					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P01					Título del documento: **Política de Seguridad de la Información**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

1. Propósito

1.1 Esta política establece el compromiso general de la organización con la seguridad de la información mediante la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) formal.

1.2 Proporciona la dirección estratégica y los requisitos fundamentales para proteger la confidencialidad, integridad, disponibilidad y resiliencia de todos los activos de información en entornos físicos, digitales y en la nube.

1.3 Esta política da cumplimiento a las cláusulas 5.1 y 5.2 de ISO/IEC 27001:2022 al expresar la intención de liderazgo, el compromiso de la alta dirección y la alineación de las actividades de seguridad con los objetivos de la organización.

1.4 Actúa como referencia autorizada para todas las políticas, normas y procedimientos subordinados del SGSI y es esencial para habilitar un entorno de seguridad basado en el riesgo, orientado al cumplimiento y sujeto a mejora continua.

2. Alcance

2.1 Esta política aplica a todas las personas, activos y procesos definidos dentro del alcance del SGSI, incluidos:

2.1.1 Todas las unidades de negocio, departamentos, filiales y sucursales.

2.1.2 Empleados, contratistas, personal temporal, consultores y proveedores de servicios externos.

2.1.3 Todos los datos, sistemas de información, aplicaciones, infraestructuras y canales de comunicación.

2.1.4 Todos los entornos físicos, en la nube, remotos e híbridos en los que se traten o consulten datos de la organización.

2.2 Esta política es de obligado cumplimiento para todas las entidades que gestionen información de la organización y aplica a todas las fases del ciclo de vida de la información, desde su creación y transmisión hasta su almacenamiento y eliminación.

2.3 Cualquier exclusión o limitación de este alcance deberá documentarse en la declaración de alcance del SGSI y justificarse con la aprobación formal de la dirección ejecutiva.

3. Objetivos

3.1 Establecer un SGSI alineado con ISO/IEC 27001:2022 y capaz de respaldar la toma de decisiones basada en riesgos en toda la organización.

3.2 Garantizar que los principios de seguridad de confidencialidad, integridad y disponibilidad estén incorporados en todas las actividades, sistemas y relaciones de la organización.

3.3 Habilitar el cumplimiento normativo y contractual mediante la definición de objetivos de seguridad medibles, impulsados por políticas, e integrarlos en las operaciones de la organización.

3.4 Minimizar la probabilidad y el impacto de los incidentes de seguridad de la información mediante controles preventivos, detectivos y correctivos eficaces.

3.5 Impulsar la mejora continua del nivel de madurez de la seguridad de la información mediante indicadores de desempeño definidos, resultados de auditoría y revisiones por la dirección.

3.6 Promover una cultura de responsabilidad, concienciación y resiliencia en la que todas las personas comprendan y ejerzan sus responsabilidades en materia de seguridad.

4. Funciones y responsabilidades

4.1 Dirección ejecutiva

4.1.1 Aprueba y respalda la Política de Seguridad de la Información y el marco del SGSI.

4.1.2 Garantiza la alineación entre los objetivos de seguridad y la estrategia de negocio.

4.1.3 Lidera con el ejemplo y promueve una sólida cultura de seguridad de la información.

4.1.4 Revisa y aprueba los cambios significativos en el alcance del SGSI, el tratamiento de riesgos y la estructura de gobierno.

4.2 Director de Seguridad de la Información (CISO) / Responsable del SGSI

4.2.1 Es responsable del SGSI y mantiene esta política conforme a ISO/IEC 27001.

4.2.2 Dirige la evaluación de riesgos, la implantación de controles y los procesos de mejora continua.

4.2.3 Garantiza la coordinación transversal de las iniciativas de seguridad y supervisa las políticas subordinadas.

4.2.4 Informa a la dirección ejecutiva sobre el estado del SGSI, los incidentes, los resultados de auditoría y las métricas.

4.2.5 Garantiza que las revisiones y actualizaciones de la política se realicen de acuerdo con la sección 9 de este documento.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Frecuencia de revisión

9.1.1 Esta política deberá revisarse al menos una vez al año o cuando se produzca cualquiera de los siguientes supuestos:

9.1.1.1 Cambios significativos en obligaciones legales, regulatorias o contractuales.

9.1.1.2 Cambios materiales en el perfil de riesgo de la organización.

9.1.1.3 Resultados de auditorías internas o externas.

9.1.1.4 Incidentes graves o fallos de control.

9.2 Autoridad y proceso de revisión

9.2.1 El CISO o el Responsable del SGSI designado dirigirá el proceso de revisión.

9.2.2 Los insumos para la revisión deberán incluir:

9.2.2.1 Resultados de auditoría interna.

9.2.2.2 Tendencias de evaluación de riesgos.

9.2.2.3 Cambios en procesos de negocio y tecnología.

9.2.2.4 Desempeño frente a KPI y umbrales de riesgo.

9.2.3 Todas las actualizaciones deberán:

9.2.3.1 Estar sujetas a control de versiones y documentadas.

9.2.3.2 Ser aprobadas por la dirección ejecutiva.

9.2.3.3 Distribuirse a todas las partes afectadas a través de canales oficiales de comunicación.

9.2.3.4 Activar las actualizaciones necesarias de la documentación subordinada y de la formación.

10. Políticas relacionadas y vinculaciones

10.1 Esta política marco está directamente vinculada a las siguientes políticas y marcos de seguridad de la organización:

10.1.1 P2 – Política de funciones y responsabilidades de gobierno: define la estructura de gobierno y la jerarquía de autoridad a las que se hace referencia en este documento.

10.1.2 P3 – Política de uso aceptable: establece las normas de conducta y el tratamiento aceptable de los activos de información.

10.1.3 P4 – Política de control de acceso: operacionaliza los controles de acceso derivados de esta política marco.

10.1.4 P6 – Política de gestión de riesgos: proporciona el contexto basado en riesgos para seleccionar controles y aceptar riesgos residuales.

10.1.5 P33 – Política de auditoría y supervisión del cumplimiento: detalla cómo los mecanismos internos de aseguramiento validan la aplicación de la política.

10.2 Estas interdependencias garantizan una alineación integral y la trazabilidad en todo el SGSI, y respaldan un gobierno unificado de riesgos y cumplimiento.

11. Normas y marcos de referencia

11.1 Esta Política de Seguridad de la Información está formalmente alineada con las siguientes normas y marcos para garantizar el pleno cumplimiento, la preparación para auditorías y la capacidad de respuesta ante requerimientos regulatorios:

11.2 ISO/IEC 27001

11.2.1 Cláusula 5.1 – Liderazgo y compromiso: esta política demuestra el compromiso de la alta dirección con la seguridad de la información y define las responsabilidades y la asignación de recursos para el SGSI.

11.2.2 Cláusula 5.2 – Política de seguridad de la información: este documento constituye la política formal de seguridad de la organización, alineada con los objetivos de seguridad declarados, la estrategia de negocio y el cumplimiento de ISO/IEC 27001.

11.2.3 Cláusula 6.1 – Acciones para abordar riesgos y oportunidades: el enfoque basado en riesgos reflejado en esta política garantiza que los recursos de seguridad se apliquen de forma proporcional a las amenazas.

11.2.4 Cláusula 9.2 – Auditoría interna y cláusula 10 – Mejora: esta política está integrada en el ciclo de mejora continua de la organización y sujeta a validación mediante auditoría interna.

11.2.5 ISO/IEC 27002:2022 – Control 5.1: especifica directrices para establecer y mantener políticas de seguridad. Esta política refleja las recomendaciones de ISO 27002 en materia de documentación jerárquica, ciclos de revisión y exigibilidad.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Política y procedimientos de planificación de la seguridad): esta política cumple el requisito de desarrollar, difundir y revisar una política formal de seguridad de la información aplicable a toda la organización.

11.3.2 PM-1 a PM-5: aborda el gobierno a nivel de programa, incluidas las funciones de seguridad de la información, la asignación de recursos, la estrategia de riesgos y la integración de la planificación de la seguridad en las operaciones de la organización.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 5(2): hace efectivo el principio de responsabilidad proactiva. Esta política define las partes responsables y las acciones de aplicación trazables.

11.4.2 Artículo 24: exige la implantación de medidas técnicas y organizativas, incluidas políticas alineadas con el riesgo.

11.4.3 Artículo 32: respalda la implantación de medidas apropiadas para garantizar la seguridad de los datos personales a lo largo de su ciclo de vida.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(a): obliga a las entidades a implantar una política de seguridad documentada que aborde la gestión de riesgos y el gobierno. Esta política cumple ese requisito y respalda una preparación más amplia en ciberseguridad y la protección de infraestructuras críticas.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 5(2): exige un marco de control interno documentado para la gestión del riesgo de las TIC. Esta política respalda el cumplimiento en el sector financiero mediante la asignación de funciones, controles y mecanismos de supervisión alineados con las expectativas de gobierno de DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Establecimiento del marco de gobierno: esta política respalda el gobierno de la organización al definir las funciones del SGSI, los compromisos de liderazgo y los objetivos estratégicos.

11.7.2 APO01 – Marco de gestión: respalda el establecimiento y la operación de un SGSI estructurado.

11.7.3 APO12 – Gestión de riesgos: proporciona la base para el gobierno del riesgo de seguridad de la información.

11.7.4 MEA01/MEA03 – Supervisar, evaluar y valorar: refuerza la evaluación continua del desempeño y la supervisión del control interno mediante la aplicación del cumplimiento de la política.