



POLÍTICA SEGURIDAD DE LA INFORMACIÓN

1. OBJETO Y ÁMBITO DE APLICACIÓN	1
2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	1
<i>a. El marco regulatorio en el que desarrollamos nuestras actividades.....</i>	3
<i>b. Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación....</i>	4
<i>c. La estructura y composición del comité para la gestión y coordinación de la seguridad.....</i>	5
<i>d. Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.....</i>	6
<i>e. Los riesgos que se derivan del tratamiento de los datos personales.....</i>	6
3. REVISIÓN	6
4. OBJETIVOS Y METAS	7

1. OBJETO Y ÁMBITO DE APLICACIÓN

Este documento describe la política de seguridad de la información seguida por SAGITAL Se aplica a todos los sistemas de SAGITAL para las siguientes actividades desarrolladas:

- Servicios de limpieza
- Servicios de auxiliares

2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En SAGITAL estamos comprometidos con la excelencia en cada aspecto de nuestro trabajo. Nuestra dedicación a la innovación, la calidad y la atención al cliente nos distingue como un socio confiable en materia de seguridad. Por este motivo adquirimos los siguientes compromisos:

- La voluntad permanente en materia de Gestión de la Seguridad de la Información se pondrá de manifiesto a través de programas de formación y sensibilización que fomenten la gestión participativa en esos ámbitos, posibilitando que las habilidades del personal sean utilizadas para la mejora continua del proceso productivo.
- Cumplir con la legislación de aplicación, así como otros requisitos suscritos con nuestros clientes, incluidos los requisitos de Seguridad de la Información.
- Cumplir con los requisitos del Sistema de Gestión de la Seguridad de la Información, así como establecer objetivos con el fin de asegurar una mejora continua



- Asegurar la continuidad del negocio desarrollando planes de continuidad conforme a metodologías reconocidas.
- Realizar periódicamente un análisis de riesgos basado en métodos reconocidos, que nos permitan establecer el nivel de seguridad de la información y minimizar los riesgos mediante el desarrollo de políticas específicas, soluciones técnicas y acuerdos contractuales con organizaciones especializadas.
- El personal de SAGITAL desarrollará su trabajo orientado a la consecución de los objetivos marcados y de acuerdo, en todo momento, con los requisitos legales.
- La Dirección de SAGITAL adquiere, además, el compromiso de proporcionar todos los medios materiales y humanos necesarios para llevar a buen término la Política de la organización y declara de obligado cumplimiento las exigencias contenidas en la documentación que constituye el Sistema de Gestión de la Información.

Esta política de seguridad de la información se ha desarrollado hasta completar un sistema de gestión que cumple con los requisitos establecidos en el Esquema Nacional de Seguridad, y que incluye los siguientes apartados:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos de seguridad.
- h) Mínimo privilegio.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de la actividad y detección de código dañino.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- o) Mejora continua del proceso de seguridad.



a. El marco regulatorio en el que desarrollamos nuestras actividades

SAGITAL desarrolla su actividad en un marco regulatorio marcado por el cumplimiento de los requisitos establecidos en materia de protección de datos, propiedad intelectual y seguridad privada.

En el desarrollo de nuestras actividades, estamos comprometidos con el cumplimiento de los requisitos legales establecidos en:

- Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 5/2014, de 4 de abril, de Seguridad Privada.



b. Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

La información comercial y el saber hacer de las personas son factores decisivos para la competitividad de SAGITAL, y constituyen activos esenciales para el crecimiento y desarrollo de nuestra organización. Por este motivo, se han establecido los siguientes roles de seguridad:

1. Director General Corporativo. Forma parte del Comité de Seguridad de la información y es el último responsable de las decisiones adoptadas por el mismo.

2. Comité de Seguridad de información. Es el órgano encargado de determinar los requisitos de seguridad de la información tratada, aprobando los niveles de seguridad de la información. Entre sus funciones se incluye la aprobación de esta política de seguridad.

3. Responsable del servicio. Al frente de cada servicio ofrecido por SAGITAL, se ha designado un responsable, como máximo representante de los servicios ofrecidos por SAGITAL.

Valora las consecuencias de un impacto negativo sobre la seguridad de los servicios. Esta valoración se efectúa atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

4. Responsable de seguridad. Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.

Participa en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones seleccionando, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que 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 su juicio.

Las medidas del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas a juicio del Responsable de Seguridad de la información, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

Es el responsable de aprobar la declaración de aplicabilidad que incluya las medidas del Anexo II del Esquema Nacional de Seguridad.



