SUARDIAZ Group

PL 16.2_1

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

REGISTRO DE CAMBIOS

Edición	Fecha	Página	Descripción del cambio
01	15/09/2026		Edición Inicial

LISTA DE DISTRIBUCCIÓN INTERNA

Personal/Cargo	Fecha	Modo
Departamento IT	15/09/2026	Compartido en la red

ELABORADO	REVISADO	APROBADO
Ciriaco Guisasola Alonso Information & Technologies Director	Laura Rodriguez Caviedes Integrated Management System Coordinator (QHSE)	Laura Cajade Frías Compliance & Sustainability (ESG) Director
15/09/2026	15/09/2026	15/09/2026

TODOS LOS DERECHOS RESERVADOS

SUARDIAZ Group *posee en propiedad el original de este documento. Las copias que de este documento se suministren tienen carácter confidencial y no podrán ser utilizadas para fines diferentes a aquellos para los cuales son solicitadas, ni tampoco podrán ser reproducidas sin la autorización de* ***SUARDIAZ Group.*** *Cualquier persona, aparte de las autorizadas, que encuentre este documento, deberá enviarlo, deberá enviarlo a: C/ de Ayala, 6, 28001 Madrid o a través del formulario de contacto de la web: https://www.suardiaz.com.*

Contenido

1. OBJETO 1
2. ALCANCE 1
3. DOCUMENTOS DE REFERENCIA 1
4. DEFINICIONES 2
5. RESPONSABILIDADES 2
6. PRINCIPIOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN 4
   6.1 Contexto y partes interesadas 4
   6.2 Protección y clasificación de la información 5
   6.3 Gestión de riesgos y oportunidades 6
   6.4 Inteligencia de amenazas 7
   6.5 Cumplimiento de requisitos aplicables 8
   6.6 Objetivos de seguridad de la información 8
   6.7 Mejora continua del SGSI 9
   6.8 Roles, responsabilidades y autoridades 10
7. COMUNICACIÓN DE LA POLÍTICA 11
8. REVISIÓN, ACTUALIZACIÓN Y CONTROL DE LA POLÍTICA 11
9. DOCUMENTACIÓN RELACIONADA 12
10. ANEXOS 12

1. OBJETO

El objeto de este documento es establecer la **Política de Seguridad de la Información** de SUARDIAZ Group como marco general para proteger la confidencialidad, integridad y disponibilidad de la información, pudiendo incluir adicionalmente autenticidad y trazabilidad, dentro del alcance del Sistema de Gestión de Seguridad de la Información, en adelante SGSI, de conformidad con ISO/IEC 27001:2022. Esta política ampara la protección de la información y de los activos, servicios, procesos y entornos que la soportan, con independencia de su formato, soporte, ubicación o medio de tratamiento.

2. ALCANCE

Esta política aplica a SUARDIAZ Group y es de obligado cumplimiento para las áreas, procesos, sistemas de información, activos, empleados y terceros incluidos en el alcance del SGSI. Aplica a toda la información gestionada en dicho alcance, con independencia de su formato, soporte o medio de tratamiento.

Esta política constituye el marco general al que deben ajustarse las normas, procedimientos y demás documentos del SGSI, en coherencia con el alcance aprobado y con los requisitos aplicables identificados por la organización.

La protección definida por el SGSI se extiende a la información, a los sistemas que la tratan y a los activos tecnológicos, servicios de soporte, infraestructuras y entornos asociados incluidos en el alcance. Cuando proceda, también comprenderá servicios prestados por terceros cuya afectación pueda repercutir en la seguridad de la información de SUARDIAZ Group.

3. DOCUMENTOS DE REFERENCIA

La documentación de referencia para esta política incluye, entre otra documentación aplicable del SGSI, ISO/IEC 27001:2022, ISO/IEC 27002:2022, el Documento de Gestión y Descripción del SGSI, el análisis de contexto y partes interesadas, la documentación de roles y responsabilidades, los objetivos de seguridad de la información, la Declaración de Aplicabilidad y la documentación vigente sobre comunicación y control de la información documentada.

