SAG
Societat anònima de gestió
Sagunt

SGSI01 – Política de Seguridad

Política

Información del documento:

Título del documento	SGSI01 – Política de Seguridad.docx
Tipo de documento	Política
Nivel de seguridad	Difusión Publica
Ámbito de difusión	Todos los empleados y colaboradores externos
Responsable del documento	Responsable de Seguridad de la Información

Registro de versiones		
Descripción	Versión	Fecha
Versión inicial del documento.	1.0	03/02/2025
Cambios en el apartado 6	1.1	15/04/2025
Se indica la fecha de entrada en vigor	1.2	01/10/2025
Se alineas las dimensiones del ENS	1.3	26/01/2026
Se ajusta el apartado de la política	1.4	28/01/2026
Se añade gestión EOL de los activos	1.5	17/03/2026
Actualizar		

CONTENIDO

1. INTRODUCCIÓN

SOCIETAT ANONIMA DE GESTIO SAGUNT MITJA PROPI MUNICIPAL S.A. (en adelante, SAG) depende de manera crítica de los sistemas de Tecnologías de la Información y las Comunicaciones (TIC) para el cumplimiento de sus objetivos y la correcta prestación de los servicios que tiene encomendados. En consecuencia, dichos sistemas deben ser gestionados con la debida diligencia, aplicando las medidas necesarias para protegerlos frente a daños accidentales o deliberados que puedan comprometer cualquiera de las cinco dimensiones de la seguridad de la información definidas en el Esquema Nacional de Seguridad: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

El objetivo de la seguridad de la información en SAG es garantizar la calidad, fiabilidad y uso legítimo de la información, así como la prestación continuada de los servicios, mediante un enfoque preventivo, la supervisión permanente de la actividad y la capacidad de reacción rápida y eficaz ante incidentes de seguridad.

Los sistemas TIC deben estar protegidos frente a amenazas en constante evolución que puedan afectar negativamente a la información y a los servicios, ya sea comprometiendo su confidencialidad, alterando su integridad, interrumpiendo su disponibilidad, poniendo en duda su autenticidad o impidiendo la adecuada trazabilidad de las acciones realizadas sobre los sistemas. Para hacer frente a este escenario, SAG debe disponer de una estrategia de seguridad dinámica, capaz de adaptarse a los cambios del entorno tecnológico y de riesgo, garantizando en todo momento la continuidad de los servicios.

A tal efecto, los distintos departamentos deberán aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, realizar un seguimiento continuo de los niveles de prestación de los servicios, identificar y analizar las vulnerabilidades detectadas o notificadas, y mantener una capacidad de respuesta eficaz ante incidentes, asegurando la recuperación de los servicios y la minimización de impactos.

Asimismo, los departamentos deberán garantizar que la seguridad de las TIC forma parte integral de todas las fases del ciclo de vida de los sistemas, desde su concepción y diseño, pasando por su desarrollo o adquisición y su explotación, hasta su retirada de servicio. Los requisitos de seguridad y las necesidades de financiación asociadas deberán identificarse y contemplarse de forma explícita en los procesos de planificación, en las solicitudes de oferta y en los pliegos de contratación de proyectos TIC.

Finalmente, los departamentos deberán estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad, de conformidad con lo establecido en el Artículo 7 del Esquema Nacional de Seguridad, garantizando una gestión de la seguridad basada en el riesgo y orientada a la mejora continua.

2. MISIÓN

SAG tiene como misión la prestación eficiente y sostenible de servicios públicos y privados que contribuyan al desarrollo económico, social, industrial y medioambiental del municipio de Sagunto, garantizando el bienestar de la ciudadanía y promoviendo el interés público.

Su objeto social abarca una amplia gama de actividades orientadas a la mejora y mantenimiento del entorno urbano, incluyendo:

- Recogida y gestión de residuos, incluyendo enseres y la administración del ecoparque.
- Aseo urbano y limpieza de edificios públicos.
- Mantenimiento de jardines, playas y colegios.
- Señalización vial y servicio de grúas.
- Gestión de infraestructuras como el aparcamiento de camiones y la planta de transferencia de residuos.

La SAG se compromete a operar bajo principios de calidad, sostenibilidad e innovación, asegurando la mejora continua en la prestación de sus servicios y el cuidado del medio ambiente.

3. ALCANCE

La presente Política de Seguridad de la Información es de aplicación a los sistemas de información, infraestructuras tecnológicas, aplicaciones, redes, servicios y activos de información que dan soporte a la prestación de los servicios gestionados por SOCIETAT ANONIMA DE GESTIÓ SAGUNT MITJÀ PROPI MUNICIPAL S.A. (SAG) y que se encuentran incluidos en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

En concreto, esta Política aplica a los sistemas de información que soportan los siguientes servicios:

a) Mantenimiento de jardines

b) Limpieza de edificios públicos

c) Limpieza viaria

d) Recogida de residuos

e) Ecoparque

f) Señalización

g) Servicio de grúa municipal

h) Limpieza de playas

i) Aparcamiento de camiones

j) Mantenimiento de colegios

Asimismo, el alcance incluye los sistemas corporativos transversales necesarios para la gestión, planificación, control y soporte de los servicios anteriores, tales como los sistemas de gestión administrativa, económica, de recursos humanos, contratación, gestión documental, comunicaciones, soporte TIC y seguridad de la información.

Forman igualmente parte del alcance las instalaciones, dependencias, centros de trabajo y ubicaciones físicas, propias o de terceros, en las que se ubiquen, alojen o desde las que se operen los sistemas de información, infraestructuras tecnológicas y activos de información que dan soporte a los servicios anteriormente descritos, incluyendo los elementos necesarios para su funcionamiento, mantenimiento y protección física.

