

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO DE GESTAGUA

SGSI ENS - MSG-CAP.15 - POLÍTICA DE SEGURIDAD - REV.01

Como muestra del compromiso adquirido con la seguridad de la información, la Dirección de GESTAGUA adquiere de manera pública los siguientes compromisos:

- Realizar un enfoque a la mejora continua en las áreas y actividades que se encuentran bajo el alcance del SGSI de GESTAGUA y en todos los aspectos relativos a la seguridad de la información y su gestión.
- Definir y asignar las Responsabilidades correspondientes, generando la estructura organizativa necesaria para una correcta gestión, operación y supervisión de la seguridad en el seno de la organización.
- Buscar proactivamente la salvaguarda de la seguridad de la información en sus dimensiones de Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.
- Fomentar una cultura organizacional basada en el cumplimiento normativo y la sensibilización en seguridad de la información.
- Cumplir con los requisitos establecidos en la norma **ISO/IEC 27001:2022** y en el **Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad**.

Gestión y Técnicas del Agua, S.A. (en adelante, "GESTAGUA", la "Compañía" o la "Organización"), tiene como actividad principal la prestación de servicios vinculados a la gestión integral del ciclo del agua para el sector público, incluyendo la captación, tratamiento, distribución y depuración del recurso hídrico, operando en el sector de los servicios medioambientales y de gestión del agua.

GESTAGUA siendo consciente de la relevancia de la seguridad de la información de los datos dentro de su organización y con el fin de garantizar que toda la actividad de GESTAGUA se realiza bajo principios de diligencia debida, proactividad y compromiso con las buenas prácticas existentes, la Dirección ha acordado la implantación de un **Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los requisitos establecidos en los estándares ISO/IEC 27001:2022 y RD 311/2022 (ENS)**. En este sentido, la implementación del Sistema de Gestión abarca el alcance de los procesos relacionados con la gestión integral del ciclo de agua realizada por GESTAGUA.

Tanto el SGSI, como esta Política y cualquier otra normativa de desarrollo serán de obligado cumplimiento para todos los profesionales de GESTAGUA, incluyendo colaboradores, partners y cualquier tercero que opere bajo el control o la supervisión de GESTAGUA en la prestación de sus servicios. La no observación de lo establecido en estos documentos conllevará diversas consecuencias para todas las partes involucradas, incluyendo la ejecución del procedimiento sancionador para el personal interno o la extinción de los acuerdos alcanzados entre GESTAGUA y los terceros con los que colabore. GESTAGUA ha establecido procedimientos específicos para que todo el personal conozca, comprenda y cumpla con la Política del SGSI y toda su normativa de desarrollo.

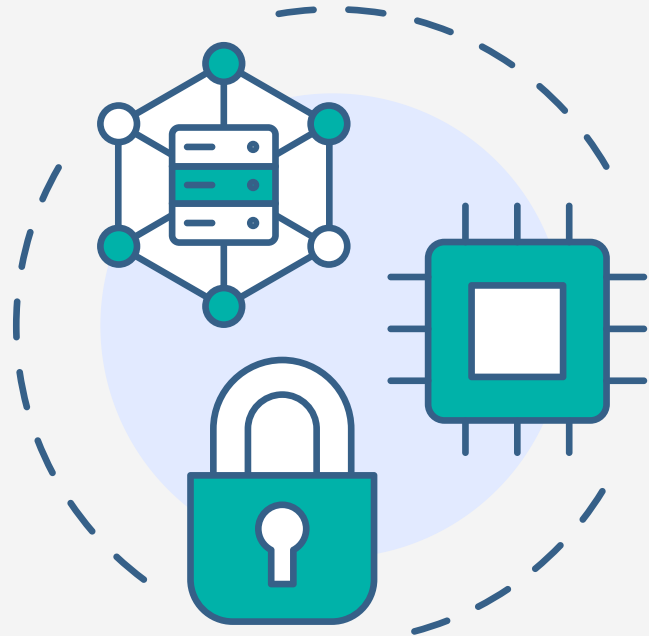


En lo relativo a, en la gestión diaria de la seguridad y la operativa de GESTAGUA, se procederá siempre en atención a los siguientes principios básicos y requisitos mínimos de seguridad:

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.
- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Toda la documentación, registros y directrices documentadas del SGSI se gestionan conforme a los procedimientos documentados que GESTAGUA ha desarrollado teniendo en cuenta los estándares nacionales e internacionales que aplique en cada caso, siendo en este caso la norma principal el procedimiento de la gestión documental de GESTAGUA, **el manual de procedimientos S61.1 – Gestión de la documentación**.

GESTAGUA ha dotado a la Organización de los recursos necesarios para la implementación, desarrollo, mantenimiento y seguimiento del SGSI. A tal efecto, cuenta con un Comité de Seguridad de la Información y un Delegado de Protección de Datos (DPD).



Funciones del Comité de Seguridad de la Información de GESTAGUA:

El Comité de Seguridad de la Información de GESTAGUA:

- Coordinar la implantación, seguimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI), conforme a la norma ISO/IEC 27001:2022.
- Evaluar y aprobar las medidas de seguridad propuestas por las distintas áreas.
- Canalizar las decisiones estratégicas en materia de seguridad de la información hacia la Dirección.
- Asegurar la integración de la seguridad de la información con los procesos y estructuras de gestión de la organización.

