AYUNTAMIENTO DE
ROQUETAS DE MAR

Política de Seguridad de la Información

Documento en el que se recoge el compromiso del Ayuntamiento de Roquetas con garantizar la seguridad de la información y se establecen las medidas y controles que se adoptarán para asegurar la confidencialidad, integridad y disponibilidad de la información, así como para prevenir y mitigar los riesgos a los que los activos de información están expuestos.

Uso público

26/02/2024

Versión: 1.0

Información del documento

Título:	Política de Seguridad de la Información
Descripción:	Documento en el que se recoge el compromiso del Ayuntamiento de Roquetas con garantizar la seguridad de la información y se establecen las medidas y controles que se adoptarán para asegurar la confidencialidad, integridad y disponibilidad de la información, así como para prevenir y mitigar los riesgos a los que los activos de información están expuestos.
Calificación	Uso público
Responsable:	Responsable de Transformación Digital
Aprobador por:	Pleno Municipal
Autor/es:	Técnico de Transformación Digital
Fichero:	ROQ STIC-ENS-5 Política de Seguridad v1.0
Versión:	1.0
Fecha:	26/02/2024

Control de cambios

Versión	Fecha	Cambios realizados
1.0	26/02/24	Versión inicial del documento

Índice

1 Introducción

El Ayuntamiento de Roquetas de Mar, como muestra de compromiso con la seguridad de la información de sus sistemas, ha desarrollado la presente Política de Seguridad de la Información, en adelante Política de Seguridad, de conformidad con lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).

La Política de Seguridad es una declaración ética, responsable y de estricto cumplimiento en todo el Ayuntamiento de Roquetas de Mar, la cual es desplegada a través de las diferentes Normativas y Procedimientos con los que se procura que los riesgos sean tratados adecuadamente.

El uso de los Activos de información debe estar en consonancia con las buenas prácticas y procedimientos de trabajo profesionales, así como con los requisitos legales, reglamentarios y contractuales, que deben garantizar la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la información y los servicios.

2 Objetivos y ámbito de aplicación

- Este documento constituye el establecimiento de un marco organizativo y tecnológico en el Ayuntamiento de Roquetas de Mar.
- Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos y materiales y organizativos relacionados con los sistemas de información del Ayuntamiento de Roquetas de Mar, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.
- Debe ser conocida y cumplida por todos los empleados del Ayuntamiento de Roquetas de Mar, independientemente del puesto, cargo y responsabilidad dentro del mismo.

El Ayuntamiento de Roquetas de Mar depende de los Sistemas TIC (Tecnologías de la Información y las Comunicaciones) para alcanzar sus objetivos y prestar sus servicios a los ciudadanos, personal propio o externo, empresas terceras, otros organismos de la AAPP, etc. Estos sistemas deben ser administrados con diligencia, implantando las medidas adecuadas para protegerlos frente a daños deliberados o daños accidentales, que puedan afectar a las diferentes dimensiones de la Seguridad: Disponibilidad, Integridad, Confidencialidad, Trazabilidad y/o Autenticidad de la Información tratada o de los Servicios prestados.

El objetivo de la Seguridad de la Información consiste en garantizar la calidad de la Información y la prestación continuada de los Servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con rapidez a los incidentes de seguridad.

Los Sistemas TIC deben estar protegidos frente a las cambiantes amenazas, de rápida evolución, que puedan influir sobre las diferentes dimensiones de la Seguridad. Esto implica que las diferentes Áreas del Ayuntamiento de Roquetas de Mar deben aplicar las medidas de Seguridad exigidas por el ENS, así como realizar un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades detectadas o reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes Áreas del Ayuntamiento de Roquetas de Mar deben cerciorarse de que la Seguridad TIC es una parte integral de cada etapa del ciclo de vida de los sistemas de información, desde su concepción y diseño, hasta su retirada del servicio, pasando por las fases de desarrollo o adquisición, puesta en marcha y explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificadas e incluidas en la planificación, en la solicitud de ofertas, y en pliegos de licitación, para proyectos TIC.