Asimismo, esta política se interpreta de forma coherente con el marco legal, reglamentario, contractual y corporativo aplicable a SUARDIAZ Group en materia de seguridad de la información, continuidad, uso de activos tecnológicos, protección de datos personales, propiedad intelectual, confidencialidad y demás obligaciones que resulten pertinentes dentro del alcance del SGSI, incluyendo, cuando resulte aplicable, el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018 (LOPDGDD) y otras disposiciones sectoriales o contractuales relevantes.

4. DEFINICIONES

SGSI: Sistema de Gestión de Seguridad de la Información establecido, implementado, mantenido y mejorado continuamente por SUARDIAZ Group de acuerdo con los requisitos aplicables de la norma ISO/IEC 27001:2022.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información, pudiendo incluir adicionalmente otras propiedades relevantes como la autenticidad y la trazabilidad.

Partes interesadas pertinentes: personas u organizaciones que pueden afectar, verse afectadas o percibirse afectadas por el desempeño del SGSI y cuyos requisitos son relevantes para la seguridad de la información dentro del alcance definido.

Sistemas de información: conjunto de aplicaciones, servicios, infraestructuras, redes, equipos, soportes y otros medios tecnológicos, propios o de terceros, que permiten tratar, almacenar, transmitir o salvaguardar información dentro del alcance del SGSI.

Clasificación de la información: proceso mediante el cual la información y, cuando proceda, los activos asociados se categorizan en función de su sensibilidad, criticidad, valor y requisitos aplicables, con el fin de determinar las medidas de protección adecuadas.

Activo de información: información, sistema, servicio, proceso, soporte, infraestructura, aplicación, equipo, instalación o cualquier otro recurso que tenga valor para la organización y cuya afectación pueda comprometer la seguridad de la información o la continuidad de las actividades incluidas en el alcance del SGSI.

5. RESPONSABILIDADES

La **Alta Dirección** demuestra liderazgo y compromiso con la seguridad de la información, **aprueba esta política**, asegura su **alineación con la dirección estratégica** de la organización y vela por la **disponibilidad de los recursos**

necesarios para establecer, implementar, mantener y mejorar continuamente el SGSI. En el ejercicio de este liderazgo, **SUARDIAZ Group se compromete a cumplir los requisitos aplicables del SGSI y a mejorar de forma continua su idoneidad, adecuación y eficacia**, como base para la protección de la información dentro del alcance definido.

Asimismo, la Alta Dirección promueve una **cultura de seguridad**, apoya la integración del SGSI en los procesos de negocio y respalda la toma de decisiones necesaria para mantener un nivel de protección adecuado frente a los riesgos identificados.

La asignación de responsabilidades en materia de seguridad de la información se realizará de forma coherente con la estructura organizativa definida por SUARDIAZ Group, promoviendo, cuando proceda, criterios de **segregación de funciones** y evitando concentraciones indebidas de tareas críticas en una misma persona.

El **Responsable del SGSI** vela por la gestión, mantenimiento, revisión, control documental y actualización de esta política, coordina su aplicación dentro del alcance del SGSI e informa a la Alta Dirección sobre el desempeño del sistema y las necesidades de mejora identificadas.

Asimismo, asegura la coherencia entre esta política y el resto de la información documentada del SGSI y coordina su revisión cuando se produzcan cambios organizativos, regulatorios, tecnológicos o de riesgo que requieran su actualización.

Todo el personal y, cuando resulte aplicable, **los terceros incluidos en el alcance** del SGSI deben **conocer**, **respetar** y **aplicar** esta política y las directrices que la desarrollen, contribuyendo a la eficacia del sistema y al **cumplimiento de los requisitos de seguridad de la información** establecidos por la organización.

Este deber implica actuar de forma diligente sobre la información y los activos bajo su responsabilidad, cumplir las normas internas aplicables y colaborar en las actividades de concienciación, seguimiento, revisión y mejora continua del SGSI.

