Marco Normativo
Política de Seguridad

Ayuntamiento de León

Título:	Política de Seguridad
Tipo de documento:	Marco Normativo
Nombre del Fichero:	2023-09-20-ENS_POL_Politica_de_seguridad.docx
Clasificación:	Uso Oficial

Revisión y aprobación		**Fecha**
Revisado por:	Responsable de Seguridad	18/09/2023
Aprobado por:	Comité de Seguridad	20/09/2023

Control de Cambios

Versión	Fecha	Autor	Descripción del Cambio
1.0	18/09/2023	Javier García Diez	Versión Inicial
1.1	20/09/2023	Comité de Seguridad	Versión Revisada

Índice

1. Introducción

El Ayuntamiento de León, depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados.

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

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que las áreas, subáreas, servicios y demás unidades administrativas en los que se estructura el Ayuntamiento de León (en adelante, los departamentos) deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y la valoración de su coste, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, con la aplicación de las medidas que se relacionan a continuación. Ajustar esta conducta a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

2. Misión y servicios prestados

El Ayuntamiento de León, en su calidad de Entidad Local, y, por tanto, como Administración Pública, sirve con objetividad los intereses generales y actúa de acuerdo a los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de los habitantes del municipio.

En este sentido, el Ayuntamiento de León ejerce sus competencias con el alcance y en los términos previstos en la legislación del Estado y de la Comunidad Autónoma de Castilla y León.

Para la gestión de sus intereses y de las funciones y competencias que tiene atribuidas en las diferentes normas y/o convenios, el Ayuntamiento de León promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población. A tal efecto, pone a disposición de ésta la realización de trámites online con el objetivo de impulsar la tramitación electrónica de los procedimientos administrativos, la mejora en la prestación de los servicios y la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la mejora de la eficacia y eficiencia de la acción pública.

Se pretende, por tanto, potenciar el uso de las nuevas tecnologías no solo en el propio Ayuntamiento, sino también en la ciudadanía, siendo los principales objetivos que se persiguen, entre otros, los siguientes: fomentar la relación electrónica de la ciudadanía con el Ayuntamiento; y crear la confianza necesaria entre ciudadano y Ayuntamiento en esta relación.

3. Principios básicos y requisitos mínimos

3.1. Principios básicos

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes principios básicos:

a) La Seguridad como proceso integral.

b) Vigilancia continua y reevaluación periódica.

c) Gestión profesional.

d) Gestión de la seguridad basada en los riesgos.

e) Prevención, detección, respuesta y conservación.

f) Existencia de líneas de defensa.

g) Diferenciación de responsabilidades.

3.2. Requisitos mínimos

Los anteriores principios básicos se desarrollarán aplicando los siguientes requisitos mínimos:

La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al Ayuntamiento de León, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

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

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

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

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continuada del proceso de seguridad

La vigilancia continua por parte del Ayuntamiento de León permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

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

Gestión de personal y profesionalidad

Todo el personal, propio o ajeno, relacionado con los sistemas de información del Ayuntamiento de León dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo, bajo las siguientes premisas:

a) Todos los empleados del Ayuntamiento de León deberán recibir información, formación y concienciación en materia de seguridad. A tal efecto, se establecerá un programa de concienciación continua.

b) 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 se necesaria para realizar su trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo

de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II el Real Decreto 311/2022, de 3 de mayo, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Incidentes de seguridad, prevención, detección, reacción y recuperación

El Ayuntamiento de León dispondrá de procedimientos de gestión de incidentes de seguridad ajustados a lo previsto en el artículo 33 del Real Decreto 311/2022, de 3 de mayo, y a la Instrucción Técnica de Seguridad correspondiente, y habilitará mecanismos de detección, criterios de clasificación y procedimientos de análisis y resolución, estableciendo los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

El Ayuntamiento de León ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, integradas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema del Ayuntamiento se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

El Ayuntamiento de León ha organizado su seguridad comprometiendo a todos los integrantes de la organización mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de modelo de gobernanza del presente documento.

Autorización y control de los accesos

El Ayuntamiento de León dispondrá de mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Protección de las instalaciones

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

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad el Ayuntamiento de León tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

Protección de la información almacenada y en tránsito y continuidad de la actividad

El Ayuntamiento de León prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el Real Decreto 311/2022, de 3 de mayo, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Registro de actividad y detección de código dañino

El Ayuntamiento de León, con el propósito de satisfacer los objetivos del Real Decreto 311/2022, de 3 de mayo, con plenas garantías del derecho al honor, a la

intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, el Ayuntamiento podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Infraestructuras y servicios comunes

El Ayuntamiento de León tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, y facilitará el cumplimiento de lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras

El Ayuntamiento de León, tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para Entidades Locales que sean de aplicación.

