04 Políticas del sistema

CONTROL EDICIONES			
EDICIÓN	**FECHA**	**MOTIVO DEL CAMBIO**	**APARTADO**
01	1/09/2025	Edición inicial.	

1. Política de general de Calidad y medioambiente

GRUPO SOLUTIA, tiene como propósito ofrecer soluciones integrales en el ámbito empresarial mediante la distribución, instalación y mantenimiento de hardware, el desarrollo de aplicaciones software y servicios de outsourcing de personal especializado en informática, a través de un comprometido equipo profesional.

Nuestra misión es satisfacer las necesidades de los clientes ofreciendo soluciones innovadoras y vanguardistas en el sector de las tecnologías de la información, incorporando tecnologías de último generación, y un equipo de alta cualificación profesional.

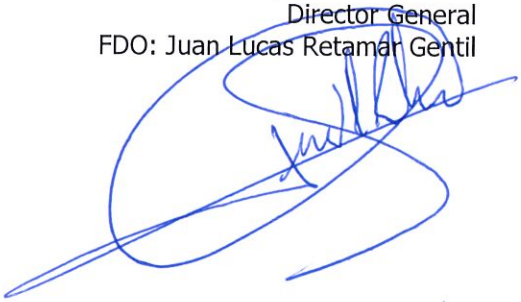
En este marco, la Dirección de **SOLUTIA** establece los siguientes compromisos:

- **Inversión continua** en **tecnologías innovadoras de última generación**, así como, en **formación del equipo de profesional** para ofrecer soluciones a medida con atención técnica inmediata, flexible y, especializada.
- **Ofrecer productos y servicios** que cumplan los más **altos estándares de calidad, respetando y protegiendo el medio ambiente.**
- **Optimizar nuestros procesos** para asegurar el **cumplimiento normativo** de aplicación, y de nuestros **objetivos ambientales y de calidad**, la **satisfacción y expectativas de los clientes** y partes interesadas, **minimizando** a la vez los **impactos ambientales** de nuestra actividad.
- **Impulsar la mejora continua** de los procesos de gestión a lo largo de la vida de cada proyecto, así como, **la prevención de la contaminación.**
- **Fomentar la concienciación** con la **calidad**, la **eficiencia energética**, y la **protección al medioambiente** contribuyendo a la mitigación del impacto de la actividad de SOLUTIA en **el cambio del climático.**
- **Asegurar** una **gestión eficiente de los recursos materiales, técnicos, económicos y del talento,** así como **fomentar** un **buen clima laboral y entorno colaborativo** que permita **consolidar nuestra posición en el mercado,** reforzando nuestra **imagen verde e innovadora,** y la confianza de nuestros clientes para que nos permita seguir creciendo como **organización líder del sector.**
- **Detectar las incidencias que surjan de nuestros procesos, analizarlas y proponer las acciones correctivas que garanticen el correcto desarrollo de la organización.**

Esta política es la base para conseguir los objetivos y metas de la empresa, con estrategias que mejoren la eficiencia, la rentabilidad y los procesos en base a la importancia de la **calidad** y **el respeto al medioambiente** en el correcto desarrollo de sus actividades.

Este compromiso se revisa anualmente como parte del proceso de mejora continua y alineación con la estrategia corporativa. Además, esta política se comunicará a los empleados y personal externo subcontratado, y se pone a disposición de todos los clientes y otras partes interesadas.

Sevilla, 1 de septiembre de 2025
Director General
FDO: Juan Lucas Retamar Gentil



2. Política de presupuestos y contabilidad de los servicios

En **GRUPO SOLUTIA**, el proceso de **presupuestos y contabilidad de servicios** constituye la base para planificar, evaluar y controlar los costes asociados a la prestación de servicios tecnológicos.

Su objetivo es garantizar una gestión económica transparente, eficiente y alineada con los compromisos adquiridos con los clientes, asegurando al mismo tiempo la sostenibilidad y rentabilidad de la organización.

