

III. ADMINISTRACIÓN LOCAL

AYUNTAMIENTO DE

52

LAS ROZAS DE MADRID

ORGANIZACIÓN Y FUNCIONAMIENTO

La Junta de Gobierno Local, en sesión ordinaria, celebrada el día 25 de noviembre de 2022, entre otros, adoptó el acuerdo cuya parte dispositiva es del tenor literal siguiente:

“1.º Aprobar el documento de “Política de seguridad de la información del Ayuntamiento de Las Rozas de Madrid”.

2.º Designar los siguientes puestos en seguridad de la información:

- Responsable de la Información: Sonia Crespo Nogales, Directora General de la Oficina Digital.
- Responsable de los Servicios: María José Jiménez Moreno, jefa de Servicios Digitales, Calidad y Atención Ciudadana.
- Responsable de Seguridad: María Teresa Cuesta Cosías, jefa de Tecnologías de la Información y la Comunicación.
- Responsable del Sistema: Jorge Pablos Carretero, responsable de Sistemas.
- Interlocutor del delegado de Protección de Datos, Miguel Ángel García López, adjunto a la Asesoría Jurídica.

3.º Publicar dicho documento en la página web municipal (normativa de aplicación), en el Portal de Transparencia y remitir anuncio indicativo, para su publicación, en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID.

4.º La vigencia de dicho documento comenzará con la aprobación del documento por la Junta de Gobierno Local, sin perjuicio de su publicación en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID y Portal de Transparencia”.

Siendo el texto del documento de “Política de seguridad de la información del Ayuntamiento de Las Rozas de Madrid” el siguiente:

«POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE LAS ROZAS DE MADRID

1. Introducción

El desarrollo de la Administración Electrónica implica el tratamiento de gran cantidad de información por parte de los sistemas de tecnologías de la información y de las comunicaciones. La información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. El Real Decreto por el que se regula el Esquema Nacional de Seguridad (ENS) 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.

Al objeto de dar cumplimiento al ENS, el Ayuntamiento de Las Rozas de Madrid, conocedor de los riesgos que pueden afectar a los sistemas de información, que soportan los trámites electrónicos puestos a disposición a la ciudadanía, y teniendo en cuenta que ésta pone a su disposición su activo más valioso “su propia Información” es consciente de que éstos deben ser administrados con la suficiente diligencia, y que se deben de tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

De este modo, todos los departamentos y/o áreas del Ayuntamiento de Las Rozas, que se encuentran dentro del ámbito del ENS, tienen presente que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser iden-

tificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, para el Ayuntamiento de Las Rozas de Madrid, 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 recuperarse lo antes posible, acorde a lo establecido en el ENS.

2. Misión del Ayuntamiento de Las Rozas de Madrid

El Ayuntamiento de Las Rozas de Madrid pone a disposición de la ciudadanía la realización de trámites online con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la administración electrónica y la eficacia de la acción pública, potenciando el uso de las nuevas tecnologías en la Organización y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con la Administración reduciendo así los tiempos de espera y de resolución de trámites solicitados por éstos.

Y todo ello porque es exigencia de la normativa de procedimiento administrativo común, así como de diversa normativa sectorial.

3. Alcance

Esta política se aplicará a los sistemas de información del Ayuntamiento de Las Rozas de Madrid que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del alcance del Esquema Nacional de Seguridad (ENS).

Todos los empleados públicos y cargos electos (miembros) del Ayuntamiento de Las Rozas de Madrid, así como el personal de terceros relacionados con éste, que se encuentren afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

4. Marco normativo

El marco normativo relevante en que se desarrollan las actividades del Ayuntamiento de Las Rozas de Madrid, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía está integrado por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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 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.
- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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.
- Toda aquella normativa en vigor que regule la administración electrónica a nivel municipal.

El Ayuntamiento mantendrá un registro con el marco normativo aplicable al ayuntamiento, incluyendo las instrucciones técnicas de seguridad de obligado cumplimiento tal y como se contempla en el Esquema Nacional de Seguridad, siendo el Comité de Seguridad de la Información el encargado del mantenimiento del precitado registro.

Asimismo, el Comité de Seguridad de la Información también será responsable de identificar las guías de seguridad del CCN, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

5. Cumplimiento de los requisitos mínimos de seguridad

El Ayuntamiento de Las Rozas, para lograr el cumplimiento del Real Decreto por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

5.1. 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 Las Rozas, 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.

5.2. Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad:

La vigilancia continua por parte del Ayuntamiento de Las Rozas 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.

5.3. Gestión de personal y profesionalidad:

Todo el personal, propio o ajeno relacionado con los sistemas de información del Ayuntamiento de Las Rozas, 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.

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.

5.4. 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 del ENS, 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.

5.5. Incidentes de seguridad, prevención, detección, reacción y recuperación:

El Ayuntamiento de Las Rozas dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el ENS, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de 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.

5.6. Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados:

El Ayuntamiento de Las Rozas, ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas 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 Ley 9/2014, de 9 de mayo, General 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.

5.7. Diferenciación de responsabilidades, organización e implantación del proceso de seguridad:

El Ayuntamiento de Las Rozas, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de “Organización de la seguridad” del presente documento.

5.8. Autorización y control de los accesos:

El Ayuntamiento de Las Rozas, ha implementado 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.