En particular, las personas incluidas en el alcance del SGSI deben utilizar la información y los sistemas de información de forma adecuada a sus funciones, **proteger la confidencialidad** de la información a la que accedan y **comunicar** sin demora, a través de los canales definidos por la organización, **cualquier incidente**, debilidad, uso indebido o situación que pueda comprometer la seguridad de la información. Esta obligación se integra en un **marco formal de gestión de incidentes de seguridad de la información** que contemple, de forma proporcionada, actividades de identificación, registro, evaluación, clasificación, respuesta, escalado, resolución, recuperación y aprendizaje derivado de los

incidentes. Este marco de desarrolla mediante el *PR16.10. Procedimiento de gestión de incidentes* de la información vigente en la organización.

La comunicación deberá abarcar no solo incidentes confirmados, sino también vulnerabilidades, debilidades de control o situaciones observadas que, aun no habiéndose materializado, puedan incrementar el riesgo de seguridad de la información y requieran valoración o tratamiento por parte de la organización.

Cuando la **contratación, supervisión o gestión de terceros** implique acceso a información, sistemas o servicios incluidos en el alcance del SGSI, deberán considerarse los **riesgos asociados** y aplicarse las **medidas de control**, supervisión y formalización que resulten adecuadas conforme a los requisitos de seguridad de la información definidos por SUARDIAZ Group.

6. PRINCIPIOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

La presente política establece un marco general para la protección de la información y de los activos incluidos en el alcance del SGSI, promoviendo una aplicación coherente, estructurada y proporcionada de las medidas de seguridad de la información en función de los riesgos identificados y de los requisitos aplicables. En este contexto, la organización considerará, entre otros, aspectos relacionados con el **control de accesos**, la **gestión de identidades y privilegios**, la **criptografía**, la **seguridad física y ambiental**, la **seguridad en operaciones**, el **registro y monitorización**, la **gestión de vulnerabilidades**, la **continuidad**, la **seguridad en las relaciones con terceros** y la **protección de la información documentada**, sin perjuicio del desarrollo específico que se realice mediante la normativa y procedimientos del SGSI.

6.1 Contexto y partes interesadas

Esta política se establece teniendo en cuenta **el propósito de la organización**, su **contexto interno** y **externo** y las **necesidades** y **expectativas** de las **partes interesadas** pertinentes para el SGSI.

SUARDIAZ Group determina y analiza estos elementos como base para gestionar la seguridad de la información de forma adecuada a su entorno operativo y a los requisitos aplicables. Esta información queda recogida en el documento 'Documento de partes interesadas (Pdte de aprobación)'.

Las directrices de esta política se aplican de forma coherente con el **análisis de contexto**, las **partes interesadas** y los **requisitos legales**, reglamentarios,

contractuales y organizativos aplicables, y se revisan cuando se producen cambios relevantes.

SUARDIAZ Group mantendrá, cuando resulte aplicable, contactos adecuados con **grupos de interés relevantes** en materia de seguridad de la información, incluyendo autoridades, organismos reguladores, clientes, proveedores, asociaciones sectoriales u otros interlocutores pertinentes, con el fin de facilitar la coordinación, el conocimiento de requisitos aplicables y el intercambio de información necesaria para la gestión eficaz del SGSI. Todos los contactos de interés, quién debe comunicarse, qué se comunica, en qué casos y el canal está recogido en el documento de 'Plan de Comunicación (WIP)'.

6.2 Protección y clasificación de la información

La información gestionada dentro del alcance del SGSI deberá protegerse de acuerdo con su valor, sensibilidad, criticidad y requisitos aplicables, promoviendo criterios de clasificación y medidas de protección proporcionales durante todo su ciclo de vida, con independencia de su formato, soporte, ubicación o medio de tratamiento. A estos efectos, la organización establecerá y mantendrá criterios de clasificación definidos que permitan diferenciar, al menos, entre información **Pública**, de **Uso Interno**, **Confidencial** y, cuando proceda, **Restringida** o equivalente, asociando a cada nivel requisitos proporcionales de acceso, tratamiento, almacenamiento, transmisión, conservación y eliminación. El desarrollo específico de los criterios de clasificación, etiquetado, tratamiento y revisión de la información se establecerá en el documento de Procedimiento de Clasificación de la Información vigente en la organización.