3 Legislación y normativa de referencia

El marco normativo que afecta al desarrollo de las actividades y competencias del Ayuntamiento de Roquetas de Mar está constituido por normas jurídicas estatales (y autonómicas, si procede) orientadas a la administración electrónica, a la seguridad de la información y los servicios que la manejan, así como a la protección de datos de naturaleza personal. Las normas que constituyen dicho marco se encuentran recogidas en un registro al efecto, el cual se mantiene actualizado según señala el correspondiente procedimiento de gestión de requisitos legales.

El registro de la normativa aplicable estará recogido en el documento "Legislación y normativas aplicables en la Política de Seguridad" que puede ser consultado en la sección Política de Seguridad del portal web del Ayuntamiento de Roquetas de Mar.

4 Principios y directrices

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son la prevención, la detección, la respuesta y la recuperación, de manera que las amenazas existentes no se materialicen o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

4.1 Prevención

Se debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello deberán implementarse las medidas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas informáticos antes de entrar en funcionamiento.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

4.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10. Vigilancia continua y reevaluación periódica del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

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

4.3 Respuesta

Se debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

4.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.

4.5 Otros principios generales

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información del Ayuntamiento de Roquetas de Mar deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

4.6 Auditorías de la seguridad

Los sistemas de información serán objeto de una auditoría regular ordinaria, con carácter bianual, que verifique el cumplimiento de los requerimientos del ENS. Estas auditorías ordinarias, así como las extraordinarias se harán de acuerdo con lo establecido en el art. 31 del ENS y la Instrucción Técnica de

Seguridad de Auditoría de la Seguridad de los Sistemas de Información, aprobada por Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.

Los informes de auditoría serán presentados a la persona Responsable del Sistema competente, al/a Delegado/a de Protección de Datos, si afectara a estos, y al Responsable de Seguridad. Estos informes serán analizados por esta última persona que presentará sus conclusiones a la persona Responsable del Sistema para que adopte las medidas correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.

Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre seguridad TIC y seguridad de protección de datos, siempre que sea posible, las auditorías de seguridad de sistemas de información y las auditorías de protección de datos o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos se realizarán de manera conjunta.

5 Organización de la Seguridad de la Información

La estructura organizativa de la gestión de la seguridad de la información está compuesta por los siguientes agentes:

a) Junta de Gobierno
b) El Comité de Seguridad de la información
c) El Responsable de Seguridad
d) Responsables de la Información y de los Servicios
e) Responsable del Sistema de Información
f) Delegado de Protección de Datos
g) Responsable del Tratamiento
h) Responsables funcionales de los Tratamientos

Se llevará a cabo el nombramiento de los roles y funciones descritas en la presente Política de Seguridad de la Información a través de Decreto del Ayuntamiento de Roquetas de Mar incluyendo las funciones de cada uno de ellos.

5.1 Junta de Gobierno

Por Delegación del Ayuntamiento Pleno, el órgano colegiado que decide la misión y los objetivos de la Organización y aprueba la normativa derivada de esta Política.

5.2 Comité de Seguridad de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de Seguridad de la Información, dentro del ámbito de la presente Política de Seguridad, formado por un equipo multidisciplinar institucional que podrá estar integrado por el Alcalde-Presidente, Concejales y Funcionarios de Carrera, estos debidamente capacitados y habilitados, que coordinará las actividades y controles de seguridad establecidos en el Ayuntamiento de Roquetas de Mar y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de seguridad de la información y protección de datos de carácter personal.

Son funciones del Comité de Seguridad de la Información las siguientes:

- Atender las inquietudes de la Alcaldía-Presidencia, Junta de Gobierno Local y/o Concejales Delegados del Ayuntamiento de Roquetas de Mar, así como de los responsables funcionariales de los diferentes departamentos orgánicos estructurales.
- Informar regularmente del estado de la seguridad de la información a la Alcaldía-Presidencia, Junta de Gobierno Local y Corporación Municipal del Ayuntamiento de Roquetas de Mar, así como, de los responsables funcionariales de los diferentes departamentos orgánicos estructurales.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación.
- Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar 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 TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad de la Información es un órgano colegiado dentro del marco jurídico de la gobernanza municipal y la gestión pública, cuándo sea preciso, podrá recabar regularmente de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas:

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

El Responsable de la Seguridad (del ENS) será el secretario del Comité de Seguridad de la Información, y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.

- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El Comité de Seguridad estará compuesto por los siguientes miembros:

- Presidente. Concejal con máxima responsabilidad en materia de Tecnología de la Información y la Comunicación.
- Secretario. Responsable de Seguridad.
- Vocales:
  - Responsable Secretaría General.
  - Responsable Intervención Municipal
  - Responsable Tesorería.
  - Responsable Asesoría Jurídica.
  - Responsable de Recursos Humanos.
  - Responsable del Sistema de la Información.
  - Delegado de Protección de Datos.
  - Administrador de Seguridad.

El Comité de Seguridad de la Información, se reunirá con carácter ordinario, al menos una vez al año, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

5.3 Comité Operativo de Seguridad de la Información

El Comité Operativo de Seguridad de la Información adscrito a la Alcaldía-Presidencia o en quien delegue con competencias en materia de Tecnologías de la Información y Comunicaciones. Como órgano colegiado su misión será coordinar actuaciones destinadas al cumplimiento de los requisitos técnicos y operativos de la normativa de Seguridad de la Información y Protección de Datos Personales, y de la estrategia de Seguridad de la Información aprobada por el Comité de Seguridad de la Información.

El Comité Operativo de Seguridad de la Información se reunirá con carácter ordinario cada tres meses y con carácter extraordinario a propuesta de la Presidencia o de un tercio de los vocales que la integran.

El Comité Operativo de Seguridad de la Información estará compuesto por los siguientes miembros:

- Responsable de Seguridad.

- Responsable del Sistema de Información.
- Administrador de Seguridad.

Son funciones del Comité Operativo de Seguridad de la Información las siguientes:

- Elaborar estudios, análisis previos y propuestas de modificación y actualización de la Política de Seguridad de la Información y del resto de la normativa de seguridad.
- Elaborar o apoyar en la elaboración de Normativas y Procedimientos de Seguridad de la Información.
- Llevar a cabo la aprobación de los Procedimientos e Instrucciones de Seguridad de la Información.
- Analizar el cumplimiento de la Política de Seguridad de la Información y de su desarrollo normativo, realizando propuestas de mejora.
- Aprobar Planes de Mejora de Seguridad para mitigar riesgos.
- Controlar e informar regularmente del estado de la seguridad de la información, así como de las necesidades normativas y procedimentales y de las necesidades de medios materiales y/o personales en materia de seguridad de la información.
- Resolver posibles conflictos operativos causados por la diferenciación de responsabilidades en caso de que se produzca.

5.4 Responsable de Seguridad

Es el responsable de que los servicios y sistemas de información del Ayuntamiento de Roquetas de Mar se mantengan con el nivel aceptable de seguridad atendiendo a los principios de:

a) Confidencialidad: la información asociada a los servicios electrónicos al ciudadano solo debe poder ser conocida por las personas autorizadas para ello.
b) Integridad: la información asociada a los servicios electrónicos al ciudadano no debe ser alterada por personas no autorizadas.
c) Trazabilidad: Capacidad para demostrar que una acción ha sido realizada por un determinado individuo o entidad, asegurando la posibilidad de auditar y verificar dichas acciones.
d) Autenticidad: Verificación de que los sujetos o entidades involucrados en la comunicación o transacción son quienes afirman ser, evitando la suplantación de identidad.
e) Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios relativos a la Administración Electrónica permanecerán disponibles.

Las dos funciones esenciales del Responsable de la Seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización.

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

Además, podrá desempeñar las siguientes funciones:

- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del RD-l 12/2018 y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

En aquellos sistemas de información que, por su complejidad, distribución, separación física de elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones del Responsable de Seguridad, por la autoridad competente en esta materia podrá designar cuantos Responsables de Seguridad Delegados considere necesarios, los cuáles se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencias funcionales directas con él.