4. Objetivos de la seguridad de la información

El Ayuntamiento de León establece como objetivos de la seguridad de la información, los siguientes:

- Garantizar la calidad y protección de la información.

- Lograr la plena concienciación de los usuarios respecto a la seguridad de la

información.

- Gestión de activos de información: Los activos de información de la organización se encontrarán inventariados y categorizados y estarán asociados a un responsable.

- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.

- Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

- Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto. Siendo obligada la supervisión por parte del Servicio de Recursos para la Información y la Comunicación para añadir o modificar sistemas de Información en cualquier área.

- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.

- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

5. Alcance

La Política de Seguridad de la Información contenida en este documento se aplicará a los sistemas de información del Ayuntamiento de León que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo, y que se encuentran dentro del ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

6. Marco normativo

El marco normativo que afecta al desarrollo de las actividades y competencias del Ayuntamiento de León, en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituido por las siguientes normas:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

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

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD).

- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.

- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.

- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

- Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro electrónico de facturas en el sector público.

- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.

- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en cuanto al archivo de documentos.

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, conforme a la vigencia establecida en la Disposición Derogatoria Única de la Ley 11/2022, de 28 de junio.

- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

- Ley 11/2022, de 28 de junio, General de Telecomunicaciones, conforme a la disposición que regula su entrada en vigor.

- Forman parte del presente marco normativo, las normativas sectoriales y la

normativa autonómica que, en su ámbito de aplicación, afecten a las entidades locales en lo que se refiere a la prestación de servicios y/o procedimientos.

- Forman igualmente parte de este marco normativo las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en la Disposición Adicional Segunda del Real Decreto 311/2022, de 3 de mayo.

- Se incluyen, asimismo, en este marco normativo las guías de seguridad del CCN, a que se refiere el artículo 30 del Real Decreto 311/2022, de 3 de mayo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

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

El mantenimiento del marco normativo será responsabilidad del Ayuntamiento de León, y se mantendrá actualizado en un **Anexo** a este documento.

7. Organización de la seguridad de la información

7.1. Criterios de la seguridad de la información

El Ayuntamiento de León, teniendo en cuenta la regulación legal establecida en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), establece las siguientes acciones para organizar la Seguridad de la Información:

i) Designará roles de seguridad, diferenciando entre Responsable de la Información, Responsable de la Seguridad de la Información, Responsable del Sistema, Responsable del Servicio (conforme a la estructura organizativa de la Entidad Local) y Delegado de Protección de Datos.

ii) Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se denominará "**Comité de Seguridad de la Información**".

7.2. Definición de Roles y Responsabilidades asociados al ENS

7.2.1. Responsable de la Información (RI)

Es el cargo de mayor responsabilidad, en el que se situará a una persona situada en el máximo nivel directivo de la organización. A quien asuma dicha responsabilidad le corresponden, sin carácter limitativo, las siguientes funciones:

- Establecer los requisitos de seguridad aplicables a la información (niveles de seguridad de la Información) en coordinación con el Responsable del Servicio (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.

- Aceptar los niveles de riesgo residual que afectan a la información y a los servicios.

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

- Dictaminar respecto a los derechos de acceso a la información y a los servicios.

- Comunicar al Responsable de Seguridad cualquier variación respecto a la Información de la que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.

- Tiene la responsabilidad última del uso que se haga de la información de la que es responsable, y, por tanto, de su protección.

- Tiene la responsabilidad última de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

7.2.2. Responsable de la Seguridad de la Información (RSEG)

Es la persona que adopta las decisiones necesarias para satisfacer los requisitos de seguridad dentro de la entidad. Al Responsable de seguridad, le corresponden, sin carácter limitativo, las siguientes funciones:

- Mantener y verificar el nivel adecuado de Seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.

- Promover la formación y concienciación en materia de seguridad de la información.

- Designar los responsables de la ejecución del análisis de riesgos, aprobar la Declaración de Aplicabilidad, identificar las medidas de seguridad, determinar las configuraciones necesarias y elaborar la documentación del sistema.

- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad.

- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.

- Gestionar las revisiones externas o internas del sistema.