Colaborar de forma estrecha con el Delegado de Protección de Datos (DPD), en cumplimiento del REGLAMENTO (UE) 2016/679 de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), así como con otros comités internos con competencias relacionadas.

Integrantes del Comité

El Comité de Seguridad de la Información: se encuentra compuesto por los siguientes responsables , incluyendo a la Dirección Técnica y con la excepción del DPD.

Este Comité tiene como principales funciones:

- Coordinar la implantación, seguimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI), conforme a la norma ISO/IEC 27001:2022.
- Evaluar y aprobar las medidas de seguridad propuestas por las distintas áreas.
- Canalizar las decisiones estratégicas en materia de seguridad de la información hacia la Dirección.
- Asegurar la integración de la seguridad de la información con los procesos y estructuras de gestión de la organización.
- Colaborar de forma estrecha con el Delegado de Protección de Datos (DPD), en cumplimiento del REGLAMENTO (UE) 2016/679 de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), así como con otros comités internos con competencias relacionadas.
- Intervenir como órgano de decisión en caso de conflicto entre los diferentes Responsables, pudiendo decidir el escalado de una decisión a la Dirección en caso de considerarlo necesario.

Responsable de definir, implantar y supervisar las medidas de seguridad. Garantiza la alineación del SGSI con los objetivos organizacionales. Debe coordinarse con el Responsable del Servicio y del Sistema, así como con el DPD.

**RESPONSABLE DE
SEGURIDAD DE LA
INFORMACIÓN Y
GESTIÓN**

**Director del
Departamento de
Tecnología de la
Información (IT),**

Tiene a su cargo el funcionamiento seguro del sistema, incluyendo su arquitectura, componentes y servicios tecnológicos. Debe implementar las medidas de seguridad técnicas y operativas que aseguren la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de los activos del sistema.

**RESPONSABLE
DEL SISTEMA DE
INFORMACIÓN**

**Responsable
del Área de
Sistemas**

Responsable de la gestión, clasificación y protección de la información tratada. Define los requisitos de seguridad de la información de acuerdo con su nivel de sensibilidad, y debe asegurar el cumplimiento de las políticas y procedimientos que garanticen su confidencialidad, integridad y disponibilidad.

**RESPONSABLE DE
LA INFORMACIÓN Y
DE LOS SERVICIOS**

**Comité de
Seguridad**

Responsable de la gestión, clasificación y protección de la información tratada. Define los requisitos de seguridad de la información de acuerdo con su nivel de sensibilidad, y debe asegurar el cumplimiento de las políticas y procedimientos que garanticen su confidencialidad, integridad y disponibilidad.

**RESPONSABLE DEL
SISTEMA DE GESTIÓN
DE SEGURIDAD
DE LA INFORMACIÓN:**

**Responsable del
Departamento de
Calidad**

Ejercerá también funciones como Compliance Officer, asumiendo la responsabilidad de supervisar el cumplimiento normativo en materia de protección de datos personales, debiendo colaborar con el Responsable de la Seguridad en aspectos relacionados con datos personales.

**DELEGADO DE
PROTECCIÓN DE
DATOS
(DPD)**

**Compliance
Officer**

Reglamento General de Protección de Datos (RGPD)

En materia de Protección de Datos, GESTAGUA es consciente de que el desarrollo de sus actividades puede implicar el **tratamiento de datos personales** en diversos contextos, como la gestión administrativa, financiera, contractual, de personal, o en el ámbito de la atención a clientes y proveedores.

Por ello, se han identificado determinadas situaciones que requieren una especial atención, como el adecuado control de accesos, la correcta conservación y supresión de la información, la atención a los derechos de las personas interesadas, y la garantía de confidencialidad e integridad de los datos.

GESTAGUA trabaja activamente en la implantación de medidas organizativas y técnicas que aseguren un tratamiento diligente, lícito y transparente, en línea con los principios establecidos por el **Reglamento General de Protección de Datos (RGPD)**.

Los roles correspondientes a los Responsables de Seguridad serán designados formalmente por la Dirección de GESTAGUA. Las personas designadas para estas funciones permanecerán en su cargo hasta que abandonen la organización o se decida su sustitución, no siendo necesario realizar una renovación explícita.



Legislación vigente

GESTAGUA se compromete también a cumplir toda legislación vigente aplicable en materia de seguridad de la información y protección de datos personales. En este sentido, la principal normativa aplicable a la organización en materia de seguridad de la información dentro del alcance establecido es la siguiente:

GESTAGUA se compromete también a cumplir toda legislación vigente aplicable en materia de seguridad de la información y protección de datos personales. En este sentido, la principal normativa aplicable a la organización en materia de seguridad de la información dentro del alcance establecido es la siguiente:

- **Real Decreto 311/2022, de 3 de mayo**, por el que se regula el Esquema Nacional de Seguridad
- **Ley 39/2015, de 1 de octubre**, del Procedimiento Administrativo Común de las Administraciones.
- **Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014**, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- **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) (Texto pertinente a efectos del EEE)
- **Ley Orgánica 3/2018, de 5 de diciembre**, de Protección de Datos Personales y garantía de los derechos digitales.
- **Ley Orgánica 7/2021, de 26 de mayo**, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

La presente Política ha sido aprobada formalmente por la Dirección de GESTAGUA.

Fdo. El Consejo de Administración.