Esta Política será de obligado cumplimiento para todo el personal propio y externo, proveedores y terceros que, en el ejercicio de sus funciones, tengan acceso a los sistemas de información o a la información gestionada por SAG.

Quedan igualmente incluidos en el alcance los sistemas de información que soportan el ejercicio de derechos y obligaciones por medios electrónicos, el acceso a la información y, en su caso, los procedimientos administrativos y servicios electrónicos prestados por la entidad.

El alcance definido será revisado y actualizado cuando se produzcan cambios significativos en los servicios prestados, en los sistemas de información o en la estructura organizativa de SAG.

4. MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias de SAG 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 constituida por la siguiente legislación:

- 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 (enlace a https://www.boe.es/doue/2014/257/L00073-00114.pdf), 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 16/1985, de 25 de junio, del Patrimonio Histórico Español (archivo).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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 (Vigente en los apartados señalados 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 (según plazos entrada en vigor de Disposición de esta Ley).

El mantenimiento del marco normativo será responsabilidad de SAG y se mantendrá en un Anexo a este documento (SGSI06 - Legislación Aplicable). Incluido 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 el Real Decreto

Así mismo, SAG también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

5. CUMPLIMIENTO DE ÁRTICULOS

SAG para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, que recogen 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.

Seguridad como un proceso integral y mínimo privilegio

La seguridad constituye un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad a SAG 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 que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán y configurarán otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

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

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.

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.

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 continua del proceso de seguridad

La vigilancia continua por parte de SOCIEDAD ANONIMA DE GESTION SAGUNTO MITJA PROPI MUNICIPAL S.A 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.

La organización mantendrá un inventario actualizado de activos, donde gestionará el ciclo de vida y fin de soporte de los activos tecnológicos, incluyendo su adquisición, mantenimiento y retirada. Se evitará el uso de sistemas fuera de soporte del fabricante (EOL y EOS), o en su defecto, se gestionará el riesgo asociado mediante análisis de riesgos, medidas compensatorias y aprobación expresa por la Dirección.

Gestión de personal y profesionalidad

Todo el persona, propio o ajeno relacionado con los sistemas de información de SAG 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.

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, 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

SAG dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el artículo 33, 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.

Existencia de líneas de defensa y prevención ante otros sistemas interconectados

SAG 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 de SOCIEDAD ANONIMA DE GESTION SAGUNTO MITJA PROPI MUNICIPAL S.A 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

SAG 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.

Autorización y control de los accesos

SAG ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones

SAG 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.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos, SAG tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

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

SAG 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.

Registros de actividad y detección de código dañino

SAG 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, o laborales, 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 Sector público, 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, SOCIETAT ANONIMA DE GESTIO SAGUNT MITJA PROPI MUNICIPAL S.A 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 de relevancia, 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

SAG tendrá en cuenta que la utilización de infraestructuras y servicios comunes, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.

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

SAG tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para Sector público local que sean de aplicación.

6. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad de la información en SOCIETAT ANONIMA DE GESTIO SAGUNT MITJA PROPI MUNICIPAL S.A. (SAG) se estructura de acuerdo con los principios del Esquema Nacional de Seguridad (ENS) y las directrices establecidas por la Guía CCN-STIC 801.

SAG ha definido y formalizado los distintos roles de seguridad exigidos por el ENS (responsable de la Información, del Servicio, de Seguridad, del Sistema y delegado de Protección de Datos), así como la constitución de un Comité de Seguridad de la Información como órgano colegiado encargado de coordinar y supervisar las acciones en esta materia.

Con el fin de facilitar la gestión y garantizar la trazabilidad y actualización de esta estructura organizativa, la composición del Comité de Seguridad de la Información, sus funciones específicas, y las responsabilidades asociadas a cada rol se encuentran descritas detalladamente en el documento anexo:

"Documento Anexo: Constitución del Comité de Seguridad de la Información y Roles ENS"

Este anexo forma parte integrante de la presente Política de Seguridad y será actualizado cada vez que se produzcan cambios en los integrantes, funciones o periodicidad de las reuniones.

7. DATOS DE CARÁCTER PERSONAL

SOCIEAT ANONIMA DE GESTIO SAGUNT MITJA PROPI MUNICIPAL S.A 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.

SOCIETAT ANONIMA DE GESTIO SAGUNT MITJA PROPI MUNICIPAL S.A realiza tratamientos en los que hace uso de datos de carácter personal sometidos a lo dispuesto por 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 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Las políticas de seguridad aplicables a los tratamientos se rigen por las medidas de seguridad implantadas de acuerdo con el Anexo II (Medidas de seguridad) del Real Decreto del Esquema Nacional de Seguridad.

Además, se dispone de un RAT (Registro de Actividades del Tratamiento) donde se indexan los distintos tratamientos de datos afectados por la normativa.

Todos los sistemas de información de SOCIETAT ANONIMA DE GESTIO SAGUNT MITJA PROPI MUNICIPAL S.A se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal. El delegado de protección de Datos del Grupo velará por el cumplimiento del RGPD y de la LOPDGDD.

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 del 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 esta, para su aprobación por parte de la Dirección general.

9. TERCERAS PARTES

Cuando el preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. SAG definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el SOCIETAT ANONIMA DE GESTIO SAGUNT MITJA PROPI MUNICIPAL S.A lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando SAG utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las

obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

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

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto 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.

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. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.

10. ENTRADA EN VIGOR

La política inicial entró en vigor el 1 de octubre de 2025

El presente texto entrará en vigor en la fecha referenciada a la última versión de este documento.

Esta Política de Seguridad de la Información será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva versión de la Política.