El acceso a la información y a los sistemas incluidos en el alcance del SGSI debe limitarse conforme a las **necesidades del negocio** y a las funciones asignadas, aplicando criterios de necesidad de conocer, mínimo privilegio y, cuando proceda, segregación de funciones, de manera que se reduzca el riesgo derivado de accesos inadecuados o incompatibilidades en la asignación de responsabilidades.

Los activos y sistemas de información puestos a disposición de las personas incluidas en el alcance del SGSI deberán utilizarse exclusivamente para **fines autorizados** y en **el marco de las funciones profesionales** que correspondan, de acuerdo con la normativa interna y con las medidas de seguridad establecidas por la organización.

La organización promoverá la **identificación de los activos de información relevantes**, la asignación de responsabilidades sobre ellos y su clasificación y revisión periódica cuando resulte necesario, con el fin de aplicar medidas de protección adecuadas y coherentes con su criticidad, uso y requisitos aplicables.

6.3 Gestión de riesgos y oportunidades

SUARDIAZ Group adopta **un enfoque basado en riesgos** para la gestión de la seguridad de la información. En la planificación, operación y mejora del SGSI se identifican, analizan, evalúan y tratan los riesgos y oportunidades que puedan afectar al logro de los resultados previstos del sistema.

La organización mantiene **criterios de valoración y aceptación del riesgo**, determina las **opciones de tratamiento** apropiadas, selecciona los **controles necesarios** y **documenta** estas decisiones en la información documentada del SGSI, incluida la Declaración de Aplicabilidad y, cuando corresponda, los planes de tratamiento.

El tratamiento de riesgos se orienta a proteger la información y los activos asociados mediante medidas organizativas, físicas y lógicas adecuadas y proporcionadas, **revisándose periódicamente** para asegurar la eficacia del SGSI frente a la evolución del contexto y de los riesgos.

Las acciones para abordar riesgos y oportunidades se integran en los procesos del SGSI y, cuando resulta aplicable, en los procesos afectados por el alcance, evaluándose su eficacia para contribuir al logro de los resultados previstos y a la mejora continua del sistema.

SUARDIAZ Group promoverá que la seguridad de la información se integre en la **gestión de proyectos**, cambios relevantes e **iniciativas** que puedan afectar a la información, a los activos, a los sistemas, a los servicios o a los procesos incluidos en el alcance del SGSI, con independencia de su naturaleza. En estos casos deberán considerarse, desde las fases iniciales de planificación y durante su desarrollo, los requisitos de seguridad aplicables, los riesgos asociados, las medidas de protección necesarias, las responsabilidades implicadas y el impacto que puedan generar sobre la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información, de forma coherente con los principios del SGSI, con la gestión de riesgos y con las necesidades del negocio.

En este marco, SUARDIAZ Group considera de forma expresa los **riesgos derivados de incidentes de seguridad**, interrupciones operativas, accesos no autorizados, fuga o pérdida de información, indisponibilidad de servicios y dependencias con terceros que puedan afectar a la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información. La organización promoverá un tratamiento proporcionado de dichos riesgos, orientado no solo a su prevención y mitigación, sino también **al refuerzo de la capacidad de respuesta** y recuperación ante situaciones que puedan comprometer la continuidad y fiabilidad de las actividades incluidas en el alcance del SGSI.

La organización promoverá asimismo medidas orientadas a asegurar la continuidad de las actividades incluidas en el alcance del SGSI y la recuperación de la información y de los servicios afectados cuando se produzcan incidentes o situaciones disruptivas, en un nivel adecuado a la criticidad de los procesos y activos afectados.

De forma complementaria, SUARDIAZ Group promoverá la **protección física** y ambiental de las instalaciones, equipos, soportes y entornos que soportan la información incluida en el alcance del SGSI, en un nivel adecuado al riesgo y a la criticidad de los activos afectados.

6.4 Inteligencia de amenazas

SUARDIAZ Group promoverá la obtención, revisión, análisis y utilización de **información sobre amenazas de seguridad** de la información y ciberamenazas relevantes para la organización, teniendo en cuenta su contexto, sus actividades, sus activos, sus servicios, sus relaciones con terceros y los riesgos aplicables al alcance del SGSI.