Para ello, la Dirección ha establecido el procedimiento de **Presupuesto y Contabilidad de Servicios**, basado en las siguientes premisas:

- **Previsión financiera rigurosa**: elaborar estimaciones realistas y documentadas de los costes previstos durante el ciclo de vida de los servicios, considerando recursos humanos, tecnológicos y materiales.
- **Control y seguimiento**: establecer referencias y métricas que permitan contrastar periódicamente los costes reales frente a los presupuestados, identificando desviaciones y adoptando acciones correctivas oportunas.
- **Gestión de riesgos económicos**: reducir la incertidumbre y mitigar el riesgo de sobrecostes no planificados, aplicando mecanismos de control preventivo.
- **Análisis de impacto en cambios**: evaluar las repercusiones económicas de modificaciones en los servicios, contratos o acuerdos de nivel de servicio (SLA), garantizando la sostenibilidad de márgenes y beneficios.
- **Eficiencia en la asignación de recursos**: optimizar el uso de los recursos financieros, humanos y tecnológicos, asegurando su correcta imputación a los proyectos y servicios correspondientes.
- **Apoyo a la toma de decisiones**: proporcionar información contable y presupuestaria clara y actualizada que sirva de soporte a la Dirección y a la planificación estratégica de la organización.

De esta forma, el proceso no solo controla los costes, sino que se convierte en una **herramienta de gestión estratégica**, que contribuye a mantener la competitividad de **SOLUTIA** y a garantizar la calidad y rentabilidad de sus servicios tecnológicos.

3. Política de Configuración

Con el objetivo de garantizar el cumplimiento de los acuerdos de nivel de servicio (SLA) suscritos con los clientes y optimizar las actividades relacionadas con la gestión de sus sistemas (cambios, gestión de incidencias, soporte, etc.), **GRUPO SOLUTIA** debe disponer de información precisa y actualizada sobre los equipos, componentes y activos incluidos en el alcance de los servicios contratados, incluyendo al menos datos clave como número de serie, marca y modelo.

La Dirección establece un proceso de **Gestión de la Configuración**, en cumplimiento de lo establecido en esta política, se basa en las siguientes directrices:

- **Exactitud de la información**: proporcionar datos fiables y completos sobre las características de los elementos de configuración (hardware, software, documentación y servicios) para dar soporte al resto de procesos del sistema de gestión.

- **Actualización continua**: garantizar que la información registrada sobre los elementos de configuración se mantiene actualizada, reflejando su estado real en todo momento.

- **Control de cambios**: registrar y supervisar los cambios que afecten a los activos, asegurando la trazabilidad de su historial y la correcta vinculación con incidencias, problemas o modificaciones.

- **Disponibilidad de datos**: asegurar que la información de configuración esté disponible para las áreas que la requieran, facilitando la toma de decisiones, la resolución de incidencias y la planificación de mejoras.

- **Apoyo a la mejora del servicio**: utilizar la información de configuración como herramienta estratégica para mejorar la eficiencia, reducir riesgos, optimizar recursos y garantizar la calidad de los servicios ofrecidos.

Con esta política, **SOLUTIA** refuerza su capacidad de controlar y gestionar los activos tecnológicos de los clientes, mejorando la **eficiencia operativa**, reduciendo riesgos asociados a cambios no controlados y garantizando la entrega de servicios de calidad alineados con los compromisos adquiridos.

4. Políticas de seguridad de la información

4.1 Propósito, alcance y compromiso de la Dirección

La presente **Política de Seguridad de la Información** de **GRUPO SOLUTIA** establece el marco de actuación para proteger los recursos de información frente a amenazas internas o externas, deliberadas o accidentales, que puedan afectar a la organización, a sus clientes o a terceros relacionados.

Su **objetivo** es garantizar:

- La **confidencialidad**, asegurando que la información solo esté disponible para personas autorizadas.
- La **integridad**, preservando la exactitud y fiabilidad de los datos y sistemas.
- La **disponibilidad**, garantizando que la información y los servicios estén accesibles cuando sean requeridos.

El **alcance** de esta política incluye:

- Todos los procesos, sistemas, servicios, infraestructuras y activos tecnológicos de **SOLUTIA**.
- Toda la información gestionada, tanto propia como de clientes y terceros, independientemente de su soporte (digital, físico o verbal).
- A todas las personas que accedan a los recursos de información: empleados, colaboradores, contratistas y proveedores autorizados.

Esta política es de **obligado cumplimiento** para **todo el personal** y se complementa con las normas y procedimientos específicos del Sistema de Gestión de Seguridad de la Información (SGSI), en conformidad con la **ISO/IEC 27001:2023**, la **ISO/IEC 27002:2023** y el **Esquema Nacional de Seguridad (RD 311/2022)**.

