Documento de primer nivel del Sistema de Gestión de Seguridad de la Información (SGSI) de VIRTUAL SECURE. Da cumplimiento al requisito 5.2 «Política» de la norma ISO/IEC 27001:2022 y al control A.5.1 «Políticas de seguridad de la información» de su Anexo A. Se emite de forma integrada con la Política de Calidad (SG-DI-PC) del Sistema de Gestión de la Calidad certificado bajo ISO 9001:2015.

1. INTRODUCCIÓN Y PROPÓSITO

VIRTUAL SECURE (razón social Inversiones Virtual Group SpA) es una organización especializada en servicios de ciberseguridad que, en su preocupación por mejorar continuamente sus procesos y con la finalidad de satisfacer plenamente los requerimientos de sus clientes, asume el desafío de establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022.

Siendo la ciberseguridad el objeto mismo del negocio, la protección de la información propia y de la información que los clientes confían a la organización constituye un requisito habilitante de su propuesta de valor y de su reputación como especialista del sector. Los propósitos de la presente Política General de Seguridad de la Información —en adelante también «la Política de Seguridad»— son:

- Gestionar los riesgos de seguridad de los activos de información que soportan la provisión de los servicios comprendidos en el alcance del SGSI.
- Establecer las expectativas de la Alta Dirección respecto del uso correcto que los colaboradores y terceros hagan de los recursos de información de la organización, y de las medidas que deben adoptar para su protección.
- Instalar en todo el personal la necesidad de la seguridad de la información y promover la comprensión de sus responsabilidades individuales.
- Determinar las medidas esenciales que la organización debe adoptar para protegerse de las amenazas que puedan afectar la confidencialidad, la integridad y la disponibilidad de la información.
- Proporcionar a los colaboradores una herramienta que facilite la toma de decisiones apropiadas en situaciones relacionadas con la preservación de la seguridad de la información.
- Constituir el marco de referencia para el establecimiento y la revisión de los objetivos de seguridad de la información.

La materialización de una falla de seguridad puede ocasionar a VIRTUAL SECURE la pérdida o el mal uso de activos de información, la pérdida de imagen como organismo técnico especialista en ciberseguridad, la interrupción total o parcial de los procesos que soportan el negocio y el incumplimiento de obligaciones legales o contractuales con sus clientes.

2. ALCANCE

El cumplimiento de esta Política es obligatorio y alcanza a todo el personal que utiliza los activos de información de VIRTUAL SECURE, así como a los contratistas, proveedores y terceros que presten servicios ligados a la seguridad de la información de la organización.

El alcance del Sistema de Gestión de Seguridad de la Información comprende los siguientes procesos, definidos en el Mapa de Procesos (SG-DI-MP) y declarados en el Alcance del Sistema de Gestión (SG-F-ASGC):

Proceso en el alcance del SGSI	Descripción
Mesa de Servicio — Gestión de Requerimientos	Recepción, registro, categorización, atención, escalamiento y cierre de los requerimientos de servicio de los clientes, incluyendo el resguardo de la información contenida en los tickets y en las plataformas de gestión.
SOC — Gestión de Incidentes de Seguridad de la Información	Monitoreo, detección, análisis, contención, erradicación, recuperación, notificación y aprendizaje de los incidentes de seguridad de la información detectados en los servicios entregados a los clientes.

Contexto operacional determinante

La operación de VIRTUAL SECURE se desarrolla predominantemente en modalidad remota y sobre plataformas SaaS con redundancia geográfica. Esta condición reduce significativamente la cantidad de controles físicos aplicables y desplaza el perímetro de seguridad hacia el puesto de trabajo remoto, la identidad digital y el acceso a las plataformas. En consecuencia, la evaluación y el tratamiento del riesgo del trabajo remoto constituyen un eje prioritario de esta Política y del SGSI. No se consideran dentro del alcance los colaboradores destinados a clientes bajo modalidad de suministro de personal, por no administrar información de VIRTUAL SECURE.

