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

SGSI ENS - MSG-CAP.15 – POLÍTICA DE SEGURIDAD – REV.02

Agosto 2025

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.

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.
- Hacer patente el compromiso de GESTAGUA con la seguridad de la información mediante su apoyo al Comité de Seguridad dotándole de los medios adecuados, incluidos el personal, los recursos financieros, los procesos, las herramientas, las tecnologías y facultades necesarias para la realización de sus funciones y la aplicación de esta Política de Seguridad de la Información.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de GESTAGUA respecto a la seguridad de la información.
- Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.
- Crear y promover de manera continua una "cultura de seguridad" tanto internamente, a todo el personal, como externamente a los clientes y proveedores que permita asegurar la eficiencia y eficacia de los controles implantados y aumente la confianza de nuestros clientes.
- 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.

Riesgos identificados

Los riesgos identificados se documentan en el Análisis de Riesgos de Seguridad de la Información Valoración de activos riesgos amenazas y **PTR (I-R11.2.02**).

Para aquellos riesgos que superan los umbrales aceptables, se elabora un **Plan de Tratamiento de Riesgos,** que incluye acciones concretas y medibles y su efectividad se evaluará a través de los resultados del siguiente Análisis de Riesgos que se realice.

El análisis de riesgos contempla las siguientes etapas:

1. Identificación y valoración de activos: Se clasifican según su criticidad, sensibilidad o valor estratégico y se establecen las relaciones entre los mismos.
2. Identificación de amenazas: Se usan como referencia los catálogos de MAGERIT v3, aunque se permite incluir amenazas específicas según el contexto de la organización.
3. Análisis de riesgos: Se cruzan activos y amenazas, estimando la probabilidad de ocurrencia y el impacto en cada dimensión de seguridad.
4. Cálculo del riesgo inherente: Se determina el riesgo antes de aplicar medidas de control.
5. Identificación y asignación de salvaguardas: Se vinculan controles existentes o nuevos a cada riesgo identificado.
6. Cálculo del riesgo residual y repercutido: Se calcula el riesgo remanente tras aplicar controles y el riesgo proyectado sobre activos dependientes.
7. Establecimiento de umbrales de riesgo: Definidos por el Comité de Seguridad como parte de evaluación de la eficacia del sistema y de la mejora continua, siendo un punto de análisis en el proceso E23.1 REVISIÓN POR LA DIRECCIÓN como mejora continua del sistema.

#missionwater

Principios rectores

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 rectores:

- **Seguridad como proceso integral:** la gestión de la seguridad se ha concebido como un proceso que aplica y es tenido en consideración en todos los procesos comprendidos dentro del alcance del SGSI de GESTAGUA, así como en aquellos procesos adicionales que, sin estar comprendidos dentro del alcance, pueden llegar a afectar negativamente en la seguridad de estos.
- **Gestión de la seguridad basada en los riesgos:** la implantación de los procedimientos y medidas de seguridad se plantean siempre en base a los resultados obtenidos a través del proceso establecido de gestión de riesgos de seguridad de la información, priorizando el tratamiento de aquellos riesgos considerados como más relevantes.
- **Prevención, detección, respuesta y conservación:** la gestión de los riesgos y los incidentes de seguridad se ha planteado desde el punto de vista de la gestión del ciclo de vida completo de ambos aspectos de la seguridad, de forma que se dé adecuado tratamiento a todos estos aspectos.
- **Existencia de líneas de defensa:** la aplicación práctica de la seguridad se ha diseñado, de forma que existan diversas medidas de seguridad que den respuesta a las diferentes situaciones de riesgo que puedan llegar a producirse en cada caso, especialmente en lo relativo a los riesgos con un mayor impacto para los sistemas y la información de GESTAGUA.
- **Vigilancia continua y reevaluación periódica:** tanto el sistema de gestión como las medidas de seguridad se controlan desde el SGSI de GESTAGUA, de forma que sean regularmente sometidas a evaluación y mejora.
- **Seguridad por defecto y desde el diseño**: el despliegue de los sistemas se realiza de forma que se dé respuesta a estos dos principios, es decir, que las funcionalidades que proporcionen el sistema por defecto sean inherentemente seguras, que una minoración de la seguridad requiera de una acción consciente del usuario y que los sistemas se planteen siempre teniendo en cuenta los diferentes aspectos de la seguridad que sean relevantes para estos en cada caso.
- **Diferenciación de responsabilidades:** los roles y responsabilidades definidos dentro del SGSI de GESTAGUA se han definido de forma que no se den situaciones de riesgo vinculadas a un exceso de autorización de alguno de estos, definiendo claramente las funciones que cada uno de los roles debe realizar.
- **Organización e implantación del proceso de seguridad:** la gestión de la seguridad de la información soportada en los sistemas informáticos de GESTAGUA tiene como finalidad gestionar la seguridad de los servicios, activos y recursos IT de GESTAGUA, garantizando que las medidas de seguridad aplicadas en torno a dichos servicios y recursos satisfacen el cumplimiento de los requisitos legales vigentes, así como asegurando la accesibilidad, la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de la información asociada a los procesos de la empresa
- **Análisis y gestión de los riesgos:** En materia de gestión de riesgos, GESTAGUA ha definido un procedimiento estructurado para identificar, evaluar y tratar los riesgos que afectan a la seguridad de la información. El procedimiento está basado en la metodología MAGERIT v3, incorporando las cinco dimensiones de seguridad requeridas por el RD 311/2022.
- **Gestión de personal:** se realiza una supervisión activa de la actuación del personal dentro del alcance del SGSI de GESTAGUA, incluyendo la adecuación de su actuación profesional, así como la garantía de la capacitación de estos.
- **Profesionalidad:** El personal que asume funciones clave en el SGSI cuenta con la formación, concienciación, experiencia y competencia necesarias.
- **Autorización y control de los accesos:** En cuanto al control de accesos y la gestión de identidades, GESTAGUA se enfoca en garantizar la autenticación segura y la asignación adecuada de privilegios de acceso a los sistemas, redes y recursos de la organización. Los equipos informáticos de los usuarios deben cumplir con requisitos de autenticación, permitiendo la identificación única y controlando que cada usuario realice solo las tareas autorizadas. Las responsabilidades del Comité de Seguridad incluyen controlar el acceso físico y lógico a la información, establecer procedimientos de autenticación, monitorizar la actividad de los administradores y proteger las redes inalámbricas. En cuanto a la administración de derechos de acceso, GESTAGUA se asegura de que cada usuario tenga acceso solo a la información necesaria para el desarrollo de su trabajo y regula la asignación de estos derechos mediante procedimientos establecidos (principio del mínimo privilegio).
- **Protección de las instalaciones:** GESTAGUA se encargará de implementar y garantizar la efectividad de los mecanismos de seguridad física y control de acceso en sus instalaciones (sede y CPD), protegiendo el perímetro de todas sus sedes. Además, controlará las amenazas físicas internas y externas, así como las condiciones medioambientales, buscando minimizar el impacto del cambio climático. Las áreas de procesamiento o almacenamiento de información sensible y las que contienen equipos de soporte a los sistemas de información se considerarán de acceso restringido. Cualquier solicitud de acceso a los centros de cableado debe ser aprobada por el Comité de Seguridad de la Información, y los visitantes deben estar acompañados por un trabajador del Departamento de Tecnologías de la Información, con sus accesos registrados. GESTAGUA para evitar la pérdida, robo o exposición al peligro de sus recursos tecnológicos que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos de seguridad de la información. El sistema de gestión de seguridad física se rige según lo establecido en el procedimiento S43.3 de Seguridad física y del entorno.
- **Adquisición de productos de seguridad y contratación de servicios de seguridad:** GESTAGUA velará porque los elementos que formen parte integral del sistema de información cumplan con los requisitos de seguridad, buenas prácticas en el desarrollo seguro de software y protección de los datos de prueba entregados a los desarrolladores y cuenten con las certificaciones de seguridad y de producto necesarias para determinar que son adecuados. También se asegurará de que se apliquen metodologías adecuadas para realizar pruebas de aceptación y seguridad en el software desarrollado por terceros, desde las fases iniciales del proyecto, incluyendo su planificación y diseño. Además, se llevará a cabo una revisión periódica de los objetivos y medidas de seguridad. Todo ello conforme a la IT-S43.5.02 de Instrucción de adquisición, desarrollo y mantenimiento.
- **Mínimo privilegio:** GESTAGUA ha desplegado y configurado sus sistemas de información de manera que los usuarios y entidades del sistema que tienen acceso puedan hacer
- **Integridad y actualización del sistema:** Los sistemas informáticos están sujetos a políticas de mantenimiento correctivo y preventivo, aplicación de parches de seguridad y pruebas periódicas.
- **Protección de la información almacenada y en tránsito:** GESTAGUA busca activamente proteger la información propia de GESTAGUA, la información de terceros tratada por GESTAGUA, así como la información que terceros tratan de GESTAGUA, reconociendo la especial relevancia del factor humano para el cumplimiento de los objetivos de seguridad de la información. Se aplican medidas de cifrado y control de acceso a la información crítica tanto en almacenamiento como en tránsito, con uso de tecnologías criptográficas y procedimientos de clasificación de la información. También se han implantado los registros de entrada/salida necesarios para un correcto control de los soportes.
- **Prevención ante otros sistemas de información interconectados:** Se establece el control de interconexiones con sistemas externos mediante segmentación de red, firewall, monitorización y aplicación de normas de seguridad homogéneas entre sistemas conectados, así como la supervisión y evaluación de las interconexiones de forma previa a su aplicación:
- **Registro de la actividad y detección de código dañino:** Se mantienen registros de actividad mediante logs de auditoría que permiten la trazabilidad y que son supervisados de forma automatizada y manual, según el caso. Adicionalmente, se implementan medidas de detección y protección contra software malicioso (antivirus, IDS, escaneo de vulnerabilidades).
- **Incidentes de seguridad:** a este respecto, GESTAGUA fomentará entre todos sus miembros y terceros el reporte de incidentes relacionados con la seguridad de la información de cara a realizar una correcta gestión de estos incidentes, investigándolos, evaluándolos y tomando decisiones para solucionarlos. Además, tomará medidas para evitar su repetición y escalará los incidentes según su criticidad, siguiendo los procedimientos establecidos. El sistema de gestión de incidentes se regula conforme al procedimiento S43.8 de Gestión de incidentes de seguridad.
- **Continuidad de la actividad:** GESTAGUA se compromete a proporcionar los recursos necesarios para garantizar una respuesta eficaz ante contingencias, incidentes o eventos que puedan afectar la continuidad de sus operaciones. Esto incluye restablecer las operaciones con el menor coste posible y asegurando un nivel adecuado de seguridad de la información durante la interrupción. La organización también mantendrá canales de comunicación adecuados con su personal y terceros para notificar sobre incidentes o eventos relacionados con la seguridad de la información.
- **Mejora continua del proceso de seguridad:** GESTAGUA a través del Comité de Seguridad de la Información, revisará periódicamente la aparición de vulnerabilidades técnicas y amenazas emergentes sobre los activos de información o recursos tecnológicos que soporten procesos de información, por medio de la realización periódica de pruebas de vulnerabilidades y alertas de fuentes oficiales, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. El SGSI se revisa al menos anualmente, o cuando ocurran cambios significativos. Se ejecutan auditorías internas, revisiones por la dirección y evaluación continua del cumplimiento legal y contractual, buscando una mejora continua del nivel de seguridad.