De conformidad con lo previsto en punto 3, del artículo 13 del ENS: *El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.*

5.5 Responsable de la Información

La información es la materia prima de la que se nutre la actividad de las entidades del Sector Público y puede tener su origen en la propia entidad, los ciudadanos y en terceras entidades (públicas o privadas).

El Responsable de la Información es habitualmente una persona situada en en la máxima jerarquía técnica del servicio correspondiente del Ayuntamiento de Roquetas de Mar. Esta figura tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

El Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

Son los responsables de establecer los requisitos de la Información en materia de seguridad, y por tanto determinar los niveles de seguridad de la información en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), pudiendo contar con el asesoramiento del Responsable de Seguridad y del Responsable del Sistema de Información.

5.6 Responsable del Servicio

El Responsable del Servicio es habitualmente una persona situada en la máxima jerarquía técnica del servicio correspondiente.

Son los responsables de establecer los requisitos de los Servicios en materia de seguridad, y por tanto determinar los niveles de seguridad de los citados Servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), pudiendo contar con el asesoramiento del Responsable de Seguridad y del Responsable del Sistema de Información.

La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice "se heredan los requisitos"), a los que se suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad.

5.7 Responsabilidades unificadas de Información y Servicio

En el caso del Ayuntamiento de Roquetas de Mar, coinciden en las mismas personas las responsabilidades de la información y del servicio, concretamente en los Responsables de los diferentes Servicios del Ayuntamiento de Roquetas de Mar. Estos Responsables pueden ser requeridos periódicamente por el Responsable de Seguridad para la definición de los requisitos de seguridad de la información y los servicios que manejan. Para facilitar esta interacción, cada Responsable de la Información y Servicio deberá designar una persona

intermediaria que sirva de contacto para al colaboración y coordinación de las funciones del Responsable de Seguridad.

5.8 Responsable del Sistema de Información

El Responsable del Sistema de información tomará decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones, instalaciones y operación.

Tiene las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- 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 de seguridad se integren adecuadamente en el marco general de seguridad.
- Implementar, documentar, monitorizar y verificar las copias de seguridad de los sistemas de información.

El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.

En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, el Ayuntamiento de Roquetas de Mar podrá designar cuantos Responsables del Sistema Delegados considere necesarios. La designación corresponde al Responsable del Sistema, que delega funciones, no responsabilidad.

Los Responsables del Sistema Delegados se harán cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información.

Cada Responsable del Sistema Delegado mantendrá una dependencia funcional directa del Responsable del Sistema, a quien reportarán.

5.9 Administrador de Seguridad

Atendiendo a la estructura organizativa de la entidad, el Administrador de Seguridad (AS) puede depender, debidamente justificado en su nombramiento, del Responsable del Sistema o del Responsable de la Seguridad.

Sus funciones más significativas serían las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

5.10 Los Puntos o Personas de Contacto (POC)

De conformidad con lo previsto en el punto 5, del art, 13 del ENS, en el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos directivos, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio. Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, y formará parte de su área o tendrá comunicación directa con la misma.

5.11 Resolución de conflictos

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.

5.12 Obligaciones del Personal

Todo el personal, interno y externo, del Ayuntamiento de Roquetas de Mar tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad de la Información disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

6 Asesoramiento Especializado en Materia de Seguridad

6.1 Asesoramiento especializado

El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en el Ayuntamiento de Roquetas de Mar con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

6.2 Cooperación entre organismos y otras Administraciones Públicas

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, el Ayuntamiento de Roquetas de Mar mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad.

6.3 Revisión independiente de la Seguridad de la Información

El Comité de Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas en el Ayuntamiento de Roquetas de Mar reflejan adecuadamente sus disposiciones.