El inventario de activos de información de VIRTUAL SECURE comprende los activos que dan soporte a los procesos del alcance, categorizados por su nivel de criticidad (alta, media y baja), priorizándose los de nivel alto. Los riesgos asociados a dichos activos son tratados mediante los controles del SGSI, conforme a la Declaración de Aplicabilidad.

3. DECLARACIÓN DE LA ALTA DIRECCIÓN

La Alta Dirección de VIRTUAL SECURE declara que la seguridad de la información es un componente esencial de la calidad y de la continuidad de sus servicios, y se compromete a proteger la confidencialidad, la integridad y la disponibilidad de la información propia y de la información que sus clientes le confían, mediante un Sistema de Gestión de Seguridad de la Información basado en riesgos, conforme a la norma ISO/IEC 27001:2022, integrado con el Sistema de Gestión de la Calidad y sometido a mejora continua.

Para ello, la Alta Dirección asume los siguientes compromisos:

- **Adecuación al propósito de la organización:** mantener esta Política apropiada al propósito, al contexto y a la dirección estratégica de VIRTUAL SECURE.
- **Cumplimiento de los requisitos aplicables:** satisfacer los requisitos legales, reglamentarios y contractuales aplicables en materia de seguridad de la información y de protección de datos personales.
- **Marco para los objetivos:** proporcionar el marco de referencia para establecer, medir y revisar los objetivos de seguridad de la información.
- **Provisión de recursos:** asignar los recursos humanos, tecnológicos y financieros necesarios para operar y mejorar el SGSI.
- **Gestión del riesgo:** evaluar y tratar sistemáticamente los riesgos de seguridad de la información, con criterios de aceptación definidos y aprobados.
- **Cultura de seguridad:** promover la concientización, la capacitación y la responsabilidad individual de todos los colaboradores.
- **Mejora continua:** mejorar de forma continua la conveniencia, adecuación y eficacia del SGSI.

4. PRINCIPIOS RECTORES

VIRTUAL SECURE pone énfasis en el cumplimiento de las siguientes directrices, que orientan todas las decisiones y actuaciones en materia de seguridad de la información:

- La información es un activo fundamental para el cumplimiento de los objetivos de la organización y debe protegerse de forma consistente con su importancia, valor y criticidad.
- La seguridad de la información es un atributo necesario de los servicios y productos ofrecidos por la organización, y no un requisito accesorio.

- La seguridad de la información es responsabilidad de todos, con independencia del cargo que se desempeñe y de la modalidad de trabajo.
- La información se clasifica según criterios de valoración vinculados a su importancia para el cumplimiento de los objetivos de la organización. Toda información creada o procesada se considera de uso interno mientras no se determine otro nivel de clasificación.
- Todo colaborador o tercero tiene la obligación de notificar oportunamente cualquier situación, evento o debilidad que afecte o pueda afectar la seguridad de los activos de información.
- La sensibilización, capacitación y entrenamiento en materias de seguridad de la información constituyen una tarea prioritaria y permanente.
- El acceso a la información y a los sistemas se otorga bajo los principios de mínimo privilegio, necesidad de conocer y segregación de funciones, con autenticación reforzada para los accesos remotos y privilegiados.
- De la presente Política se desprende un conjunto de políticas específicas, procedimientos, normas e instructivos, con sus respectivas herramientas de implantación.