Asimismo, todos los empleados, colaboradores, contratistas y proveedores con acceso a información de **SOLUTIA** o de sus clientes están sujetos al **Acuerdo de Confidencialidad** y a las **Cláusulas de protección de datos incluidas en los contratos laborales o mercantiles**, en cumplimiento del **Reglamento General de Protección de Datos (RGPD)** y la **Ley Orgánica 3/2018 (LOPDGDD)**. Estas obligaciones se mantienen incluso después de la finalización de la relación contractual.

4.2 Marco Normativo y Referencias

El **Sistema de Gestión de Seguridad de la Información (SGSI)** de **SOLUTIA** se desarrolla y aplica en cumplimiento de la legislación vigente y de las normas internacionales de referencia, garantizando así un marco de actuación sólido y reconocido.

Legislación y normativa aplicable:

- **Reglamento (UE) 2016/679 (RGPD)**, 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.
- **Ley Orgánica 3/2018 (LOPDGDD)**, de Protección de Datos Personales y garantía de los derechos digitales.
- **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad (ENS)**, aplicable a proveedores de servicios tecnológicos que trabajan con el sector público y que constituye una referencia de buenas prácticas también para el sector privado.
- **Norma UNE-EN ISO/IEC 27001:2023**, referente internacional para la gestión de la seguridad de la información.
- **Norma UNE-EN ISO/IEC 27002:2023**, guía práctica para la implementación de controles de seguridad.
- **XIX Convenio Colectivo Estatal de Empresas de Consultoría, Tecnologías de la Información y Estudios de Mercado y de la Opinión Pública**, recogido y registrado mediante Resolución de 4 de abril de 2025, de la Dirección General de Trabajo, sus posteriores actualizaciones, así como, otra normativa fiscal, mercantil, laboral y sectorial que se aplique a la actividad de la organización.

Compromisos contractuales y regulatorios

Además de la normativa general, **SOLUTIA** asume el compromiso de:

- Cumplir con los requisitos contractuales específicos que en materia de seguridad sean exigidos por sus clientes.
- Respetar los acuerdos de confidencialidad firmados con empleados, colaboradores y terceros.
- Incorporar en su SGSI los **requisitos adicionales de seguridad y protección de datos** que resulten de contratos, auditorías externas o certificaciones.

Mantenimiento y actualización normativa

El Comité de Seguridad de la Información es responsable de:

- Mantener actualizado el **listado de requisitos legales** (**R01.02**)
- Analizar periódicamente los cambios normativos y contractuales, valorando su impacto en el SGSI y asegurando su cumplimiento.
- Difundir internamente las actualizaciones normativas relevantes para garantizar que todos los empleados y colaboradores conozcan sus obligaciones.

4.3 Estructuración de la documentación de seguridad

La documentación de seguridad del sistema se estructurará conforme a una jerarquía documental que incluirá: Política de Seguridad, normas y procedimientos, instrucciones técnicas y registros asociados, garantizando su coherencia con el Sistema de Gestión de Seguridad de la Información (SGSI). Toda la información documentada será identificada, versionada, revisada y aprobada formalmente, manteniéndose accesible únicamente al personal autorizado mediante controles de acceso adecuados, asegurando su confidencialidad, integridad, disponibilidad y trazabilidad durante todo su ciclo de vida.

4.4 Principios Generales de Seguridad

En cumplimiento del **artículo 12.6 del Real Decreto 311/2022 (ENS**), la Política de Seguridad se desarrolla conforme a los principios básicos del **Capítulo II** y se concreta en los siguientes requisitos mínimos:

1. **Organización e implantación del proceso de seguridad:** la organización establece y mantiene un proceso formal de seguridad integrado en su sistema de gestión, definiendo claramente roles, responsabilidades y autoridades. La Dirección impulsa, supervisa y garantiza la implantación efectiva de las medidas de seguridad.
2. **Análisis y gestión de los riesgos:** la organización realiza un análisis sistemático y periódico de los riesgos que afectan a los sistemas de información, identificando amenazas, vulnerabilidades e impactos. Los riesgos se tratan conforme a criterios aprobados, aplicando medidas proporcionadas a la categoría del sistema.
3. **Gestión de personal:** la organización garantiza que el personal conoce y cumple sus responsabilidades en materia de seguridad, mediante formación, concienciación y compromisos formales. Se aplican controles durante todo el ciclo de vida laboral, incluyendo la incorporación, cambios de puesto y cese.
4. **Profesionalidad:** las funciones relacionadas con la seguridad de la información se desempeñan por personal cualificado, con la competencia técnica y experiencia adecuadas. La organización fomenta la actualización continua de conocimientos en seguridad y normativa aplicable.
5. **Autorización y control de los accesos:** el acceso a los sistemas de información se concede únicamente a usuarios autorizados conforme a sus funciones y responsabilidades. Se aplican mecanismos de identificación, autenticación y control que garantizan la trazabilidad y revisión periódica de permisos.
6. **Protección de las instalaciones:** las instalaciones que albergan sistemas de información disponen de medidas de protección física y ambiental adecuadas a su categoría. Se controla el acceso físico para prevenir daños, intrusiones o accesos no autorizados.
7. **Adquisición de productos de seguridad y contratación de servicios de seguridad:** la organización incorpora requisitos de seguridad en los procesos de adquisición y contratación de productos y servicios TIC. Se verifica que proveedores y soluciones cumplen los estándares y obligaciones de seguridad exigibles.
8. **Mínimo privilegio:** cada usuario dispone exclusivamente de los permisos estrictamente necesarios para el desempeño de sus funciones. Los privilegios especiales se asignan de forma controlada, justificada y revisada periódicamente.
9. **Integridad y actualización del sistema:** la organización protege la integridad de los sistemas mediante una adecuada gestión de configuración, control de cambios y aplicación de actualizaciones de seguridad. Se supervisa el estado de los sistemas para detectar alteraciones no autorizadas.
10. **Protección de la información almacenada y en tránsito:** la información se protege mediante medidas técnicas y organizativas que garantizan su confidencialidad, integridad y disponibilidad, tanto en almacenamiento como en transmisión. Se aplican mecanismos de cifrado y controles adecuados según su nivel de clasificación.
11. **Prevención ante otros sistemas de información interconectados:** las interconexiones con otros sistemas se autorizan formalmente y se someten a análisis de riesgos previo. Se implantan controles específicos para evitar que dichas conexiones comprometan la seguridad del sistema.
12. **Registro de la actividad y detección de código dañino:** la organización registra y conserva la actividad relevante de los sistemas para garantizar la trazabilidad y facilitar la detección de incidentes. Se implantan mecanismos de protección y detección frente a código malicioso y otras amenazas.
13. **Incidentes de seguridad:** la organización dispone de un procedimiento formal para la detección, notificación, gestión y resolución de incidentes de seguridad. Los incidentes se analizan, documentan y utilizan como base para la adopción de medidas correctivas.
14. **Continuidad de la actividad:** la organización establece y mantiene planes de continuidad y recuperación que garantizan la prestación de los servicios esenciales ante situaciones adversas. Dichos planes se prueban y actualizan periódicamente.

15. **Mejora continua del proceso de seguridad:** la organización revisa periódicamente el sistema de seguridad mediante auditorías, seguimiento de indicadores y revisión por la Dirección. Se adoptan acciones correctivas y de mejora para garantizar su eficacia y adecuación permanente.

Adicionalmente, en base a la **UNE-EN ISO/IEC 27001:2023, la ISO/IEC 27002:2023, SOLUTIA** aplica a todas las personas, procesos, servicios, sistemas y terceros relacionados con la organización son los siguientes principios de actuación fundamentales:

1. **Confidencialidad**

La información será accesible únicamente a las personas debidamente autorizadas:

- Todo el personal y terceros que accedan a información de **SOLUTIA** o de sus clientes están sujetos al **Acuerdo de Confidencialidad** y a las **cláusulas contractuales de protección de datos**.
- Se aplicarán controles de acceso físico y lógico, así como la clasificación de la información según su nivel de sensibilidad, de acuerdo con los controles y procedimientos establecidos acordes al marco regulatorio aplicable.

2. **Integridad**

Se garantizará la exactitud, coherencia y fiabilidad de la información y de los sistemas que la gestionan:

- Se adoptarán mecanismos de verificación, control de cambios, trazabilidad y protección frente a modificaciones no autorizadas.
- Los sistemas y servicios serán objeto de pruebas y validaciones periódicas para asegurar su correcto funcionamiento.

3. **Disponibilidad**

La información y los servicios estarán accesibles cuando sean necesarios para la continuidad de la actividad de la organización:

- Se mantendrán planes de **continuidad del negocio y recuperación ante desastres**, conforme a la **UNE-EN ISO/IEC 27001:2023, la ISO/IEC 27002:2023** y el **ENS**.
- Se garantizarán medidas de redundancia, copias de seguridad periódicas y sistemas alternativos para reducir el impacto de incidentes graves.

