante la siguiente jerarquía: el Comité Municipal de Seguridad de la Información da instrucciones al Responsable de la Seguridad que se encarga de cumplimentar, supervisando que los responsables y técnicos de sistemas implementan las medidas de seguridad según lo establecido en la Política de Seguridad de la Información del Ayuntamiento de Valladolid.

El Responsable del Sistema:

- Informa al Responsable de la Información/Servicio de las incidencias funcionales relativas a la información que le compete.
- Informa al Responsable de la Información/Servicio de las incidencias funcionales relativas al servicio que le compete.

- Da cuenta al Responsable de la Seguridad de la Información de:
  - Las actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
  - El resumen consolidado de los incidentes de seguridad.
  - Las medidas de la eficacia de las medidas de protección que se deben implantar.

El Responsable de la Seguridad de la Información:

- Informa al Responsable de la Información 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 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.
- Da cuenta al Comité Municipal de Seguridad de la Información de los siguientes aspectos:
  - Resumen consolidado de las actuaciones en materia de seguridad y de las actuaciones llevadas a cabo en el resto de Comités.
  - Resumen consolidado de incidentes relativos a la seguridad de la información.
  - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

5.3. Detalle de los roles

5.3.1. Dirección (Junta de Gobierno Local)

La Junta de Gobierno Local del Ayuntamiento de Valladolid desempeña la función de Dirección, pues es quien entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde de que se alcancen.

Corresponde a la Junta de Gobierno Local en este ámbito:

a) Hacer cumplir las disposiciones establecidas en el ENS en el ámbito de las actividades del ayuntamiento y, en su caso, emitir directrices.

b) Aprobar la Política de Seguridad de la Información del Ayuntamiento de Valladolid y cualquier otra política sectorial complementaria de la anterior, así como de todas aquellas modificaciones o actualizaciones de las mismas, que el Comité Municipal de Seguridad de la Información pueda proponer y permita el cumplimiento de la normativa aplicable en los ámbitos de la seguridad de la información.

c) Constituir y realizar el nombramiento de los integrantes del Comité Municipal de Seguridad de la Información, así como de los roles clave en seguridad de la información, salvo los que pudiera delegar en el Comité Municipal de Seguridad de la Información.

d) Aprobar las políticas sectoriales que complementen a la Política de Seguridad de la Información presentadas por el Comité Municipal de Seguridad de la Información.

e) Aprobar las resoluciones necesarias para el desarrollo de la Política de Seguridad de la Información propuestas por el Comité Municipal de Seguridad de la Información.

f) Aprobar las directrices para coordinar la comunicación del Ayuntamiento de Valladolid con el Centro Criptológico Nacional propuestas por el Comité Municipal de Seguridad de la información.

g) Proporcionar los recursos necesarios, a propuesta del Comité Municipal de Seguridad de la Información, para el aseguramiento del cumplimiento de los objetivos definidos de seguridad de la información.

5.3.2. Comité Municipal de Seguridad de la Información

El Comité Municipal de Seguridad de la Información es el órgano colegiado de seguimiento, asesoramiento, coordinación y control en materia de Seguridad de la Información.

La Seguridad de la Información se define como la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

5.3.2.1. Finalidad y funciones.

El Comité Municipal de Seguridad de la Información tiene como finalidad velar por la seguridad de la información en el Ayuntamiento de Valladolid, asegurando y facilitando la correcta coordinación e integración de todas las actuaciones de los diversos órganos afectados en esta materia.

Para el cumplimiento de la finalidad descrita, el Comité Municipal de Seguridad de la Información es responsable de las siguientes funciones:

a) Elaborar las propuestas de aprobación, modificación y actualización de la Política de Seguridad de la Información del Ayuntamiento de Valladolid, evaluando su idoneidad con una periodicidad mínima anual y proponiendo a su aprobación y revisión cuando proceda.

b) Elaborar y proponer las políticas sectoriales que complementen a la Política de Seguridad de la Información, así como cambios sobre éstas, con el objetivo de cumplir con los esquemas nacionales de seguridad e interoperabilidad.

c) Aprobar los planes de adecuación y planes de mejora y planes de tratamiento de riesgos en el ámbito de aplicación de la PSI.

d) Aceptar los niveles de riesgo aceptable y residual identificados dentro los análisis de riesgos realizados.