5. ROLES Y RESPONSABILIDADES

Rol	Responsabilidades
Gerente General (Alta Dirección)	Aprobar y validar la Política General de Seguridad de la Información y los objetivos del SGSI. Proveer las definiciones estratégicas, lineamientos, prioridades y recursos. Asegurar que las estrategias de control sobre los activos de información sean coherentes con las políticas institucionales. Aceptar formalmente los riesgos residuales. Liderar la Revisión por la Dirección integrada.
Comité del Sistema Integrado de Gestión	Impulsar y proponer las directrices en materia de seguridad de la información. Coordinar las decisiones de seguridad (políticas, normas, análisis de riesgos, continuidad y recuperación ante desastres). Sancionar las políticas específicas, procedimientos e instructivos. Sesionar periódicamente conforme a la planificación anual y levantar acta de los acuerdos. Revisar el desempeño del SGSI y del SGC de forma integrada.
Encargado de Calidad y SGSI (Oficial de Seguridad de la Información)	Mantener actualizada la Política y la documentación del SGSI. Promover su difusión y verificar su aplicación. Coordinar la identificación de activos, la apreciación y el tratamiento de riesgos y la Declaración de Aplicabilidad. Monitorear el avance de la implementación de los controles y el cumplimiento de los objetivos. Coordinar las auditorías internas integradas y el seguimiento de hallazgos. Gestionar la priorización y respuesta a incidentes y riesgos.
Jefe / Analistas del SOC	Monitorear, detectar, analizar y gestionar los incidentes de seguridad de la información en los servicios entregados a los clientes, conforme a los procedimientos establecidos. Registrar la evidencia, notificar oportunamente y aportar las lecciones aprendidas al proceso de mejora.
Mesa de Servicio	Gestionar los requerimientos de los clientes resguardando la confidencialidad, integridad y disponibilidad de la información contenida en los tickets y plataformas. Derivar al SOC todo requerimiento que constituya o pueda constituir un evento o incidente de seguridad.
Colaboradores	Conocer, comprender y cumplir la presente Política y las políticas específicas derivadas. Proteger los activos de información y las credenciales asignadas. Reportar eventos, incidentes y debilidades de seguridad. Participar en las actividades de concientización y capacitación.
Terceras partes (proveedores, contratistas, consultores, auditores externos, personal temporal)	Cumplir las obligaciones de seguridad de la información establecidas en los contratos, acuerdos de confidencialidad y niveles de servicio acordados con VIRTUAL SECURE, y someterse a la evaluación y seguimiento definidos por la organización.

6. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información se realiza mediante un proceso sistemático, documentado y conocido por toda la organización, basado en la norma ISO/IEC 27001:2022. El cumplimiento de los objetivos del SGSI se sustenta en el análisis de riesgos sobre los procesos del alcance, lo que implica llevar a cabo, junto a los responsables de cada proceso, las siguientes actividades esenciales:

1. Identificar los activos de información críticos que intervienen en la operación de los procesos del alcance —información digital, plataformas, personas e infraestructura— y mantenerlos catalogados y clasificados en el inventario de activos.
2. Realizar la apreciación y el tratamiento de los riesgos conforme a la metodología vigente, definiendo los controles necesarios para mitigarlos, con especial atención a los riesgos derivados del trabajo remoto, del acceso a plataformas SaaS y de la dependencia de proveedores de servicio.
3. Determinar los controles aplicables del Anexo A de la norma, justificar las inclusiones y exclusiones y mantener actualizada la Declaración de Aplicabilidad con la evidencia que respalda cada control.
4. Difundir de forma planificada los objetivos de seguridad de la información, sus características y las responsabilidades individuales, integrando estas actividades al plan anual de capacitación y al proceso de inducción del nuevo personal.
5. Establecer, mantener y probar los planes de continuidad del negocio (BCP) y de recuperación ante desastres (DRP) del servicio SOC, incluidos los procedimientos manuales de continuidad ante caídas de plataformas o cortes generales de conectividad.
6. Medir, analizar y evaluar el desempeño del SGSI mediante los indicadores definidos, las auditorías internas integradas y la Revisión por la Dirección, y gestionar las no conformidades y acciones de mejora conforme al procedimiento único del Sistema Integrado de Gestión.