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)**.

En este sentido, GESTAGUA lleva a cabo una actuación proactiva desde un enfoque de prevención y minimización de riesgos para garantizar la seguridad y privacidad de los datos personales tratados.

Para ello, el DPD y el Responsable de Seguridad trabajan de manera coordinada garantizando la seguridad y el cumplimiento de la normativa aplicable en la materia.

Por otro lado, 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.

gestagua

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:

- **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.
- **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones.
- **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público.
- **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 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.
- **Reglamento (UE) Nº 910/2014** del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, modificado en lo que respecta al establecimiento del marco europeo de identidad digital por el Reglamento (UE) Nº 1183/2024, de 11 de abril de 2024,(Reglamento eIDAS).
- **Directiva Nº (UE) 2022/2555** del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. (Directiva NIS2)
- **Reglamento de Ejecución (UE) 2024/2690** de la Comisión, de 17.10.2024, por el que se establecen disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas de gestión de riesgos en materia de ciberseguridad.
- **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.
- **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.
- **Real Decreto-ley 14/2019,** de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- **Real Decreto-ley 13/2012** de 30 de marzo, ley de cookies.
- **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.
- **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 9/2014**, 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).
- **Real Decreto Legislativo 2/2015**, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- **Prevención de Riesgos Laborales Ley 31/1995** de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- **Ley 10/2021**, de 9 de julio, de trabajo a distancia.
- **Real Decreto Legislativo 1/2001** – Texto refundido de la Ley de Aguas
- **Real Decreto 3/2023** – Criterios técnico-sanitarios del agua de consumo
- **Orden TED/1191/2024** – Control electrónico de volúmenes de agua
- **Reglamento del Dominio Público Hidráulico** (RD 849/1986)

Funciones del Comité de Seguridad de la Información de GESTAGUA:

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).

- 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.
- Establecer y acordar los criterios de tolerancia (aceptabilidad) del riesgo.
- Definir e implementar un procedimiento de evaluación de riesgos y selección de estrategias de tratamiento.
- Analizar la información aportada por el análisis de riesgos.
- Definir y aprobar el plan de tratamientos del riesgo, garantizando que se proveen de los recursos (humanos y materiales) necesarios para su ejecución.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- 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 y sus Roles

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

Velará por el cumplimiento de los requisitos del SGSI, la gestión documental y la mejora continua del sistema. Coordina y dinamiza la mejora del SGSI, elabora políticas y planes, y verifica su aplicación.

RESPONSABLE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:

Responsable del Departamento de Calidad

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.
- o Asegurar la integración de la seguridad de la información con los procesos y estructuras de gestión de la organización.
- o 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.
- o 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.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Compuesto por los Responsable anteriormente mencionados, con la excepción del DPD.

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.
El Delegado de protección de datos personales deberá ser invitado a las sesiones del Comité de Seguridad de la Información en aquellos casos en que los temas a tratar estén relacionados con la privacidad y la protección de los datos personales.

DELEGADO DE PROTECCIÓN DE DATOS (DPD)

Compliance Officer

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

El cumplimiento de los objetivos marcados en esta Política se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad.

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información proponiendo en caso de que sea necesario mejoras de esta, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

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

Fdo. El Consejo de Administración.