e) Elaborar y proponer el desarrollo organizativo que permita el cumplimiento de los esquemas nacionales de seguridad e interoperabilidad, en el ámbito de la organización municipal.

f) Velar por el cumplimiento y difusión de la Política de Seguridad de la Información, promoviendo las actividades de concienciación y formación en materia de seguridad de la información para el personal del Ayuntamiento de Valladolid.

g) Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial referente a la seguridad de la información.

h) Desarrollar, aprobar y distribuir, con el apoyo del Responsable de Seguridad de la Información, la Normativa de Seguridad que desarrolla la PSI en el ámbito de la seguridad de la información.

i) Proponer las resoluciones necesarias para el desarrollo de la Política de Seguridad de la Información.

j) Monitorizar y gestionar de los riesgos de seguridad de la información presentes en la organización.

k) Monitorizar y proponer actuaciones respecto de la gestión de incidentes de seguridad.

l) Elaborar la estrategia de evolución de la organización con respecto a la seguridad de la información.

m) Promover la realización periódica de auditorías de cumplimiento en materia de seguridad de la información.

n) Difundir los acuerdos aprobados por el Comité Municipal de la Seguridad de la Información a toda la organización municipal.

o) Coordinar los esfuerzos de las diferentes áreas implicadas en la gestión de la seguridad de la información.

p) Resolver los conflictos que pudieran surgir en la interpretación y aplicación de la Política de Seguridad de la Información y su desarrollo entre los diferentes responsables de información, servicios y sistemas de información municipales, escalándolos a los órganos municipales competentes si fuese necesario.

q) Proponer la aprobación de las directrices para coordinar la comunicación del Ayuntamiento de Valladolid con el Centro Criptológico Nacional.

r) Recabar informes regulares del estado de seguridad de la información de la organización municipal y de los posibles incidentes referentes a Tecnologías de Información y Comunicación (TIC); trasladando sus conclusiones a los órganos municipales competentes y a los diferentes grupos de trabajo que se pudieran crear como apoyo en la gestión de la seguridad de la información.

s) Promover inversiones racionales y proporcionadas de carácter horizontal para garantizar la disponibilidad de recursos para atender a las diferentes necesidades de seguridad de la información.

t) Definir criterios de valoración para los diferentes tipos de información manejados y los diferentes servicios prestados con el fin de armonizar los análisis de riesgos de los diferentes sistemas de información.

u) Aprobar la Declaración de Aplicabilidad, establecida en la regulación del ENS, de la información, servicios y sistemas de información del Ayuntamiento de Valladolid.

5.3.2.2. Composición

Se crea el Comité Municipal de Seguridad de la información que estará compuesto por la Presidencia, las Vocalías y la Secretaría.

5.3.2.2.1. Presidencia del Comité

La presidencia del Comité Municipal de Seguridad de la Información corresponde al titular de la Concejalía Delegada Especial de Modernización Administrativa.

Corresponde a la Presidencia las siguientes funcione:

a) Ostentar la representación del Comité Municipal de Seguridad de la Información.

b) Acordar las convocatorias de las sesiones y determinar el orden del día.

c) Presidir las sesiones y moderar los debates que pudieran originarse.

d) Concluir los empates en la toma de decisiones, si estos se dieran, con su voto de calidad.

e) Asegurar el cumplimiento de las leyes.

f) Visar las actas y propuestas adoptadas por el Comité Municipal de Seguridad de la Información, así como las certificaciones de sus acuerdos.

g) Remitir a la Junta de Gobierno Local los acuerdos y resoluciones del Comité Municipal de Seguridad de la Información para su aprobación cuando ello fuese procedente.

h) Ejercer cuantas otras funciones sean inherentes a su condición.

5.3.2.2.2. Secretaría del Comité

La secretaria del Comité Municipal de Seguridad de la Información corresponde al titular del Centro de Sistemas y Comunicaciones, y no ostentará la condición de vocal. Las funciones del Secretario del Comité son las siguientes:

a) Asistir a las reuniones con voz pero sin voto.

b) Efectuar las convocatorias de las sesiones por orden de la Presidencia, así como las citaciones a cada miembro del órgano.

c) Preparar el despacho de los asuntos.

d) Redactar las actas de las sesiones, autorizándolas con su firma y el visto bueno de la Presidencia.

e) Expedir certificaciones de las consultas, dictámenes y acuerdos aprobados con el visto bueno de la Presidencia.

f) Recibir las comunicaciones de cada miembro del órgano y, por tanto, las notificaciones, peticiones de datos, rectificaciones o cualquier otra clase de escritos de los que deba tener conocimiento.

g) Ejercer cuantas otras funciones sean inherentes a su condición.