- Gestionar los procesos de certificación.

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

- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (que no sean competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información, para su aprobación por el órgano municipal competente.

- Actuar como Secretario del Comité de Seguridad de la Información, realizando las siguientes funciones:

a) Convocar las reuniones del Comité de Seguridad de la Información.

b) Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.

c) Elaborar el acta de las reuniones.

d) Es responsable de la ejecución directa o delegada de las decisiones del Comité en materia de Seguridad de la Información.

7.2.3. Responsable del Sistema (RSIS)

Es la persona que mantiene, controla y tiene conocimiento sobre todo el Sistema de Información de la entidad. A dicho responsable le corresponden, sin carác-

ter limitativo, las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.

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

- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

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

- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información de la Información.

- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.

- Coordinar las funciones del administrador de la seguridad del sistema. A este respecto, le corresponden las siguientes funciones:

a) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.

b) La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.

c) Aprobar los cambios en la configuración vigente del Sistema de Información.

d) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

e) Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.

f) 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.

g) Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

h) Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

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

7.2.4. Responsable del Servicio (RS)

Es el responsable de la información de los servicios que se prestan directa o indirectamente al ciudadano. Pueden ser designados varios Responsables del Servicio, en función de la estructura organizativa de la entidad. Al Responsable del Servicio le corresponden, sin carácter limitativo, las siguientes funciones:

- En cuanto al Reglamento General de Protección de Datos (RGPD), por delegación del Responsable del tratamiento, se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su área concreta.

- Establecer los requisitos de los servicios en materia de seguridad, lo que, en el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

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

- Tiene la responsabilidad última de cualquier error o negligencia que lleve a un incidente de disponibilidad del servicio.

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

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

Conforme a ello, y teniendo en cuenta la actual estructura organizativa del Ayuntamiento de León, se designarán los siguientes **Responsables del Servicio**:

- En el Área de Secretaria General: La Sra. Secretaria General.

- En el Área de la Intervención: El Sr. Interventor Municipal.

- En el Área de Tesorería: El Sr. Tesorero Municipal.

- En el Área de Cohesión Social e Igualdad: La Coordinadora del Área.

- En el Área de Servicios a la Ciudadanía: La Coordinadora del Área.

- En el Servicio de Policía Local: El Intendente-Jefe de la Policía Local.

- En el Servicio de Prevención, Extinción de Incendios y Salvamento: El Oficial Superior del citado Servicio.

- En el Área de Fomento y Hábitat Urbano: El Coordinador del Área.

- En el Área de Organización y Recursos: El Coordinador del Área.

7.2.5. Delegado de Protección de datos (DPD)

Son funciones del Delegado de Protección de Datos en materia de seguridad de la información, sin carácter limitativo, las siguientes:

- 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 de la normativa vigente en materia de Protección de Datos.

- Supervisar el cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos (RGPD) y en la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDyGDD), 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.

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.

- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, y actuar como punto de contacto con ésta para cuestiones relativas al tratamiento de datos incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

- El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento. Para ello debe de ser provisto de los medios necesarios para:

a) Recabar información para determinar las actividades de tratamiento.

b) Analizar y comprobar la conformidad con la normativa de las actividades de tratamiento.

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

d) Recabar información para supervisar el registro de las operaciones de tra-

tamiento.

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

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

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

h) Asesorar al responsable del tratamiento sobre qué áreas deben someterse a auditoría de protección de datos interna o externa y sobre que qué actividades de formación internas proporcionar al personal o los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

7.3. Comité de Seguridad de la Información

El Ayuntamiento de León ha creado el "**Comité de Seguridad de la Información**" (en adelante, y de forma abreviada, Comité de Seguridad), que estará formado por todas aquellas personas con responsabilidad en materia de seguridad de la información en el Ayuntamiento de León.

El Comité de Seguridad se constituye como órgano colegiado, de conformidad con lo señalado en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y sus funciones y competencias, así como su funcionamiento, son las que se concretan a continuación.

7.3.1. Composición del Comité de Seguridad

El Comité de Seguridad vendrá integrado por:

- Presidente.
- Secretario.
- Vocales.

Corresponde el cargo de **Presidente del Comité** al **Responsable de la Información (RI)** del Ayuntamiento de León, mencionado en el apartado 7.2.1 anterior.

Corresponde el cargo de **Secretario del Comité**, al **Responsable de Seguridad de la Información (RSEG)** del Ayuntamiento de León, mencionado en el apartado 7.2.2 anterior.