4. **Legalidad y cumplimiento**

Todas las actividades relacionadas con la seguridad de la información se ajustarán a la normativa vigente, y compromisos contractuales asumidos recogidos en el apartado **4.2 Marco Normativo y Referencias.**

5. **Responsabilidad proactiva**

La seguridad de la información es responsabilidad de todos los empleados y colaboradores de **SOLUTIA**:

- Cada usuario es responsable del uso adecuado de los sistemas y activos a los que tenga acceso.
- La Dirección impulsará programas de **formación y concienciación** continua, en cumplimiento de la normativa en relación con la normativa aplicable en el marco de la seguridad de la información.

6. Mejora continua

El SGSI será revisado y actualizado anualmente para garantizar su adecuación y eficacia. Se tendrán en cuenta los resultados de las auditorías, revisiones por la Dirección, análisis de riesgos e incidentes servirán para la identificación de oportunidades de mejora.

4.5 Gobernanza, Roles y Responsabilidades

La implantación efectiva de la **Política de Seguridad de la Información** requiere que todas las personas que forman parte de **GRUPO SOLUTIA** comprendan y asuman sus obligaciones en función de su rol.

Para garantizar una gobernanza adecuada, se constituye el **Comité de Seguridad de la Información**, como órgano de decisión, coordinación y supervisión en materia de seguridad, que está integrado por los siguientes perfiles clave:

1. **Responsable de la Información** y **Responsable del Servicio, a nivel de gobierno** (**Director General)**

Responsabilidades como Responsable de la Información:

- Crear formalmente el Comité de Seguridad de la Información.
- Establecer los requisitos de seguridad de la información gestionada por la organización.
- Determinar los niveles de seguridad de la información basándose en las propuestas del Comité de Seguridad.

Responsabilidades como Responsable del Servicio:

- Definir los requisitos de seguridad de los servicios prestados a clientes.
- Determinar los niveles de seguridad aplicables a dichos servicios, en coherencia con los acuerdos de nivel de servicio (SLA) y los objetivos estratégicos de la organización.

2. **Responsable del Sistema de Información, a nivel operativo (Director de SSCC):**

- Establecer los requisitos de seguridad aplicables a la información gestionada en los sistemas de información.
- Determinar los niveles de seguridad de los sistemas de información conforme a las propuestas del Comité de Seguridad.
- Desarrollar, operar y mantener los sistemas de información durante todo su ciclo de vida (especificaciones, instalación, verificación de funcionamiento).
- Definir la **topología** y los **criterios de gestión** de los sistemas de información, estableciendo condiciones de uso y servicios disponibles.
- Asegurar la integración de las medidas de seguridad en el marco general del SGSI.
- Proponer al Comité de Seguridad la suspensión temporal del tratamiento de información o de la prestación de un servicio cuando existan deficiencias graves de seguridad, elevando la decisión final a la Dirección.

3. **Responsable de la Seguridad, a nivel de supervisión (Director de Ciberseguridad):**

- Determinar y coordinar las acciones necesarias para garantizar los requisitos de seguridad de la información y de los servicios TIC.
- Suscribir y mantener la **Declaración de Aplicabilidad (SoA)**, responsabilizándose de las medidas de seguridad definidas en ella.

- Realizar **auditorías internas periódicas** en materia de seguridad y elaborar los informes correspondientes.
- Promover la **formación y concienciación** del personal en seguridad de la información.
- Supervisar la adecuación y eficacia de las medidas de seguridad implantadas.
- Revisar y aprobar la documentación de seguridad del Sistema de Información.
- Monitorizar el estado de la seguridad mediante herramientas de gestión de eventos y auditorías técnicas.
- Supervisar la investigación y resolución de incidentes de seguridad.
- Determinar la categoría de los sistemas de información, considerando las valoraciones de los responsables de la información, servicios y el Comité de Seguridad.