5.3.2.2.3. Vocalías.

Serán titulares de las vocalías del Comité Municipal de Seguridad de la Información:

- El Director del Área de Hacienda, Personal y Modernización administrativa.
- El Director del Servicio de Información y Administración electrónica.
- El Responsable de Seguridad de la Información
- El Responsable del Sistema.

- El Delegado de Protección de Datos. Participará con voz, pero sin voto, en las reuniones del Comité Municipal de Seguridad de la Información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal que impliquen una decisión sobre los fines y los medios del tratamiento, así como siempre que se requiera su participación. En todo caso, si un asunto de esta naturaleza se sometiese a votación, se hará constar siempre en acta la opinión del delegado de protección de datos. Las decisiones del Comité deberán respetar su independencia cuando ejerza la posición y funciones que le otorgan los artículos 38 y 39 RGPD y el Capítulo III y la disposición adicional decimoséptima sobre tratamientos de datos de salud de la LOPDGDD.

Las vocalías tendrán asignadas las siguientes funciones:

a) Asistir a las reuniones, participar en los debates y formular ruegos y preguntas.

b) Ejercer su derecho de voto, manifestar el sentido del mismo, así como los motivos que lo justifican.

c) Ejercer aquellas funciones que le sean encomendadas expresamente por el Comité o la Presidencia.

d) Velar por que la Política de Seguridad de la Información y su desarrollo sea difundida y aplicada en el ámbito en el que ejercen su representación.

e) Obtener la información lo más precisa posible para cumplir las funciones asignadas.

f) Ejercer cuantas otras funciones sean inherentes a su condición.

Por cada vocalía se designará un suplente entre el personal funcionario del mismo Área o Departamento al que pertenezca cada uno de los vocales titulares.

5.3.2.2.4. Otros asistentes.

A las sesiones del Comité Municipal de Seguridad de la Información podrán asistir, con voz, pero sin voto, quienes ostenten la condición de Responsable de Información, Responsable de Servicio, personas titulares de las Direcciones de Área, Secretaría General, Intervención General, Tesorería, así como personal funcionario o experto que, por razón de sus funciones, conocimiento o especialización, sean convocados por la Presidencia.

5.3.2.3. Periodicidad de las reuniones y adopción de acuerdos.

El Comité Municipal de Seguridad de la Información se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

En el caso concreto de que se estén llevando a cabo acciones de adecuación al ENS de los sistemas de información, y para evaluar el desarrollo de las mismas y posibilitar su adecuado seguimiento, el Comité Municipal de Seguridad de la Información se reunirá, al menos, una vez al trimestre.

En cualquier caso, las reuniones se convocarán por el presidente, a través del secretario, a su iniciativa o por mayoría de sus miembros permanentes.

Las decisiones se tomarán por mayoría simple de los asistentes a las reuniones, y en caso de empate, se abrirá un nuevo turno de palabra y se procederá a realizar una nueva votación. Si se produce un nuevo empate, decidirá el presidente con su voto de calidad.

El Comité podrá establecer sus propias normas de funcionamiento interno y, en lo no previsto, su funcionamiento se regirá supletoriamente por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

5.3.3. Responsable de Seguridad de la Información

El Responsable de Seguridad de la Información corresponde a la persona titular del Servicio de Información y Administración Electrónica del Ayuntamiento de Valladolid, y será la encargada de determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La función de Responsable de Seguridad de la Información corresponderá a la persona que tenga asignadas dichas funciones, de conformidad con la relación vigente de puestos de trabajo del Ayuntamiento de Valladolid.

