



Política de seguridad de la información para proveedores

Sistema de Gestión de Seguridad de la Información

Empresa	Ingeniería AT S.A.S. - IAT
Código	IAT-SGSI-POL-002
Versión	1.0
Fecha de emisión	1 de octubre de 2026
Clasificación	Uso interno
Próxima revisión	Octubre de 2027 o ante cambios significativos

Actividad	Responsable	Cargo	Fecha
Elaboró	Carlos Andrés Angarita Tavera	Co-fundador	01/10/2026
Revisó	Jorge Luis Angarita Tavera	Gerente Técnico	Pendiente
Aprobó	Alta Dirección	Representante legal	Pendiente

Estado del documento: BORRADOR PARA REVISIÓN Y APROBACIÓN



Control de cambios

Versión	Fecha	Descripción	Responsable
1.0	01/10/2026	Emisión inicial para implementación del SGSI de IAT.	Responsable SGSI

Propósito de la política

Ingeniería AT S.A.S. reconoce que la información propia y la confiada por clientes, aliados y demás partes interesadas es un activo esencial. Esta política establece los requisitos mínimos de seguridad que deben cumplir los proveedores y subcontratistas durante todo el ciclo de la relación comercial, de acuerdo con los riesgos del servicio y con el Sistema de Gestión de Seguridad de la Información de IAT.

Objetivo

Proteger la confidencialidad, integridad, disponibilidad y privacidad de la información a la que accedan los proveedores, y asegurar que los servicios contratados se presten bajo controles proporcionales al riesgo, requisitos legales y obligaciones contractuales de IAT.

Alcance

Aplica a todos los proveedores, contratistas, consultores, aliados, operadores de servicios en la nube y terceros que suministren bienes o servicios a IAT, especialmente cuando accedan, almacenen, transmitan, procesen o administren información, activos tecnológicos, credenciales, instalaciones virtuales o servicios de IAT o de sus clientes.

Los requisitos serán incorporados, según corresponda, en la selección, evaluación, contratación, seguimiento, renovación y terminación de la relación con el proveedor.

Referencias y requisitos aplicables

- ISO/IEC 27001:2022 y su Enmienda 1:2024, especialmente los controles relacionados con proveedores, servicios en la nube y seguridad de la información.
- ISO/IEC 27002:2022 como guía para la implementación de controles.
- Ley 1581 de 2012, Decreto 1074 de 2015 y demás disposiciones colombianas aplicables a la protección de datos personales.
- Contratos, acuerdos de confidencialidad, ofertas, órdenes de compra, requisitos de clientes y demás compromisos asumidos por IAT.

Definiciones

Término	Definición
Información confidencial	Información no pública cuya divulgación, alteración, pérdida o indisponibilidad puede afectar a IAT, sus clientes o terceros.
Incidente de seguridad	Evento que compromete o puede comprometer la confidencialidad, integridad, disponibilidad o privacidad de la información.
Proveedor crítico	Tercero cuya falla, acceso privilegiado o tratamiento de información puede causar un impacto significativo en los servicios u objetivos de IAT.
Subcontratista	Tercero utilizado por un proveedor para ejecutar total o parcialmente un servicio contratado.
SGSI	Sistema de Gestión de Seguridad de la Información de IAT.



Principios de aplicación

- Los controles exigidos serán proporcionales al riesgo y al tipo de información involucrada.
- El acceso se limitará a la necesidad del servicio, con privilegios mínimos y autorización previa.
- La información solo podrá usarse para el propósito contratado.
- El proveedor seguirá siendo responsable por las actuaciones de su personal y de los subcontratistas autorizados.
- IAT podrá solicitar evidencias razonables y verificar el cumplimiento de los requisitos acordados.

Lineamientos de seguridad

Protección y uso autorizado de la información

El proveedor debe proteger la información de IAT y de sus clientes contra acceso, uso, modificación, divulgación, destrucción o pérdida no autorizados. No podrá copiarla, transferirla, publicarla ni utilizarla para fines distintos al servicio contratado sin autorización escrita de IAT.