4. **Administrador de Seguridad del Sistema, a nivel operativo (Responsable de Informática Interna):**

- Implementar, gestionar y mantener las medidas de seguridad técnicas aplicables al Sistema de Información.
- Configurar, administrar y actualizar el hardware y software que soporta los mecanismos de seguridad.
- Gestionar las **autorizaciones y privilegios de los usuarios**, monitorizando que la actividad se ajuste a lo autorizado.
- Aplicar los procedimientos operativos de seguridad y verificar su cumplimiento.
- Supervisar instalaciones, modificaciones o mejoras en hardware y software para garantizar que no comprometen la seguridad.
- Monitorizar el estado de seguridad mediante herramientas de gestión de eventos y auditorías técnicas.
- Informar al Responsable de Seguridad y/o al Responsable del Sistema de Información de anomalías o vulnerabilidades.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su cierre.

5. **Responsable del (SGSI), a nivel de gestión (Responsable de Calidad y Cumplimiento Legal):**

- Coordinar la implantación, desarrollo, mantenimiento y mejora continua del SGSI.
- Asegurar la integración del SGSI con los sistemas de gestión de calidad, medioambiente y compliance.
- Garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales en seguridad de la información y protección de datos.
- Coordinar las **auditorías internas del SGSI** y facilitar las revisiones por la Dirección.
- Mantener actualizada la documentación del SGSI y garantizar su difusión al personal y partes interesadas.
- Reportar periódicamente al Comité de Seguridad sobre el estado del SGSI.
- Promover la cultura de seguridad de la información en toda la organización.
- Garantizar la medición, análisis y seguimiento de los indicadores del SGSI como base para la mejora continua.

Por último, encontramos el rol de **Delegado de Protección de Datos (DPO)**, rol **externo** al Comité de Seguridad, subcontratado a la empresa especializada **RAPINFORMES ONLINE S.L.**, que actúa con independencia funcional y depende directamente del Departamento de Calidad y Cumplimiento Normativo de **SOLUTIA**.

Las responsabilidades del DPO son (según RGPD art. 39 y LOPDGDD):

- **Supervisión del cumplimiento**: garantizar que el tratamiento de datos personales se realiza conforme al **RGPD**, la **LOPDGDD** y las políticas internas de protección de datos.

- **Auditorías**: realizar auditorías periódicas en materia de protección de datos, incluyendo revisión de políticas, procesos de recogida y almacenamiento, consentimiento, medidas de seguridad y cumplimiento de la LSSICE.
- **Formación y concienciación**: promover la sensibilización y la formación del personal implicado en el tratamiento de datos personales.
- **Evaluaciones de impacto**: asesorar y supervisar la realización de **Evaluaciones de Impacto en Protección de Datos (EIPD)** conforme al art. 35 RGPD.
- **Relación con la autoridad de control**: cooperar con la Agencia Española de Protección de Datos (AEPD) y actuar como punto de contacto en caso de consultas, reclamaciones o notificaciones de brechas de seguridad.
- **Asesoramiento experto**: informar y asesorar al Responsable del Tratamiento y a los encargados sobre sus obligaciones legales y sobre eventuales cambios legislativos que impacten en el sistema de gestión.
- **Incidencias y brechas**: supervisar la gestión y comunicación de incidentes y brechas de datos personales, incluyendo la coordinación con la AEPD cuando proceda.

4.6 Gestión de riesgos y control de la información

1 - Identificación y Evaluación de Riesgos

Todos los sistemas de información sujetos a esta política deberán someterse a un proceso sistemático de **análisis y evaluación de riesgos**, que permita identificar amenazas, vulnerabilidades y su impacto potencial sobre la organización. Este análisis se repetirá:

- Con carácter regular, al menos una vez al año.
- Cada vez que cambien los servicios prestados o la información tratada.
- Tras la ocurrencia de incidentes graves de seguridad.
- Cuando se detecten vulnerabilidades críticas en los sistemas.

El **Comité de Seguridad de la Información** establecerá criterios de referencia para valorar la criticidad de la información y los servicios, dinamizando la disponibilidad de recursos para atender las necesidades de seguridad.
La gestión de riesgos quedará documentada en el **Plan de tratamiento de riesgos (IT09.01-02)**, que servirá de base para la selección de controles.

2 - Inteligencia de Amenazas

SOLUTIA incorpora información de fuentes internas y externas para mejorar la capacidad de anticipación y respuesta frente a riesgos de seguridad. Las fuentes habituales son:

- Boletines de seguridad de **INCIBE**, **CCN-CERT** y fabricantes de software y hardware.
- Alertas de proveedores de servicios de seguridad gestionada (SOC).
- Información compartida en foros sectoriales y asociaciones TIC. Los resultados de este análisis se integrarán en el proceso de gestión de riesgos y en la priorización de controles.