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

a) Determinar las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios establecidos por sus respectivos responsables.

b) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

c) Analizar y elevar al Comité Municipal de Seguridad de la Información toda la documentación relacionada con la seguridad de los sistemas de información para su aprobación.

d) Realizar el seguimiento y control del estado de seguridad de los sistemas de información, verificando que las medidas de seguridad son adecuadas a través del análisis de riesgos.

e) Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos, impulsar su ejecución, dando soporte al resto de roles implicados, y realizando una recopilación y síntesis de los resultados para su presentación al Comité Municipal de Seguridad de la Información.

f) Elaborar y proponer la aprobación de la Declaración de Aplicabilidad, establecida en la regulación del ENS, de la información, servicios y sistemas de información del Ayuntamiento de Valladolid.

g) Elaborar y proponer los planes de adecuación al ENS, planes de mejora y planes de tratamiento de riesgos de seguridad de la información.

h) Establecer el conjunto de proyectos y actuaciones que conformarán el plan director de seguridad, que permitirá implantar las medidas de seguridad propuestas, y elevarlo al responsable del sistema de Información.

i) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución. Constituir el punto de contacto especializado para la coordinación con los Equipos de Respuesta ante Incidentes (CSIRT) de referencia.

j) Comunicar a la autoridad competente sus datos de contacto como Responsable de Seguridad de la Información.

k) Recibir, interpretar y aplicar las instrucciones y guías emanadas de la autoridad competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

l) Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

m) Analizar los incumplimientos de la normativa de seguridad, así como de los acuerdos de nivel de servicio relacionados con la seguridad de la información por parte de terceros, y escalarlos, en su caso, al Comité Municipal de Seguridad para su gestión.

n) Elaborar informes periódicos de seguridad para el Comité Municipal de Seguridad de la Información, que incluirán los incidentes más relevantes de cada periodo.

o) Realizar o promover auditorías periódicas para garantizar la correcta aplicación de las medidas de seguridad y el cumplimiento de las normas y procedimientos vigentes en la organización en materia de seguridad de la información. El informe resultante de las mismas se enviará a los responsables de los sistemas de Información y al responsable de la prestación del servicio para subsanar las deficiencias encontradas.

p) Elaborar, junto los responsables de los servicios y sistemas, los procedimientos operativos de seguridad, así como los planes de continuidad y respuesta a incidentes.

q) Gestionar los procesos de certificación en el ámbito de la seguridad de la información.

5.3.4. Responsable de la Información/Responsable del Servicio

El Responsable de la Información y de los Servicios corresponde a las personas titulares de las Direcciones de Área municipales o asimiladas, incluyendo a Secretaría General, Intervención General y Tesorería.

Las funciones del Responsable de la Información y los Servicios son las siguientes:

a) Decidir sobre la finalidad, contenido y uso de la información y datos personales.

b) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información y a los derechos y libertades de los afectados, conforme a lo establecido en ENS.

c) Realizar, junto al Responsable de Seguridad de la Información, los preceptivos análisis de riesgos y seleccionar las medidas de seguridad y salvaguardas que se han de implantar.

d) Realizar, junto con el Responsable de Seguridad de la Información, el seguimiento y control de los riesgos, incluyendo los relativos al incumplimiento de los acuerdos de niveles de servicio con terceros.

e) Determinar los niveles de seguridad del servicio tratado y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información.

f) Notificar al Responsable de Seguridad cualquier incumplimiento de los acuerdos de nivel de servicio relativos a la seguridad de la información por parte de terceros que provean servicios bajo su responsabilidad.

g) Suspender, de acuerdo con el Responsable del Sistema y el Responsable de Seguridad de la Información, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

h) Elaborar, junto con el Responsable de Seguridad de la Información, los procedimientos operativos de seguridad, así como los planes de continuidad y respuesta a incidentes.

i) Cualquier otra que les atribuya la normativa básica aplicable en materia de seguridad de la información.

5.3.5. Responsable del Sistema

El Responsable del Sistema corresponde a la persona titular del Departamento de Tecnologías de la Información y las Comunicaciones.

Las funciones del Responsable del Sistema son las siguientes:

a) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

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

c) Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo, cerciorándose de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

d) 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 el Responsable de la Seguridad, antes de ser ejecutada.

e) Elaborar, junto con el Responsable de Seguridad de la Información, los procedimientos operativos de seguridad, así como los planes de continuidad y respuesta a incidentes.

f) Notificar al Responsable de Seguridad cualquier incumplimiento de los acuerdos de nivel de servicio relativos a la seguridad de la información por parte de terceros que provean servicios bajo su responsabilidad.

g) Realizar, junto con el Responsable de Seguridad de la Información, el seguimiento y control de los riesgos, incluyendo los relativos al incumplimiento de los acuerdos de niveles de servicio con terceros que provean servicios de tecnologías de la información bajo su responsabilidad.