Esta información podrá proceder, cuando resulte pertinente, de **fuentes internas y externas**, incluyendo alertas de fabricantes y proveedores, información asociada a los servicios tecnológicos utilizados por la organización, incidentes o debilidades internas, información derivada de terceros relevantes y otras fuentes especializadas que resulten razonables y proporcionadas a la naturaleza de SUARDIAZ Group. La organización revisará dicha información con una **periodicidad adecuada** y valorará su a**plicabilidad** e **impacto potencial** sobre sus operaciones, activos y servicios.

El resultado de este análisis deberá transformarse en **conocimiento útil** para **anticipar escenarios de riesgo**, apoyar la **toma de decisiones**, reforzar la **capacidad preventiva**, mejorar la **detección y respuesta** ante eventos e incidentes, revisar la **adecuación de los controles implantados**, priorizar acciones de tratamiento y favorecer la **mejora continua** del SGSI. Cuando proceda, la información analizada podrá dar lugar a la revisión de riesgos, la actualización de controles, la adopción de medidas preventivas o correctivas, actuaciones de seguimiento o monitorización, la comunicación a las partes internas o externas pertinentes y la conservación de la información documentada necesaria para evidenciar su consideración y tratamiento dentro del SGSI.

A estos efectos, la organización considerará, entre otras, **amenazas** relacionadas con *accesos no autorizados, campañas de phishing o suplantación, malware o ransomware, fuga o pérdida de información, vulnerabilidades técnicas explotables, indisponibilidad de servicios, errores de configuración, compromisos derivados de terceros* y cualquier otro escenario que, por la naturaleza de SUARDIAZ Group y de

sus operaciones, pueda afectar a la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información.

6.5 Cumplimiento de requisitos aplicables

SUARDIAZ Group se compromete a cumplir los **requisitos legales, regulatorios, y contractuales** aplicables a la seguridad de la información dentro del alcance del SGSI, así como las obligaciones asumidas frente a clientes, empleados, terceros y demás partes interesadas pertinentes.

La organización **revisa periódicamente** la adecuación de sus directrices y controles para mantener el SGSI alineado con el marco normativo y con los compromisos aplicables, adoptando las medidas necesarias cuando se identifiquen cambios o desviaciones. La información relativa a los requisitos se recoge dentro del 'Documento de requisitos legales, regulatorios y contractuales (WIP)'

Asimismo, cuando la organización autorice el uso **de herramientas de inteligencia** artificial en procesos incluidos en el alcance del SGSI, su utilización deberá realizarse de forma controlada, conforme a los requisitos aplicables, preservando la confidencialidad, integridad y disponibilidad de la información, así como la protección de datos personales, la propiedad intelectual y demás obligaciones que resulten exigibles.

Este compromiso se extiende igualmente a los requisitos de seguridad de la información que deban observarse en las **relaciones con proveedores,** colaboradores y otras terceras partes incluidas en el alcance o que tengan acceso a información, sistemas o servicios relevantes para SUARDIAZ Group. La organización promoverá que dichas relaciones se gestionen de forma coherente con los riesgos asociados y con las obligaciones contractuales, legales o regulatorias que resulten aplicables en cada caso.

Cuando SUARDIAZ Group externalice actividades o contrate servicios que impliquen acceso a información, sistemas o procesos incluidos en el alcance del SGSI, deberá asegurarse que dichos servicios se someten a **una evaluación adecuada de riesgos** y que los requisitos de seguridad, confidencialidad, continuidad, notificación y cumplimiento queden formalmente establecidos y, cuando proceda, supervisados durante la relación contractual. Todo este proceso de evaluación queda recogido en el 'Procedimiento de Gestión de Seguridad en Terceros (WIP)'.

6.6 Objetivos de seguridad de la información

Esta política proporciona el marco de referencia para el establecimiento, revisión y seguimiento de los **objetivos de seguridad de la información** en las funciones y niveles pertinentes de la organización. Dichos objetivos deben ser **medibles y**

evaluables, así como coherentes con esta política, con los resultados de la gestión de riesgos, con los requisitos aplicables y con las necesidades del negocio.