- Aplicar controles físicos, técnicos y administrativos acordes con la clasificación de la información y el riesgo.
- Mantener acuerdos de confidencialidad vigentes con las personas que participen en el servicio.
- Separar la información de IAT de la de otros clientes cuando el servicio o el riesgo lo requiera.
- Evitar el almacenamiento en cuentas personales, dispositivos no autorizados o servicios públicos no aprobados.

Acceso a sistemas, servicios y datos

- Todo acceso debe estar autorizado, asociado a una identidad individual y limitado a las funciones necesarias.
- Se prohíbe compartir credenciales. Los accesos privilegiados deberán utilizar controles reforzados y, cuando sea técnicamente viable, autenticación multifactor.
- El proveedor notificará inmediatamente los cambios, retiros o sustituciones de personal que requieran revocación o modificación de accesos.
- Al terminar el servicio, todos los accesos deberán revocarse y los activos de autenticación deberán devolverse o eliminarse.
- El acceso remoto deberá utilizar canales seguros aprobados por IAT, limitarse al tiempo necesario y quedar sujeto a registro y monitoreo cuando aplique.

Equipos, software y trabajo remoto

- Usar software licenciado, soportado y actualizado, con protección contra código malicioso y bloqueo automático de sesión.
- Cifrar los dispositivos portátiles y medios removibles que almacenen información confidencial, cuando aplique.
- Impedir el acceso de personas no autorizadas durante el trabajo remoto y mantener prácticas de pantalla y escritorio limpios.
- No conectar dispositivos ni instalar herramientas en activos de IAT sin autorización.
- Reportar de inmediato la pérdida, robo o compromiso de cualquier dispositivo que contenga o permita acceder a información de IAT.

Seguridad de servicios en la nube

Cuando el proveedor utilice o suministre servicios en la nube, deberá identificar la ubicación y condiciones de tratamiento de la información, aplicar controles de identidad y acceso, mantener registros suficientes, proteger la información durante la transmisión y el almacenamiento, y acordar mecanismos de respaldo, continuidad, portabilidad y salida del servicio. Ningún cambio de ubicación, subprocesador o condición material podrá realizarse cuando afecte los requisitos contractuales sin informar y obtener las autorizaciones aplicables.



Gestión de vulnerabilidades y cambios

- Mantener un proceso para identificar, evaluar y corregir vulnerabilidades relevantes dentro de plazos acordes con su criticidad.
- Aplicar parches y actualizaciones de seguridad de forma controlada.
- Evaluar y autorizar los cambios que puedan afectar la seguridad, disponibilidad o integridad del servicio.
- Comunicar oportunamente a IAT los cambios significativos, obsolescencias o riesgos que puedan afectar el servicio contratado.

Respaldo, continuidad y recuperación

- Mantener respaldos cuando sean necesarios para cumplir los niveles de servicio y requisitos de recuperación.
- Proteger los respaldos contra acceso, alteración y pérdida, y probar periódicamente su restauración.
- Contar con medidas de continuidad y recuperación proporcionales a la criticidad del servicio.
- Participar en pruebas de continuidad o recuperación solicitadas por IAT cuando el servicio contratado sea crítico.

Gestión de incidentes de seguridad

El proveedor notificará a IAT, sin demora indebida y dentro del plazo contractual aplicable, cualquier incidente real o sospechado que pueda afectar la información, los servicios o los activos relacionados con IAT o sus clientes. Cuando no exista un plazo contractual específico, la notificación inicial deberá realizarse tan pronto como se confirme una afectación o riesgo razonable.

- Preservar evidencias y registros pertinentes.
- Entregar información suficiente sobre naturaleza, alcance, datos afectados, impacto, acciones de contención y plan de recuperación.
- Cooperar con la investigación, comunicaciones y obligaciones legales o contractuales de IAT.
- Implementar acciones correctivas y aportar el análisis de causa cuando sea requerido.
- No realizar comunicaciones públicas relacionadas con el incidente sin autorización, salvo obligación legal.