Serán **Vocales del Comité** los siguientes **Responsables**:

a) **El Responsable del Sistema (RSIS)** del Ayuntamiento de León, mencionado en el apartado 7.2.3 anterior.

b) Los **Responsables del Servicio** de las diferentes Áreas y/o Servicios en que se estructura el Ayuntamiento de León, mencionados en el apartado 7.2.4 anterior.

c) El **Delegado de Protección de Datos (DPD)** del Ayuntamiento de León, mencionado en el apartado 7.2.5 anterior.

Los miembros del Comité de Seguridad serán sustituidos, en caso de vacante o ausencia, por las siguientes personas:

- Quienes sean FALHN, por los funcionarios que legalmente les sustituyan.

- Los Coordinadores del Área, por el Jefe de Subárea con mayor antigüedad.

- Los responsables de la Policía Local y del Servicio Prevención, Extinción de Incendios y Salvamento, por quienes normalmente les sustituyan en similares circunstancias.

7.3.2. Atribuciones del Comité de Seguridad de la Información

Serán funciones del Comité de Seguridad, sin carácter limitativo, las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de los órganos municipales y de los diferentes roles de seguridad y/o departamentos, informando regularmente del estado de aquélla.

- Asesorar en materia de Seguridad de la Información, siempre que sea requerido para ello.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes departamentos, proponiendo las correspondientes soluciones en aquellos casos en los que no tenga suficiente autoridad para decidir.

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.

- Elaborar la estrategia de evolución en lo que respecta a la Seguridad de la Información.

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

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

- Aprobar la documentación de Seguridad de la Información.

- Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.

- Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.

- Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.

- Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su Presidente, deberá dar cumplida respuesta.

- Proponer la Política de Seguridad de la Información al órgano municipal competente para su aprobación, incluyendo las revisiones periódicas de dicha Política de Seguridad.

- Aprobar el Plan de Adecuación para la implantación del ENS.

7.3.3. Régimen de funcionamiento del Comité

El **Comité de Seguridad** vendrá integrado por todos sus miembros.

No obstante, y para la gestión ordinaria de la Seguridad de la Información, se crea, en el seno del Comité una **Comisión Permanente** que vendrá integrada por los siguientes miembros:

- El Presidente (RI).
- El Secretario (RSEG).
- El Responsable del Sistema (RSIS).
- El Delegado de Protección de Datos (DPD).
- El Responsable del Servicio al que esté adscrito el “Servicio de Recursos

para la Información y la Comunicación" del Ayuntamiento de León.

A dicha Comisión Permanente **se incorporarán los distintos Responsables del Servicio** cuando los asuntos a tratar afecten a la seguridad de la información del correspondiente Servicio, a criterio de la Presidencia.

El Comité de Seguridad podrá estar asistido por aquellos asesores internos que se consideren oportunos, en función de los asuntos a tratar, que tendrán voz, pero no voto.

Asimismo, podrán asistir a la reunión, previa invitación por la Presidencia, especialistas externos, ya sean del sector público o del sector privado, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

El/La Secretario/a del Comité realizará las convocatorias y levantará actas de las reuniones del Comité de Seguridad.

7.3.4. Periodicidad de las reuniones y adopción de acuerdos

El Comité de Seguridad de la Información se reunirá, con carácter ordinario, al menos una vez al semestre, para realizar el seguimiento periódico de la Política de Seguridad, y, en todo caso, para aprobar el documento de Política de Seguridad que se haya de proponer al órgano de gobierno municipal, así como las revisiones de dicho documento.

La Comisión Permanente del Comité de Seguridad de la Información se reunirá, con carácter ordinario, al menos una vez al mes, para adoptar las decisiones de gestión ordinaria que corresponda conforme a las funciones que tiene atribuidas.

Tanto el Comité de Seguridad, como su Comisión Permanente, se reunirán en sesión extraordinaria cuando así lo decida su Presidente.

Las decisiones del Comité se adoptarán, en lo posible, por consenso de sus miembros, y si ello no fuera posible, por acuerdo mayoritario.

7.4. Designación y resolución de conflictos

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política de Seguridad, se realizará por acuerdo de la Junta de Gobierno Local del Ayuntamiento de León.

Los roles designados se desempeñarán de forma permanente mientras no se acuerde su revisión.

La bajas o modificación en cada uno de los roles designados, se comunicarán

al Comité de Seguridad. Corresponde al órgano municipal competente la designación del nuevo responsable.