SUARDIAZ Group promueve que los objetivos de seguridad de la información sean **comunicados**, **monitorizados** y **respaldados** por los recursos necesarios para su consecución, de forma que contribuyan a la eficacia del SGSI y a la protección adecuada de la información.

En particular, los objetivos de seguridad de la información podrán orientarse, entre otros aspectos, al **fortalecimiento de la capacidad preventiva**, de detección, de respuesta y de recuperación ante incidentes, a la **mejora del nivel de concienciación** del personal, al **refuerzo del control sobre terceros relevantes** y a la **protección adecuada de los activos** y servicios que soportan la información incluida en el alcance del SGSI.

De igual modo, los objetivos podrán contemplar el **fortalecimiento de la formación y concienciación en seguridad de la información**, la verificación de la eficacia de los controles implantados y la mejora progresiva del grado de cumplimiento de los requisitos de seguridad aplicables dentro del alcance del SGSI.

La organización promoverá asimismo que la **formación y concienciación** en seguridad de la información alcancen de forma adecuada a las nuevas incorporaciones, al personal interno y, cuando resulte pertinente, a terceros relevantes, en función de sus responsabilidades y del nivel de acceso o exposición al riesgo asociado.

Todos los **objetivos de seguridad** están recogidos y definidos en el Documento de Objetivos de Seguridad de la Información

6.7 Mejora continua del SGSI

SUARDIAZ Group mantiene el compromiso de **mejorar de manera continua** la idoneidad, adecuación y eficacia del SGSI, apoyándose en el seguimiento del desempeño del sistema, los resultados de auditoría, la revisión por la dirección, la evolución del contexto y de los riesgos y la identificación de oportunidades de mejora.

La organización promueve la adopción de **acciones correctivas**, de mejora o de **adecuación documental** y operativa cuando resulte necesario para asegurar que el SGSI sigue siendo apropiado para el propósito de la organización y eficaz frente a los cambios internos y externos.

Como parte de este compromiso, la organización trata adecuadamente las **desviaciones detectadas**, adopta **acciones correctivas** cuando corresponde y

aprovecha los resultados del seguimiento, las auditorías y las revisiones para **reforzar la eficacia del SGSI** y prevenir su recurrencia.

La mejora continua del SGSI se apoyará igualmente en **actividades de seguimiento**, medición, análisis, evaluación y auditoría, así como en la **revisión de incidentes**, no conformidades y resultados de control, con el fin de verificar la adecuación de las medidas implantadas y reforzar de forma continuada la eficacia del sistema.

SUARDIAZ Group promoverá la realización de **revisiones y evaluaciones periódicas** del SGSI y de los controles de seguridad de la información por personal o funciones con el grado de independencia adecuado respecto del área o actividad revisada, con el fin de **verificar su adecuación, eficacia y conformidad** con los requisitos aplicables.

6.8 Roles, responsabilidades y autoridades

SUARDIAZ Group asegura que los **roles, responsabilidades y autoridades** relevantes para la seguridad de la información se **asignan**, comunican y **mantienen** de forma coherente con la estructura organizativa y con las necesidades del SGSI. Esta asignación debe permitir asegurar la conformidad del sistema con los requisitos aplicables, la adecuada ejecución de las actividades previstas y el reporte a la Alta Dirección sobre el desempeño del SGSI y sobre las necesidades de mejora que se identifiquen.

La organización promueve que cada persona conozca las **responsabilidades que le resultan aplicables** en materia de seguridad de la información y actúe de acuerdo con ellas, favoreciendo la coordinación entre funciones, la adecuada toma de decisiones y la rendición de cuentas en relación con la protección de la información dentro del alcance definido.

SUARDIAZ Group promoverá que la asignación de roles, responsabilidades y autoridades en materia de seguridad de la información se realice, cuando proceda, bajo criterios de **segregación de funciones**, de forma coherente con la estructura organizativa y con el **organigrama de responsabilidades** definido por la organización, con el fin de reducir riesgos derivados de incompatibilidades, accesos no justificados o concentración de funciones críticas en una misma persona. La segregación de roles se ve reflejada en el Documento de roles y responsabilidades donde se muestra el organigrama oficial de Suardiaz Group.

