

POLÍTICA DE RELACIÓN CON PROVEEDORES



Código: GAL-GSI-POL-89

PREPARADO		REVISADO	APROBADO
CARGO	Profesional Sistemas de Gestión	Vicepresidente de Operaciones	Presidente
NOMBRE	Johnnifer Moreno	Zulma Urbano	Carley Urbano
FECHA	8 Septiembre 2025	17 Octubre 2025	17 Octubre 2025

1. OBJETIVO

Establecer directrices y controles para garantizar que la relación con los proveedores cumpla con los estándares de seguridad de la información y promueva la confidencialidad, integridad y disponibilidad de los activos de información compartidos con ellos. Esta política busca asegurar que los proveedores cumplan con los requisitos de seguridad establecidos por la organización y que se establezcan medidas para proteger la información y mitigar los riesgos asociados a la relación con proveedores.

2. ALCANCE

Esta política se aplica a todos los usuarios que interactúan con proveedores críticos en nombre de la organización. Incluye todas las etapas del ciclo de relación con proveedores, desde la selección y contratación hasta la terminación de la relación.

3. DEFINICIONES

- **Proveedor:** Compañías y/o persona que atiende las necesidades específicas (tangibles o intangibles) de la organización.
- **Proveedor Crítico:** Compañía y/o persona que en su relación contractual con Grow Data tiene acceso a información sensible o confidencial, manipula o almacena datos críticos de la compañía o de terceros.

4. ROLES Y RESPONSABILIDADES

Alta dirección

La alta dirección es responsable de establecer una cultura de seguridad de la información en la relación con proveedores. Deben definir los requisitos de seguridad que deben cumplir los proveedores y garantizar que se implementen los controles adecuados para proteger la información compartida.

Responsables de compras y adquisiciones

Son responsables de evaluar y seleccionar proveedores que cumplan con los requisitos de seguridad establecidos (cuando aplique) por la organización. Deben asegurarse de incluir cláusulas de seguridad en los contratos y acuerdos con los proveedores críticos.

Equipo de seguridad de la información

Es responsable de evaluar y aprobar la seguridad de la información de los proveedores críticos antes de su contratación. Deben establecer criterios de evaluación, realizar auditorías y evaluaciones de riesgos, y supervisar el cumplimiento de los proveedores críticos con las políticas de seguridad.

Usuarios

Son responsables de colaborar con los responsables de compras y adquisiciones para identificar los requisitos de seguridad de la información necesarios. Deben informar cualquier incidente de seguridad relacionado con los proveedores y seguir los procedimientos establecidos para proteger la información compartida.

Auditoría Interna

- Realizar auditorías periódicas para verificar el cumplimiento de la **GAL-GSI-POL-89_POLÍTICA DE RELACIÓN CON PROVEEDORES**.
- Evaluar la eficacia de la **GAL-GSI-POL-89_POLÍTICA DE RELACIÓN CON PROVEEDORES** y proponer mejoras o ajustes necesarios.

5. DIRECTRICES

- ✓ En el proceso de selección del tercero se deben establecer criterios que permitan verificar la experiencia, competencia, capacidad y reconocimiento en el medio.
- ✓ El SGSI debe evaluar la aplicación de estándares de Seguridad de la información y la privacidad, dando cumplimiento de la normatividad vigente y los demás establecidos por **Grow Data**. Se debe aplicar mecanismos de control que permitan asegurar el cumplimiento de lo dispuesto en el **GAL-GSI-FOR-33_FORMATO DE VERIFICACIÓN DE CUMPLIMIENTO EN SEGURIDAD DE LA INFORMACIÓN DE TERCEROS-PROVEEDORES** durante y después de la ejecución del contrato o convenio.
- ✓ El responsable de la compra, contrato o convenio deberá socializar al Profesional de Seguridad de la información y la privacidad el alcance y objeto de esta, con el fin de identificar y establecer acciones para mitigar los riesgos de seguridad con referencia al acceso por parte del tercero a los activos de información de la organización, así mismo, deberá realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y reportar los eventos e incidentes de Seguridad de la información y la privacidad.
- ✓ El equipo Jurídico en todo contrato o convenio con terceros, se debe incluir una causal de terminación inmediata de este, por el incumplimiento de las políticas y requerimientos de Seguridad de la información y la privacidad, las cuales deben ser comunicadas antes del inicio de labores y aceptadas mediante la firma del **GAL-GSI-FOR-33_FORMATO DE VERIFICACIÓN DE CUMPLIMIENTO EN SEGURIDAD DE LA INFORMACIÓN DE TERCEROS-PROVEEDORES**.
- ✓ Todo contrato celebrado con un proveedor crítico o tercero que suministre productos y servicios de tecnología de la información y comunicaciones, requerido para el desarrollo de las labores establecidas dentro del alcance del SGSI, y que pueda acceder, procesar, almacenar, comunicar o suministrar información de **Grow Data**, debe incluir como mínimo los