Tal y como dispone el artículo 13.3 del Real Decreto 311/2022, de 3 de mayo, que estipula que el Responsable de la Seguridad (RSEG) será distinto del Responsable del Sistema (RSIS), no debiendo existir dependencia jerárquica entre ambos, salvo excepciones justificadas, se establece como medida compensatoria para garantizar la finalidad del principio de diferenciación de responsabilidades, la absoluta independencia del Responsable del Sistema (RSIS) para el ejercicio de las funciones que tiene encomendadas, independencia ésta que viene garantizada por esta Política, cuyo seguimiento se encomienda al Comité de Seguridad.

8. Datos personales y riesgos que se derivan del tratamiento

El Ayuntamiento de León, en el tratamiento de los datos personales, cumple con los principios y obligaciones de la normativa vigente, entre la que se encuentra el Reglamento 679/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales; respetando, en todo caso, el derecho fundamental a la protección de los datos personales, la intimidad de la persona y los demás derechos fundamentales reconocidos tanto en la Constitución Española, como en la restante legislación nacional y en los tratados internacionales.

El Ayuntamiento de León, tiene publicado su Registro de Actividades de Tratamiento (RAT) en la Sede Electrónica municipal, en el apartado de Protección de Datos, y realiza la gestión de riesgos a través de Análisis de Riesgos y de la Evaluación de Impacto relativa a la Protección de Datos (EIPD), en el caso de que así fuera necesario ésta en la organización.

9. Obligaciones del personal

Todo el personal, tanto externo como interno, que interactúe con el sistema de información deberá de cumplir con la presente política de seguridad de la información.

Todos los empleados públicos y cargos del Ayuntamiento de León tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue al personal afectado.

10. Documentación complementaria

La presente Política de Seguridad de la Información será complementada con documentos más precisos (normas, guías y procedimientos de seguridad) que ayuden a llevar a cabo lo propuesto.

El cuerpo normativo se desarrollará en tres niveles:

a) Primer nivel normativo: constituido por la presente Política de Seguridad de la Información.

b) Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores con el objetivo de indicar el uso correcto de aspectos concretos del sistema de gestión de seguridad de la información.

c) Tercer nivel normativo: constituido por procedimientos de seguridad, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al Comité de Seguridad la aprobación de los documentos de segundo y tercer nivel normativo, así como la supervisión de su aplicación.

11. Aprobación y revisión de la Política de Seguridad

De conformidad con lo dispuesto en el artículo 21.1,s) de la Ley 7/1985, de 2 de abril, de Bases del Régimen Local, corresponde a la Alcaldía-Presidencia la aprobación de la Política de Seguridad de la Información del Ayuntamiento de León.

Dado que la Alcaldía-Presidencia tiene delegadas todas sus competencias, salvo las indelegables, en la Junta de Gobierno Local del Ayuntamiento de León, corresponde a ésta, por delegación de la Alcaldía-Presidencia, la aprobación de la Política de Seguridad de la Información del Ayuntamiento de León, a propuesta del Comité de Seguridad de la Información.

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

Corresponde aprobar la revisión de la Política de Seguridad al mismo órgano que la aprobó inicialmente, a propuesta del Comité de Seguridad de la Información.

Cualquier cambio que se lleve a efecto en la Política de Seguridad deberá ser difundido a todas las partes afectadas.

12. Terceras partes

Cuando el Ayuntamiento de León preste servicios a otros organismos o maneje información de otros organismos, se les hará participe de esta Política de Seguridad de la Información. A tal efecto, se establecerán canales 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.

Cuando el Ayuntamiento de León utilice servicios de terceros o ceda información a terceros, se les hará participe de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. A tal efecto, se establecerán procedimientos específicos de reporte y resolución de incidencias.

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

Asimismo, y teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad que establece la Disposición Adicional Segunda del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, se exigirá a dichos terceros tal Declaración.

Cuando algún aspecto de esta Política de Seguridad de la Información 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 por los servicios afectados antes de seguir adelante.

A tal efecto, la relación del Ayuntamiento de León con estas terceras partes se establecerá mediante un canal específico de comunicación.

13. Aprobación y entrada en vigor

Esta Política de Seguridad de la Información, será efectiva desde su fecha de aprobación y hasta que la misma sea reemplazada por una nueva Política.

Texto aprobado el día veintidós de septiembre de dos mil veintitrés, por la Junta de Gobierno Local del Ayuntamiento de León.