La presente política constituye el **nivel marco del cuerpo normativo del SGSI**. Su desarrollo se realizará mediante políticas específicas, normas, procedimientos,

guías e información documentada relacionada, que deberán ser coherentes con sus principios y mantenerse formalmente aprobados, vigentes y controlados.

7. COMUNICACIÓN DE LA POLÍTICA

Esta política debe **comunicarse** dentro de la organización **y ponerse a disposición** de las partes interesadas pertinentes cuando corresponda. SUARDIAZ Group determina qué comunicar, a quién, cuándo, por quién y por qué medios, para asegurar su comprensión, aplicación y disponibilidad como información documentada. A nivel externo, la organización garantizará que esta política, o una versión adecuada de la misma cuando proceda, pueda facilitarse a **partes interesadas pertinentes** mediante los **canales formalmente definidos**, ya sea de forma **pública**, **controlada** o **bajo solicitud**, de acuerdo con la naturaleza de la relación, los requisitos aplicables y los criterios de confidencialidad que correspondan.

La comunicación de esta política debe contribuir a que las personas que trabajan bajo el control de la organización **comprendan sus obligaciones** y su contribución a la eficacia del SGSI. Cuando resulte pertinente, también podrá ponerse a disposición de las partes interesadas relevantes como manifestación del compromiso de SUARDIAZ Group con la protección de la información y con el cumplimiento de los requisitos aplicables.

La organización promoverá, asimismo, acciones de **difusión**, **formación** y **concienciación** adecuadas para favorecer el conocimiento de esta política y de las obligaciones derivadas de la misma por parte del personal y, cuando resulte pertinente, de terceros relevantes incluidos en el alcance del SGSI.

8. REVISIÓN, ACTUALIZACIÓN Y CONTROL DE LA POLÍTICA

Esta política debe **revisarse a intervalos planificados** y siempre que se produzcan **cambios relevantes** en el contexto de la organización, en las partes interesadas, en **los requisitos aplicables**, en los **riesgos de seguridad** de la información o en la **operativa del SGSI** que puedan afectar a su conveniencia, adecuación o eficacia. Su actualización, revisión, aprobación, distribución y control se realizará conforme a las **directrices de gestión** de la información documentada del SGSI. En este marco, la documentación del SGSI se gestionará conforme a criterios de **identificación**, **versionado**, **revisión**, **aprobación**, **control de acceso**, **distribución**, **conservación**, **retención** y **disposición final**, asegurando su integridad, disponibilidad, trazabilidad y adecuación durante todo su ciclo de vida.

La revisión de esta política debe considerar, entre otros aspectos, el desempeño del SGSI, la evolución de los riesgos y oportunidades, los resultados de auditoría, la revisión por la dirección y los cambios en el contexto interno y externo o en los requisitos aplicables.

Cualquier excepción a los principios o requisitos derivados de esta política deberá justificarse, evaluarse en función del riesgo asociado, aprobarse por el nivel de responsabilidad que corresponda y, cuando resulte necesario, acompañarse de medidas compensatorias y de un seguimiento específico hasta su cierre o revisión.

Sin perjuicio de las revisiones planificadas, esta política deberá **revisarse cuando se produzcan incidentes relevantes**, **cambios significativos** en la organización, **modificaciones en el alcance** del SGSI, variaciones normativas o contractuales, cambios tecnológicos relevantes o resultados de auditoría y seguimiento que aconsejen su actualización.

9. DOCUMENTACIÓN RELACIONADA

La documentación relacionada con esta política es la información documentada vigente del SGSI que desarrolla, soporta o evidencia su aplicación, incluyendo, según resulte aplicable, la documentación sobre roles y responsabilidades, objetivos de seguridad de la información, análisis de contexto, partes interesadas, comunicación, gestión de riesgos, Declaración de Aplicabilidad y demás políticas o documentos corporativos de seguridad de la información que se encuentren formalmente aprobados, vigentes y controlados.

10. ANEXOS

No hay anexos relacionados con este documento.