Protección de datos personales

Cuando trate datos personales por cuenta de IAT, el proveedor actuará únicamente conforme a las instrucciones autorizadas, aplicará medidas de seguridad apropiadas, garantizará la confidencialidad, apoyará la atención de consultas o reclamos y cumplirá la normativa colombiana aplicable. Las transferencias, transmisiones internacionales y el uso de subencargados requerirán las condiciones y autorizaciones correspondientes.

Subcontratación

El proveedor no podrá delegar actividades que impliquen acceso a información o servicios críticos sin cumplir las condiciones contractuales y obtener la autorización requerida. Deberá trasladar a sus subcontratistas obligaciones equivalentes de seguridad, confidencialidad, privacidad, continuidad, notificación de incidentes y derecho de verificación. El proveedor principal conservará la responsabilidad integral frente a IAT.

Retención, devolución y eliminación

La información se conservará únicamente durante el tiempo necesario para el servicio o por obligación legal. Al finalizar la relación, o cuando IAT lo solicite, el proveedor devolverá o eliminará de manera segura la información y sus copias, incluidos respaldos cuando resulte técnicamente posible, y entregará evidencia o certificación de la disposición realizada. Las excepciones legales deberán informarse y mantenerse protegidas.

Evaluación y seguimiento de proveedores

IAT clasificará a los proveedores según la criticidad del servicio, el acceso a información, la dependencia operativa y el impacto potencial. Antes de la contratación y durante la relación, podrá solicitar evidencias tales como políticas,



certificaciones, informes independientes, resultados de pruebas, cuestionarios, planes de continuidad o acciones de mejora.

Nivel	Criterio orientador	Seguimiento mínimo
Alto	Acceso privilegiado, datos sensibles, nube crítica o dependencia operativa significativa.	Evaluación previa, requisitos contractuales específicos, evidencias periódicas y reevaluación al menos anual.
Medio	Acceso limitado a información interna o impacto operativo moderado.	Evaluación previa y reevaluación según riesgo o cambios relevantes.
Bajo	Sin acceso relevante a información ni dependencia operativa significativa.	Validación comercial y aceptación de obligaciones básicas de confidencialidad y seguridad.

Derecho de verificación

IAT podrá revisar el cumplimiento de los requisitos de seguridad mediante solicitudes documentales, reuniones, auditorías acordadas o evaluaciones técnicas razonables. Estas actividades respetarán la confidencialidad, propiedad intelectual y continuidad operativa del proveedor. Los hallazgos deberán tratarse mediante planes de acción con responsables y fechas definidas.

Incumplimiento

El incumplimiento será evaluado según su gravedad, recurrencia e impacto. IAT podrá requerir acciones correctivas, restringir accesos, suspender actividades, aplicar medidas contractuales o terminar la relación, sin perjuicio de las acciones legales correspondientes.

Roles y responsabilidades

Rol	Responsabilidad principal
Alta Dirección	Aprobar la política y asegurar los recursos necesarios para su aplicación.
Responsable del SGSI	Mantener la política, apoyar la evaluación de riesgos y supervisar el cumplimiento.
Responsable del contrato	Definir requisitos, verificar evidencias, reportar cambios y evaluar el desempeño del proveedor.
Usuarios y personal de IAT	Cumplir esta política y reportar incidentes o incumplimientos.
Proveedor	Cumplir las obligaciones, conservar evidencias y comunicar oportunamente incidentes y cambios relevantes.

Comunicación y aceptación

La política será comunicada a los proveedores según su aplicabilidad y formará parte de los requisitos contractuales o documentos de aceptación correspondientes. El responsable del contrato conservará evidencia de su comunicación y aceptación.

Revisión y mejora

La política se revisará al menos una vez al año y también cuando existan cambios significativos en el contexto, los riesgos, la tecnología, la legislación, los servicios contratados o los requisitos de clientes. Las modificaciones deberán seguir el control documental del SGSI.