7 Protección de Datos de Carácter Personal

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento las políticas, directrices, normativas y procedimientos desarrollados en materia de protección de datos personales, conforme a lo exigido en el 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); así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El tratamiento de datos personales estará marcado por los siguientes documentos del Ayuntamiento de Roquetas de Mar:

- *Manual de Procedimientos Jurídico*. Documento que proporciona diversas cláusulas y procedimientos de naturaleza jurídica con el objetivo de facilitar modelos de cumplimiento a cuanto, con carácter obligatorio, se establece en el RGPD.
- *Política de Privacidad.* Documento en el que se indica cómo se lleva a cabo el tratamiento de datos personales en el Ayuntamiento de Roquetas de Mar, incluyendo información sobre el responsable del tratamiento, los principios de tratamiento de datos personales, finalidad del tratamiento, periodo de conservación de los datos, base legítima del tratamiento, destinatarios de los datos, y ejercicio de derechos por parte del interesado.

Estos documentos serán aprobados por la Junta de Gobierno Local del Ayuntamiento de Roquetas de Mar.

8 Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal del Ayuntamiento de Roquetas de Mar y a todas las actividades de acuerdo con el principio de seguridad integral recogido en el Artículo 6. La seguridad como un proceso integral del Real Decreto 311/2022, de 3 de mayo.

A estos efectos, el Ayuntamiento de Roquetas de Mar, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren. La asistencia a estas sesiones tendrá carácter de obligado cumplimiento para los empleados públicos municipales.

9 Análisis y gestión de riesgos

El Ayuntamiento de Roquetas de Mar asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigente bajo un proceso de mejora continua para orientar las medidas de protección a minimizar los riesgos.

Como metodología base para la realización de los análisis de riesgos se utilizará MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), siendo esta metodología la más recomendable para el sector público nacional. .

Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad, los Responsables de los Sistemas de Información realizarán, con periodicidad al menos anual, análisis de riesgos cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas en caso necesario.

Se realizará un análisis de riesgos:

- Regularmente, una vez al año.
- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

El informe de análisis de riesgos deberá plasmar el nivel de riesgo aceptable definido por el Ayuntamiento de Roquetas de Mar.

En cumplimiento de lo previsto en el art. 41 del ENS, la facultad para efectuar las valoraciones a las que se refiere el artículo 40 del ENS, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados. Con base en las valoraciones señaladas, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos de carácter personal, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, así como la comunicación o acceso no autorizados a dichos datos.

Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad y éste al Comité de Seguridad de la Información.

10 Estructura normativa

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad de la Información.
- Segundo nivel: Normativas de Seguridad de la Información.
- Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

10.1 Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, del Ayuntamiento de Roquetas de Mar, recogido en el presente documento y aprobado mediante Pleno Municipal.

10.2 Segundo Nivel: Normativas de Seguridad de la Información

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será realizada por Junta de Gobierno Local.

10.3 Tercer Nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información

Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos técnicos es del Comité Operativo de Seguridad de la Información.

10.4 Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables en su ámbito.

10.5 Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC (Seguridad de las Tecnologías de la Información y las Comunicaciones), así como las guías CCN-STIC de las series 400, 500 y 600.

Las normativas UNE-ISO/IEC 27001 y/o relacionadas.

Los reglamentos, órdenes, decretos y resto de legislación relativa a la protección de datos personales tanto procedentes de la Unión Europea como del Estado Español.

11 No incremento del gasto público

La aplicación del presente acuerdo no conllevará incremento de gasto público, atendiéndose el funcionamiento del Comité de Seguridad y el resto de Responsables mencionados en el presente documento con los recursos humanos y materiales de que dispone el Ayuntamiento de Roquetas de Mar.

12 Publicación de la política de seguridad

El acuerdo municipal del Ayuntamiento Pleno, previo dictamen por la Comisión Informativa Permanente ordenará su publicación mediante anuncio en el "Boletín Oficial de la Provincia" y, simultáneamente, en la web corporativa del Ayuntamiento de Roquetas de Mar e Intranet de los empleados públicos municipales.

13 Entrada en vigor

La Política de Seguridad que se aprueba en este acuerdo será aplicable a partir del día siguiente al de su publicación en el Boletín Oficial de la Provincia.

El Alcalde del Ayuntamiento de Roquetas de Mar

Ayuntamiento de Roquetas de Mar.