7. POLÍTICAS ESPECÍFICAS DERIVADAS

De la presente Política General se derivan las siguientes políticas específicas, cuyo desarrollo, aprobación y mantención corresponde al Comité del Sistema Integrado de Gestión, y cuya aplicabilidad se determina en la Declaración de Aplicabilidad:

Política específica	Control Anexo A ISO/IEC 27001:2022
Política de clasificación y manejo de activos de información	A.5.9 · A.5.10 · A.5.12 · A.5.13
Política de control de acceso, identidad y autenticación	A.5.15 · A.5.16 · A.5.17 · A.5.18 · A.8.2 · A.8.5
Política de seguridad para el trabajo remoto y dispositivos móviles	A.6.7 · A.8.1
Política de uso aceptable de los recursos de información	A.5.10 · A.8.1
Política de seguridad en la relación con proveedores y servicios en la nube	A.5.19 · A.5.20 · A.5.21 · A.5.22 · A.5.23
Política de gestión de incidentes de seguridad de la información	A.5.24 · A.5.25 · A.5.26 · A.5.27 · A.5.28
Política de continuidad del negocio y recuperación ante desastres	A.5.29 · A.5.30 · A.8.13 · A.8.14
Política de respaldo y recuperación de la información	A.8.13
Política de gestión de vulnerabilidades técnicas y configuración segura	A.8.8 · A.8.9 · A.8.19 · A.8.20 · A.8.21
Política de registro, monitoreo y protección de la evidencia	A.8.15 · A.8.16 · A.5.28
Política de seguridad en recursos humanos y concientización	A.6.1 · A.6.2 · A.6.3 · A.6.4 · A.6.5 · A.6.6
Política de protección de la información personal y cumplimiento legal	A.5.31 · A.5.32 · A.5.33 · A.5.34 · A.5.36

8. INTEGRACIÓN CON EL SISTEMA DE GESTIÓN DE LA CALIDAD

El SGSI de VIRTUAL SECURE opera de forma integrada con el Sistema de Gestión de la Calidad certificado bajo la norma ISO 9001:2015. En consecuencia, se mantienen comunes y unificados: el análisis del contexto de la organización (SG-F-ACP y SG-F-AF), la identificación de partes interesadas y sus requisitos (SG-F-ICR), el alcance del sistema (SG-F-ASGC), el mapa de procesos (SG-DI-MP), la estructura y el control de la documentación, el programa y la ejecución de las auditorías internas, la Revisión por la Dirección y el tratamiento de no conformidades, acciones correctivas y oportunidades de mejora.

Se mantienen diferenciados, por tratar materias distintas, los objetivos de calidad y los objetivos de seguridad de la información, así como la metodología de apreciación y tratamiento de riesgos de seguridad de la información, que es específica del SGSI.

9. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información derivan de la presente Política, de los requisitos aplicables y de los resultados de la apreciación y el tratamiento de riesgos. Son medibles, se comunican, se someten a seguimiento y se actualizan cuando corresponde. Sus indicadores, metas para el período 2026 – 2028, responsables, recursos, plazos y método de evaluación se establecen en el registro

SG-F-OSIG Objetivos del Sistema Integrado de Gestión, hoja «Objetivos de Seguridad de la Información», conforme al requisito 6.2 de la norma ISO/IEC 27001:2022, y se mantienen disponibles como información documentada.

10. COMUNICACIÓN, REVISIÓN E INCUMPLIMIENTO

Aspecto	Definición
Difusión interna	La presente Política debe ser conocida por todos los colaboradores de VIRTUAL SECURE. Se comunica por correo electrónico, se publica en el repositorio documental del Sistema Integrado de Gestión y en formato afiche en las dependencias de la organización, y se incorpora al proceso de inducción del nuevo personal y a los acuerdos con terceros.
Disponibilidad externa	Se publica en el sitio web institucional (virtualsecure.cl) y se pone a disposición de clientes, proveedores y demás partes interesadas pertinentes que la soliciten.
Revisión	El Comité del Sistema Integrado de Gestión revisa y evalúa esta Política al menos una vez al año en la Revisión por la Dirección, y adicionalmente cuando se produzcan cambios significativos en el contexto, el alcance, la estructura organizacional, la tecnología, los requisitos legales o el perfil de riesgo, con el fin de asegurar su vigencia, conveniencia, adecuación y eficacia.
Incumplimiento	El incumplimiento de esta Política y de las políticas específicas derivadas se trata conforme al Reglamento Interno de Orden, Higiene y Seguridad, a la legislación laboral vigente y a las cláusulas contractuales aplicables a proveedores y terceros, sin perjuicio de las acciones legales que correspondan.