5.9. Protección de las instalaciones:

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

5.10. 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 Las Rozas 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.

5.11. Protección de la información almacenada y en tránsito y continuidad de la actividad El Ayuntamiento de Las Rozas, 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 este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, 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.

5.12. Registro de actividad y detección de código dañino:

El Ayuntamiento de Las Rozas, con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, 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.

5.13. Infraestructuras y servicios comunes:

El Ayuntamiento de Las Rozas, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

5.14. Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras:

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

6. Organización de la seguridad

La estructura organizativa de la Organización de la Seguridad de la Información en el Ayuntamiento de Las Rozas de Madrid se establece en la forma que se indica a continuación.

Roles o perfiles de seguridad:

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad, y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Responsable de la Información: Dirección General de la Oficina Digital.
- Responsable de los Servicios: Jefatura de Servicios digitales, calidad y atención ciudadana.
- Responsable de Seguridad: Jefatura de Tecnologías de la Información y Comunicación.
- Responsable del Sistema: Responsable de Sistemas y Redes.

Comité de Seguridad de la Información:

El Ayuntamiento de Las Rozas de Madrid ha constituido un Comité de Seguridad de la Información, como órgano colegiado y está formado por los siguientes miembros:

- Presidente: concejal que ostente las competencias en materia de Oficina Digital.
- Secretario: responsable de Seguridad.
- Vocales:
 - Responsable del Sistema.
 - Responsable de la Información.
 - Responsable de los Servicios.
 - Interlocutor del delegado de Protección de Datos.

El interlocutor del delegado de Protección de Datos participará con voz, pero sin voto, en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta la opinión del interlocutor del delegado de Protección de Datos.

Con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

El Comité de Seguridad celebrará sus sesiones en las dependencias del Ayuntamiento de Las Rozas de Madrid con periodicidad semestral, previa convocatoria al efecto realizada por el Presidente de dicho Comité.

El Comité de Seguridad, se encargará también, de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

Responsabilidades asociadas al Esquema Nacional de Seguridad:

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de las figuras, responsabilidades que recoge el Comité de Seguridad.

— Funciones del responsable de los Servicios:

- Establecer y aprobar los requisitos de seguridad aplicables al servicio dentro del marco establecido en el anexo I del ENS y las guías CCN-STIC, del CCN, previa propuesta al Responsable de Seguridad, y/o Comité de Seguridad de la Información.
- Informar sobre los derechos de acceso al Servicio.
- Aceptar los niveles de riesgo residual que afecten al Servicio.
- Poner en comunicación del Responsable de Seguridad, cualquier variación respecto a los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios a su cargo.

— Funciones del responsable de la Información:

- Establecer y aprobar los requisitos de seguridad aplicables a la información dentro del marco establecido en el anexo I del ENS y las guías CCN-STIC, del CCN, previa propuesta al Responsable de Seguridad, y/o Comité de Seguridad de la Información.
- Informar sobre los derechos de acceso a la Información.
- Aceptar los niveles de riesgo residual que afectan a la Información.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información de los que es responsable, especialmente la incorporación de nueva Información a su cargo.

— Funciones del responsable de Seguridad:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

— Las funciones del responsable del Sistema:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- 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.
- 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.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
 - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.

- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Cuando la complejidad del sistema lo justifique el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

Funciones del Comité de Seguridad de la Información:

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Asumir las funciones del Responsable de la Información y del Responsable del Servicio.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
 - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
 - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
 - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
 - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
 - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
 - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
 - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General del Organismo.
 - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
 - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
 - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
 - Promover la realización de las auditorías periódicas ENS que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

Procedimientos de designación:

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política será realizada por el órgano con competencias en la materia del Ayuntamiento de Las Rozas de Madrid.

Los miembros del Comité, así como los roles de seguridad serán revisados cada cuatro años o con ocasión de vacante.

Resolución de conflictos:

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

7. Datos de carácter personal

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

El Ayuntamiento de Las Rozas de Madrid ha implementado los mecanismos adecuados para garantizar la adecuación a la normativa vigente en materia de protección de datos. En particular el Ayuntamiento ha adoptado las medidas oportunas para adecuarse al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, consistentes en el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se llevan a cabo, el análisis de riesgos de los tratamientos, la evaluación de impacto en los casos en los que sea requerido, el registro de actividades y el nombramiento del Delegado de Protección de Datos.

8. Desarrollo de la política de seguridad de la información

El Comité de Seguridad de la Información ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte del concejal competente por razón de la materia del Ayuntamiento de Las Rozas de Madrid.

9. Terceras partes

Cuando el Ayuntamiento de Las Rozas de Madrid preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. 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 Las Rozas de Madrid utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad 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.

10. *Aprobación y entrada en vigor*

La Política de Seguridad de la Información será efectiva desde la fecha de aprobación por parte de la Junta de Gobierno Local del Ayuntamiento de Las Rozas de Madrid y hasta que sea reemplazada por una nueva Política.

La presente Política se publicará, además de en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID, en la Sede Electrónica y en el Portal de Transparencia del Ayuntamiento de Las Rozas de Madrid».

Las Rozas de Madrid, a 12 de febrero de 2024.—La directora general de la Oficina Digital, P. D. (decreto Alcaldía-Presidencia de 9 de octubre de 2023), Sonia Crespo Nogales.

(03/2.479/24)

