Política de Seguridad de la Información

SGSI

Versión: 2.0

Fecha de publicación: 30 de junio de 2026

Prado Norte 325-A, Lomas de Chapultepec III Sección, Miguel Hidalgo, CP 11000, CDMX
www.invested.mx

1.OBJETIVOS DE LA POLÍTICA

Invested ha definido objetivos generales de la política de seguridad de la información, siendo éstos son:

Se identifican y minimizan la exposición a riesgos y amenazas gracias a la implementación de controles, protocolos, y monitorización de procesos, logrando reducir el número de amenazas. En caso de que se produzca un incidente que afecte a los activos declarados en el alcance del SGSI, Invested estará preparado para actuar de forma inmediata minimizando su impacto.

Desarrollar y promover una cultura de seguridad de la información, enfocada a que todas las actividades realizadas sean seguras y que todo el personal esté consciente de los riesgos y amenazas existentes, capacitándose en los medios y métodos correctos para salvaguardar los activos de la organización y de nuestros clientes.
Desarrollar los lineamientos, políticas y controles a través de una correcta evaluación del SGSI.

2. ALCANCE

Esta política aplica a:

- Toda la información propiedad de Invested o bajo su custodia, en cualquier formato o medio.

- Todos los colaboradores, prestadores de servicios, consultores y terceros con acceso a la información o sistemas de Invested.

- Todos los sistemas, plataformas, infraestructuras tecnológicas, servicios en la nube, procesos, aplicaciones, equipos y operaciones relacionados con el tratamiento de información de clientes y de la organización.

El cumplimiento de esta política es obligatorio y transversal a todas las áreas de la empresa.

3.GLOSARIO

Para efectos de esta política se entenderá por:

- **SGSI:** Sistema de Gestión de la Seguridad de la Información.

- **Información:** Datos en cualquier formato, medio o sistema.
- **Confidencialidad:** Garantía de que la información solo es accesible a personas autorizadas.
- **Integridad:** Asegurar que la información se mantiene exacta, completa y sin alteraciones no autorizadas.
- **Disponibilidad:** Acceso oportuno a la información cuando es requerida.
- **Incidente de seguridad:** Evento o situación que compromete o puede comprometer la seguridad de la información.
- **Partes interesadas:** Empleados, proveedores, consultores, clientes u otros actores relevantes para el SGSI.

4.RESPONSABLES

CEO

- Aprobar esta política y sus actualizaciones.
- Asignar recursos necesarios para su implementación.
- Delegar funciones relacionadas con la gestión del SGSI cuando corresponda.

CISO

- Elaborar, mantener y actualizar esta política.
- Evaluar y promover mejoras al SGSI.
- Asegurar la implementación de controles y mecanismos de monitoreo.
- Evaluar el cumplimiento de la política mediante auditorías y revisiones.
- Coordinar y supervisar las acciones derivadas de incidentes de seguridad.
- Formalizar responsabilidades y promover la mejora continua del SGSI.
- Asegurar el cumplimiento general del marco de seguridad en la organización.

Todos los Colaboradores

- Conocer y cumplir las políticas, lineamientos y procedimientos.
- Proteger la información a la que tienen acceso.
- Reportar cualquier incumplimiento o incidente de seguridad.
- Participar en la capacitación correspondiente a su rol.

Partes Interesadas Externas

- Actuar conforme a las obligaciones contractuales y a las políticas del SGSI aplicables a su relación con Invested.

5. LINEAMIENTOS

5.1 Compromiso de Seguridad

Invested adopta un enfoque preventivo y proactivo para identificar, evaluar y tratar los riesgos de seguridad de la información. La organización sólo acepta riesgos que estén documentados, controlados y dentro del nivel tolerable definido en su metodología de gestión de riesgos.

5.2 Protección de la Información

La información propiedad o bajo custodia de Invested se protege frente a accesos, modificaciones, divulgaciones o destrucciones no autorizadas. La protección aplica a todos los formatos y medios: digitales, físicos y audiovisuales.

5.3 Confidencialidad

Se implementan medidas para asegurar la confidencialidad de la información, con especial énfasis en los datos personales de colaboradores y clientes. Los controles incluyen, entre otros: autenticación, autorización, cifrado y segregación de funciones.

5.4 Integridad

La integridad de la información se mantiene conforme a su nivel de clasificación. Invested protege los datos contra alteraciones no autorizadas mediante controles técnicos, administrativos y procedimentales.

5.5 Disponibilidad

Los servicios críticos se mantienen operativos conforme a las necesidades del negocio. Para ello, Invested cuenta con planes de continuidad y contingencia que se mantienen actualizados y se prueban al menos una vez al año.

5.6 Autenticación y Autorización

Solo usuarios debidamente autenticados y autorizados acceden a sistemas, servicios, bases de datos y plataformas de Invested. La autenticación incluye

contraseñas, tokens, certificados digitales, MFA u otros mecanismos adecuados.

5.7 Auditoría y Monitoreo

Se registran y supervisan los eventos relevantes relacionados con el uso de sistemas, accesos y actividades críticas del entorno tecnológico. Los registros se utilizan para identificar accesos válidos, accesos denegados, anomalías o acciones sospechosas, y como evidencia para auditorías o investigaciones de incidentes.

5.8 Capacitación y Concientización

Todos los colaboradores reciben capacitación continua sobre seguridad de la información, conforme a sus roles y responsabilidades. Los roles críticos reciben formación especializada.

5.9 Cumplimiento Normativo

Invested cumple con todas las leyes, regulaciones, normas y obligaciones contractuales aplicables en materia de seguridad de la información y protección de datos personales.

5.10 Gestión de Incidentes

Todo incidente real o potencial se reporta al CISO para su análisis, registro, investigación y seguimiento conforme a procedimientos establecidos