11. DEFINICIONES

Término	Definición
Confidencialidad	Propiedad por la cual la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
Integridad	Propiedad de exactitud y completitud de la información; la información está correcta y libre de corrupción o alteración no autorizada.
Disponibilidad	Propiedad de ser accesible y utilizable, en forma oportuna, por una entidad autorizada que lo requiera.
Activo de información	Todo elemento relevante en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la organización: la información en cualquier formato, las plataformas e infraestructura que la soportan y las personas que la utilizan y conocen los procesos.
Amenaza	Causa potencial de un incidente no deseado que puede resultar en daño a un sistema u organización.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.
Riesgo	Efecto de la incertidumbre sobre los objetivos; combinación de la probabilidad de ocurrencia de un evento y de sus consecuencias.
Evento de seguridad de la información	Ocurrencia identificada del estado de un sistema, servicio o red que indica una posible falla de la política de seguridad, una falla de los controles o una situación previamente desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de la información	Evento o serie de eventos de seguridad de la información con probabilidad significativa de comprometer las operaciones de la organización y de amenazar la seguridad de la información.
Declaración de Aplicabilidad (DdA)	Documento que identifica los controles del Anexo A de la norma ISO/IEC 27001:2022 aplicables al SGSI, su justificación de inclusión o exclusión, su estado de implementación y la evidencia que lo respalda.
Terceras partes	Proveedores de servicios y de red, servicios de asesoría, outsourcing de operaciones, consultores, auditores externos, proveedores de software y servicios de información, personal temporal y cualquier persona natural o jurídica externa que acceda a los activos de información de la organización.

12. DOCUMENTOS DE REFERENCIA Y CONTROL DE CAMBIOS

Código	Documento
—	ISO/IEC 27001:2022 — Sistemas de gestión de seguridad de la información. Requisitos.
—	ISO/IEC 27002:2022 — Controles de seguridad de la información.
—	ISO 9001:2015 — Sistemas de gestión de la calidad. Requisitos.
SG-DI-PC	Política de Calidad de Virtual Secure.
SG-DI-MP	Mapa de Procesos del Sistema Integrado de Gestión.
SG-F-ASGC	Alcance del Sistema de Gestión.
SG-F-ACP / SG-F-AF	Análisis de Contexto PESTEL / Análisis FODA.
SG-F-ICR	Identificación de Clientes, Partes Interesadas y sus Requisitos.
SG-F-OSIG	Objetivos del Sistema Integrado de Gestión (Calidad y Seguridad de la Información).

Versión	Fecha	Motivo de la revisión	Detalle del cambio
1.0	25-09-2026	Creación del documento	Emisión inicial de la Política General de Seguridad de la Información de VIRTUAL SECURE, en el marco de la implementación del SGSI bajo ISO/IEC 27001:2022 y de su integración con el Sistema de Gestión de la Calidad certificado bajo ISO 9001:2015. Elaborada conforme a los acuerdos de las Actas N° 001 (06-09-2026) y N° 002 (17-09-2026) del proyecto de certificación integrada.

ELABORADO POR	REVISADO POR	APROBADO POR
Luis Miguel Cárdenas Beltrán Consultor / Auditor SIG — Proceso Empresa	**Encargado de Calidad y SGSI** Virtual Secure	**Sergio Andrés Pérez Sepúlveda** Gerente General — Virtual Secure