3 - Clasificación y Etiquetado de la Información

La información será clasificada en función de su nivel de sensibilidad y del impacto que tendría su divulgación, modificación o pérdida, conforme a los controles de la **ISO/IEC 27002:2023** y el ENS. **SOLUTIA** establece los siguientes niveles de acuerdo con M365:

- **Pública**: accesible a personal interno y externo sin restricciones.

- **Uso interno**: accesible a personal de **GRUPO SOLUTIA** y a terceros autorizados.
- **Confidencial**: accesible únicamente a la Dirección y a usuarios autorizados expresamente.

La clasificación se documentará en los listados de documentos y registros del SGSI, y se reflejará en los sistemas mediante etiquetas o marcas visibles para garantizar su correcta gestión.

4 - Protección de la Información en Entornos de Usuario

Para proteger la información en entornos de usuario, se aplicarán las siguientes medidas:

- **Política de escritorio limpio y pantalla bloqueada**: no dejar documentos sensibles sobre las mesas y bloquear los equipos cuando no se usen.
- **Protección de dispositivos**: cifrado de discos duros en portátiles, uso obligatorio de antivirus actualizado y prohibición de instalar software no autorizado.
- **Restricciones de periféricos**: control del uso de memorias USB y dispositivos externos mediante políticas de DLP (Data Loss Prevention).
- **Teletrabajo seguro**: acceso remoto mediante VPN cifradas y autenticación de doble factor.

5 - Manipulación y Conservación de la Información

El acceso a la información estará condicionado por los criterios de clasificación aplicados:

- La **información confidencial** no deberá almacenarse en papel ni en soportes extraíbles salvo necesidad justificada y autorización expresa.
- Todo soporte que contenga información sensible deberá ser custodiado y eliminado de forma segura, aplicando destrucción física o borrado seguro certificado.
- Los soportes en tránsito deberán contar con medidas de seguridad adicionales: cifrado, transporte seguro o, en el caso de documentos físicos, envío en sobres cerrados y sellados.

6 - Control de Accesos a los sistemas de información

SOLUTIA aplica políticas de **control de accesos físicos y lógicos**, conforme al marco normativo de seguridad de la información con el objetivo de evitar accesos no autorizados a los sistemas de información:

- El acceso a los sistemas y la información se realiza a través de técnicas de autenticación y autorización, y se limita en función de los roles y responsabilidades definidos.
- Se aplica el principio de **"mínimo privilegio"**, asignando únicamente los permisos estrictamente necesarios.
- Se revisan periódicamente las autorizaciones y se revocan de manera inmediata en caso de cambios de puesto o desvinculación laboral.
- Se registra y monitoriza la actividad de los usuarios para asegurar la trazabilidad y detectar usos indebidos.

7 - Monitorización y Registro de Eventos

La actividad en los sistemas será objeto de monitorización y registro, con el fin de detectar accesos indebidos o incidentes de seguridad.

- Se habilitarán registros de auditoría en sistemas críticos y aplicaciones corporativas.
- Los logs se conservarán durante un periodo definido según criticidad y requisitos legales.
- Los registros estarán protegidos frente a manipulaciones y accesibles únicamente al personal autorizado.

- Se usarán herramientas de correlación y monitorización (SIEM/SOC) para detectar patrones de ataque o anomalías.

9- Conservación y Eliminación de Soportes

La eliminación de información y soportes deberá realizarse de forma controlada, segura y verificable:

- **Soportes en papel**: destrucción física mediante trituradoras.
- **Soportes digitales**: restauración y/o borrado seguro con herramientas homologadas o destrucción física.
- **Equipos en desuso**: reutilización solo tras formateo certificado o eliminación mediante procedimientos de borrado seguro.
- **Entornos en la nube**: eliminación segura mediante los mecanismos de borrado y versionado que ofrezcan los proveedores, asegurando la revocación de accesos y la trazabilidad.

4.7 Gestión de incidentes y continuidad

SOLUTIA establece un procedimiento formal para la **detección, notificación, análisis, respuesta y resolución** de incidentes de seguridad de la información, incluyendo brechas de datos personales.