5.3.6. Administrador de Seguridad del Sistema

El Administrador de Seguridad del Sistema corresponde a la persona titular de la Jefatura del Centro de Sistemas y Comunicaciones, dependiente del Departamento de Tecnologías de la Información y las Comunicaciones.

Las funciones del Administrador del Sistema son las siguientes:

a) Implementar y controlar las medidas de seguridad aplicables al Sistema de Información, asegurándose de su cumplimiento.

b) Gestionar el hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información, llevando un control sobre su configuración y actualización para mantener un nivel de seguridad adecuado.

c) Aplicar los procedimientos operativos de seguridad aprobados, así como asegurar su aplicación.

d) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

e) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

f) Informar al Responsable de Seguridad de la Información y al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

g) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

5.4. Procedimientos de designación y renovación

La creación del Comité Municipal de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los responsables clave identificados en esta Política se realizará por la Junta de Gobierno Local y comunicada a las partes afectadas.

Este mismo órgano podrá revisar los nombramientos de los miembros del Comité Municipal de Seguridad de la Información, así como del resto de roles considerados por la PSI cuando estime oportuno o con ocasión de vacante.

5.5. Resolución de conflictos

El Comité Municipal de Seguridad de la Información se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles considerados por la PSI.

6. DESARROLLO DE LA PSI

La PSI se desarrolla documentalmente en un marco normativo de Seguridad de la Información que se estructura de la siguiente manera:

a) Primer Nivel:

i. La presente PSI, aprobada por la Junta de Gobierno local.

ii. Establece los principios y directrices, así como aspectos organizativos de la gestión de seguridad.

b) Segundo Nivel:

i. Las Normas de Seguridad de la Información son de obligado cumplimiento para todo el ámbito de aplicación de la PSI y serán aprobadas por el Comité Municipal de Seguridad de la Información.

ii. Desarrollan las directrices y principios generales aplicables a los procesos de gestión de seguridad considerados en el Anexo II del ENS sobre Medidas de Seguridad.

iii. Las citadas normas serán publicadas en la intranet del Ayuntamiento y puestas a disposición de todo personal que lo requiera, siempre con el control de acceso adecuado a su nivel de confidencialidad.

c) Tercer Nivel:

i. Los Procedimientos Operativos, Instrucciones Técnicas y Guías de los ámbitos de seguridad de la información, entre otros documentos de análogo nivel, son aprobadas por el Responsable de Seguridad de la Información.

ii. Concretan la operativa y gestión para cada proceso, o medida de protección, o simplemente tienen un carácter meramente informativo (caso de las guías).

Existirá una norma concreta de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

7. DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Valladolid solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos, de acuerdo con la Política de Protección de Datos Personales del Ayuntamiento de Valladolid.

8. OBLIGACIONES DEL PERSONAL

Todo el personal del Ayuntamiento de Valladolid que se encuentran dentro del ámbito del ENS deberá ser formado e informado de su deberes y obligaciones en materia de seguridad. Se prestará la máxima atención a su formación con la realización de sesiones presenciales o de concienciación en materia de seguridad en función de la periodicidad que el Comité Municipal de Seguridad de la Información establezca como necesario y razonable en base a las necesidades detectadas, y siendo en todo caso un programa de concienciación continua que aspira a atender a todos los miembros del Ayuntamiento de Valladolid, y en particular a los de nueva incorporación.

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

9. TERCERAS PARTES

En las relaciones del Ayuntamiento con un tercero en el que este último preste un servicio al primero, se hará partícipe al tercero de esta PSI y de la normativa de seguridad de aplicación en el Ayuntamiento para su conocimiento.

La citada tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa en lo que se refiere al uso de los servicios e información del Ayuntamiento, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. En particular, se establecerán procedimientos específicos de reporte y resolución de incidencias. Igualmente se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta PSI.

Cuando algún aspecto de esta PSI 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.

De forma análoga, el Ayuntamiento deberá velar por solicitar la PSI de la tercera parte para garantizar la seguridad de la información y servicios prestados a la misma.

Cuando el Ayuntamiento de Valladolid preste servicios o ceda información a un tercero, se les hará partícipes de la presente PSI así como de la normativa de aplicación relevante.

En todo caso, se establecerán canales de comunicación entre las partes para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

10. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Junta de Gobierno Local en el día de la fecha electrónica del presente documento.

Esta PSI es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

La entrada en vigor de la presente Política del Ayuntamiento supone la derogación de cualquier otra que existiera a nivel de los diferentes departamentos municipales.