

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



Código: SIG-GSI-POL-29

	PREPARADO	REVISADO	APROBADO
CARGO	Profesional Sistemas de Gestión	Vicepresidente de Operaciones	Presidente
NOMBRE	Johnnifer Moreno	Zulma Urbano	Carley Urbano
FECHA	8 Septiembre 2025	15 Octubre 2025	15 Octubre 2025

1. OBJETIVO

Establecer directrices generales de seguridad de la información tendientes a proteger la confidencialidad, integridad y disponibilidad de la información de **Grow Data**, garantizando que los activos de información estén protegidos de manera adecuada contra amenazas internas y externas.

2. ALCANCE

Esta política se aplica a todos los empleados, contratistas, proveedores y cualquier persona con acceso a los sistemas y activos de información de **Grow Data**. Incluye todos los sistemas de información, redes, bases de datos, hardware, software y medios de almacenamiento y en general la totalidad de activos de información de la organización.

3. DEFINICIONES

- **Activo de Información:** Cualquier dato, sistema o recurso que tiene valor para la organización y, por lo tanto, requiere protección. Los activos de información pueden incluir datos, hardware, software, instalaciones y personas.
- **Amenaza:** Un potencial evento o acción que podría explotar una vulnerabilidad para causar daño o impacto negativo a un activo de información. Las amenazas pueden ser naturales, humanas o tecnológicas.
- **Análisis de Riesgos:** El proceso de identificar y evaluar los riesgos para los activos de información, considerando las amenazas, vulnerabilidades y el impacto potencial.
- **Confidencialidad:** El principio de asegurar que la información solo esté disponible para aquellos que tienen el derecho de acceder a ella. Protege la información contra la divulgación no autorizada.
- **Controles de Seguridad:** Medidas que se implementan para proteger los activos de información. Pueden ser de naturaleza técnica, física o administrativa, y están diseñadas para reducir o mitigar los riesgos de seguridad.
- **Disponibilidad:** El principio de asegurar que los datos y sistemas de información estén accesibles y utilizables cuando se necesitan por los usuarios autorizados.
- **Evento de Seguridad de la Información:** [Fuente: NTC-ISO/IEC 27000] Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de las políticas de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.
- **Incidente de Seguridad de la Información:** [Fuente: NTC-ISO/IEC 27000] Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de

comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad:** El principio de proteger la exactitud y completitud de la información, asegurando que no sea modificada de manera no autorizada.
- **Política de Seguridad de la Información:** Un conjunto de principios, reglas y prácticas que establecen cómo se gestionará la seguridad de la información en una organización.
- **Riesgo de Seguridad de la Información:** La combinación de la probabilidad de que ocurra un incidente de seguridad de la información y la gravedad de su impacto sobre los activos de información.
- **SGSI (Sistema de Gestión de Seguridad de la Información):** Un enfoque sistemático y formal para gestionar la seguridad de la información dentro de una organización, asegurando que los riesgos sean identificados y gestionados de manera efectiva.
- **Vulnerabilidad:** Una debilidad o fallo en un sistema o proceso que podría ser explotado por una amenaza para causar un impacto negativo en un activo de información.
- **Confidencialidad:** Protección de la información para asegurar que solo las personas autorizadas puedan acceder a ella.
- **Incidente:** Cualquier suceso que compromete la seguridad de la información, como una pérdida de datos, acceso no autorizado, o ataque cibernético.
- **Integridad:** Asegurar que la información sea precisa, completa y esté libre de manipulaciones no autorizadas durante su procesamiento, almacenamiento o transmisión.

4. RESPONSABLES

- **Oficial de Seguridad de la Información (CISO):** Es el ejecutivo principal responsable de la estrategia y gestión de la seguridad de la información en la organización.
- **Comité de Seguridad de la Información:** Se encargan de las actividades generales de gestión de riesgos en relación con la seguridad de la información incluyendo la supervisión, la definición de las políticas y la implementación y mantenimiento de medidas de seguridad.
- **Usuarios:** Todos los miembros de la organización y partes interesadas tienen una responsabilidad compartida en la seguridad de la información al seguir políticas de seguridad, utilizar adecuadamente las herramientas y reportar incidentes.

5. DESCRIPCIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La alta dirección de **Grow Data** se compromete con el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SG-SI) alineado con los requisitos de la norma ISO IEC 27001, adicionalmente garantiza la identificación, evaluación y gestión de los riesgos de

seguridad de la información, mediante la implementación de controles apropiados en la mitigación de estos riesgos. Adicionalmente se compromete con garantizar la confidencialidad, integridad y confidencialidad de la información bajo el cumplimiento de las normas, leyes y normativos y generando cultura de seguridad de la información mediante capacitaciones permanentes a todos los usuarios.

6. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Garantizar la confidencialidad de la Información
- Garantizar la Integridad de la Información
- Asegurar la Disponibilidad de la Información
- Gestión Efectiva de Riesgos de Seguridad de la Información
- Cumplimiento Legal y Regulatorio
- Aumento de la Concienciación y Formación en Seguridad
- Respuesta Eficaz a Incidentes de Seguridad de la Información
- Mejora Continua del Sistema de Gestión de Seguridad de la Información.

7. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada al menos una vez al año o cuando sea necesario debido a cambios en el entorno de amenazas, requisitos legales o tecnologías. Las actualizaciones serán aprobadas por la alta dirección.

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	16/08/2024	Creación	NA
2.0	15/10/2025	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 al cambio de nombre del proceso.