Obligaciones del personal empleado:

- Notificar de inmediato cualquier incidente, incluyendo accesos no autorizados, pérdida de información, infecciones de malware, uso indebido de privilegios o sospechas de brechas de datos personales.
- Documentar la incidencia en los canales seguros y confidenciales habilitados, incluyendo fecha, hora, descripción y posible impacto (cybersoc@gruposolutia.com / https://asistencia.gruposolutia.com).
- Colaborar con el cumplimiento de las medidas correctivas implantadas

Responsabilidades organizativas:

- **Responsable de Seguridad (CISO):** coordinar el análisis y respuesta; supervisar cadena de custodia y evidencias; validar la recuperación y cierre de incidentes; aprobar acciones críticas; aprobar informes post-incidente; informar y elevar lecciones aprendidas al Comité de Seguridad; validar toda notificación externa antes de su envío.
- **Delegado de Protección de Datos (DPO/DPD externo):** gestionar brechas de datos personales, evaluar el impacto y notificar a la AEPD en <72 horas; asesorar al Comité de Seguridad y apoyar en comunicaciones a interesados afectados.
- **Comité de Seguridad:** aprobar medidas de mejora, revisar métricas de incidentes, validar lecciones aprendidas y planes de acción, así como comunicar y activar las medidas necesarias ante incidentes críticos coordinados por el responsable de la seguridad.

Recopilación y preservación de evidencias:

- Toda la información y evidencias asociadas a un incidente (registros de auditoría, trazas de red, imágenes forenses, correos electrónicos, informes técnicos) deberán recopilarse y custodiarse por el personal autorizado siguiendo procedimientos formales de cadena de custodia, garantizando su validez para auditorías, procesos disciplinarios o procedimientos legales.

4.8 Auditorías y Revisión Continua

La organización llevará a cabo auditorías internas periódicas para evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) y su conformidad con los requisitos de la legislación y norma de

aplicación (**ISO/IEC 27001:2023**, **ISO/IEC 27002:2023**, el **Esquema Nacional de Seguridad (ENS)**, y normativa europea **RGPD, LOPDGDD** y demás normativa aplicable).

El alcance de las auditorías contempla el cumplimiento de políticas, procedimientos y controles del SGSI, la correcta clasificación, custodia y uso de la información, la eficacia de los controles técnicos, organizativos y físicos implantados, la gestión de riesgos, incidentes y continuidad, así como el cumplimiento de obligaciones contractuales y regulatorias.

El Comité de Seguridad, junto con la Dirección, será responsable de impulsar acciones de mejora y verificar su eficacia, asegurando que se integren en los procesos de negocio de la organización.

4.9 Régimen Disciplinario y Cumplimiento Normativo

El incumplimiento de las políticas de seguridad podrá derivar en sanciones disciplinarias, conforme al **Convenio Colectivo aplicable** y a la **legislación laboral vigente**, sin perjuicio de las responsabilidades civiles o penales que pudieran corresponder.

Asimismo, se garantizará el **cumplimiento de los requisitos legales y contractuales** en materia de seguridad de la información, incluyendo: propiedad intelectual y licencias de software, protección de datos personales, acuerdos de confidencialidad, registros y evidencias electrónicas, asegurando su integridad y trazabilidad.

Sevilla, 1 de septiembre de 2025
Director General
FDO: Juan Lucas Retamar Gentil

5. Política cambios

Los cambios requieren una planificación adecuada y meticulosa con objeto de asegurar su éxito, identificando cualquier impacto negativo sobre los servicios.

Con el objetivo de evitar interrupciones no planificadas, así como la posible degradación de los servicios, se someten al proceso de gestión de cambios, requiriendo la aprobación del Jefe de proyecto, los siguientes cambios:

- Diseño de nuevos servicios o la modificación del objetivo o alcance de los servicios incluidos en el catálogo de servicios de la entidad.
- Las modificaciones de las sistemáticas o las tecnologías empleadas para la presentación de los servicios actuales.
- Los cambios que puedan realizarse tanto en las infraestructuras de cliente gestionadas por SOLUTIA como en la propias necesarias para la prestación de los servicios.

6. Política de entrega

Con el objetivo de garantizar los servicios de entrega de forma adecuada, y en concordancia con los acuerdos de nivel, la política de entrega de SOLUTIA se basa en los siguientes principios:

- Planificación y supervisión de las entregas, asegurando su puesta en producción dentro de los plazos acordados con los clientes o marcados por los acuerdos de nivel de servicio aplicable.
- Asegurar el correcto funcionamiento de los sistemas, realizando las pruebas pertinentes sobre el contenido exacto considerado en la entrega, antes de su liberación y posterior puesta en servicio.