requerimientos de seguridad referenciados en el **GAL-GSI-FOR-33_ FORMATO DE VERIFICACIÓN DE CUMPLIMIENTO EN SEGURIDAD DE LA INFORMACIÓN DE TERCEROS-PROVEEDORES**.

- ✓ Aceptar que **Grow Data** pueda en cualquier momento con previa notificación, realizar revisiones o requerimientos de documentación de forma directa o a través de un tercero, con el fin de verificar el nivel de seguridad del servicio contratado o la solicitud de documentación donde un tercero certifique el cumplimiento en cuanto a Seguridad de la información y la privacidad.
- ✓ Reportar todo incidente de Seguridad de la información y la privacidad y propiedad de **Grow Data** al siguiente correo incidentes.seguridadinformacion@growdata.com.co de manera oportuna, con el fin de ejecutar su remediación y minimizar cualquier impacto para la organización.
- ✓ Aceptar y cumplir lo dispuesto en el **GAL-GSI-FOR-33_ FORMATO DE VERIFICACIÓN DE CUMPLIMIENTO EN SEGURIDAD DE LA INFORMACIÓN DE TERCEROS-PROVEEDORES** para terceros.
- ✓ Cumplir con los acuerdos de niveles de servicio contratados.
- ✓ Cumplir con las políticas de Seguridad de la información y la privacidad de **Grow Data** que se consideren relevantes para el tipo de contrato.

Cadena de suministro de tecnología de información y comunicación

Anualmente se realiza una evaluación a los proveedores para validar el cumplimiento de la cadena de suministro y el cumplimiento de los acuerdos contractuales.

Gestión de la prestación de servicios de proveedores

Los proveedores críticos que prestan servicios de TI deben ser identificados y sus servicios deben ser monitoreados, para asegurar el cumplimiento contractual acordado.

Gestión de cambios en los servicios de los proveedores

Todo cambio que impacte el suministro de servicios de los proveedores involucrados en el alcance del SGSI y que tenga repercusiones en la infraestructura tecnológica de **Grow Data**, deberá ser gestionado dando cumplimiento a lo establecido en la **SIG-GSI-POL-09_ POLÍTICA PLANIFICACIÓN DE LOS CAMBIOS DEL SGSI**.

6. CAPACITACIÓN Y CONCIENTIZACIÓN

La organización debe proporcionar capacitación y concientización regular a los usuarios involucrados en la relación con proveedores. Esto incluye la comprensión de los requisitos de seguridad establecidos, la identificación de riesgos asociados a los proveedores y las mejores prácticas para proteger la información durante la

relación con proveedores. Además, se deben proporcionar actualizaciones periódicas sobre cambios en los requisitos de seguridad y buenas prácticas en la relación con proveedores.

7. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada y actualizada anualmente o en respuesta a cambios significativos en el entorno de amenazas, normativas, o en la estrategia de negocio de **Grow Data**.

8. DISCIPLINARIOS

El incumplimiento de esta política puede resultar en sanciones disciplinarias que podrían incluir en la terminación del empleo, en faltas graves y/o acciones legales.

9. CONTROL DE CAMBIOS

Versión	Fecha	Tipo de modificación	Descripción de los cambios
1.0	11/10/2024	N.A.	Creación
2.0	17/10/2025	Modificación	*Se etiqueto el documento con el tipo de clasificación de la información, en el pie de página. *Se ajusto el código del documento, dado a que se codifico a otro proceso.