Es el responsable de analizar y determinar las medidas compensatorias de forma justificada mediante su aprobación formal.

Es el responsable de analizar y supervisar los supuestos concretos de utilización de las infraestructuras y servicios comunes de la organización.

Es el responsable de analizar los informes de auditoría, y encargarse de que se adopten las medidas correctivas adecuadas.

5. Responsable de cada sistema de información. Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.

6. Delegado de protección de datos. Es la persona encargada de determinar los fines y los medios del tratamiento de la información que contengan datos de carácter personal, y se asegura de que se cumplen los requisitos establecidos en el RGPD y la LOPD.

Estos roles son desempeñados por los miembros de la organización designados por el Comité de Seguridad sin una duración determinada hasta que decida su renovación.

En el caso de que durante la realización de alguna actividad se requiriese su coordinación o mediación en la resolución de un conflicto, éste será elevado al Comité de Seguridad para su resolución.

Para los demás puestos de trabajo se han establecido sus funciones y responsabilidades en sus perfiles de puesto de trabajo.

c. La estructura y composición del comité para la gestión y coordinación de la seguridad.

El Comité de Seguridad de la Información se encuentra compuesto por:

- Director General Corporativo.
- Responsable de Seguridad.

El Comité de Seguridad realiza las funciones de responsable de la información, coordinación de las actividades desarrolladas por los cargos nombrados para garantizar la seguridad y actúa como máximo órgano de decisión con los otros miembros de la organización.



d. Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso

La documentación del sistema de gestión está estructurada de forma piramidal, en cuya parte superior se encuentra esta política.

Un Manual, que describe cómo se da cumplimiento a los diferentes puntos del Esquema Nacional de Seguridad y que referencia a los documentos que desarrollan cada apartado.

Instrucciones Técnicas de Seguridad, que describen las políticas de seguridad aplicadas a los sistemas de la organización.

Por último, los registros que sirven como evidencia para demostrar el cumplimiento de los requisitos establecidos en el Esquema Nacional de Seguridad.

Los documentos se encuentran compartidos con los miembros pertinentes de la organización a través de las carpetas de red a las que pueden acceder en modo solo lectura y que administra el responsable de sistemas de seguridad.

e. Los riesgos que se derivan del tratamiento de los datos personales

Durante el desarrollo de su actividad, SAGITAL accede a información personal que es tratada conforme a los requisitos legales establecidos tanto en el RGPD y la LOPD.

En aquellos casos en los que se cuenta con un encargado de tratamiento, se establecen los acuerdos y condiciones que rigen la forma en la que deben ser tratados en función de los riesgos detectados por el responsable de protección, que evalúa el tratamiento que debe aplicarse en cada caso, y al que puede acceder para ejercer los derechos contemplados en la legislación a través de la dirección de correo electrónico informatica@gruposagital.com.

3. REVISIÓN

Esta política será revisada de forma anual, cualquier actualización será aprobada por la Alta Dirección y comunicada a las áreas responsables para su implementación inmediata.

Política de Compras Sostenibles aprobada por Dirección:

Última revisión	10/02/2025
-----------------	------------



4. OBJETIVOS Y METAS

OBJETIVO	META	ACCIÓN A DESARROLLAR
Aumentar la seguridad en el acceso y gestión de usuarios	Crear usuarios únicos y seguros dentro del	Configurar cuentas individuales en el dominio, asegurando contraseñas robustas y seguimiento de accesos.
Actualizar la infraestructura de servidores	Completar la migración de datos a servidores Windows 2022 en un 100%	Migrar la información y verificar compatibilidad y seguridad de los nuevos servidores.
Mejorar la autenticación y firma electrónica	Obtener certificación eIDAS en todos los procesos de firma y autenticación	Adquirir certificados acreditados bajo eIDAS para cumplimiento y seguridad en transacciones electrónicas.
Fortalecer la seguridad perimetral	Integrar un firewall del catálogo CCN para reforzar protección externa	Adquirir e instalar el firewall, ajustando configuración para el entorno y requisitos específicos
Asegurar la integridad de la información	Configurar copias de seguridad externas periódicas	Establecer backups automáticos en ubicaciones seguras fuera de las instalaciones.
Optimizar la administración de IT	Externalizar el soporte técnico.	Contratar servidores externos para una gestión más eficiente y profesionalizada de los sistemas.