	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON PROVEEDORES	CÓDIGO	SIG-PL-4
		VERSIÓN	5
		FECHA	29/08/2024
		CLASIFICACIÓN	Uso Público

1. OBJETIVO

El objetivo de esta política es establecer las directrices y procedimientos para la gestión de la seguridad de la información en las relaciones con los proveedores, asegurando que se mantengan los estándares de seguridad de la información y que se protejan los activos de información frente a riesgos asociados con los proveedores.

2. ALCANCE


Esta política se aplica a todos los proveedores que tienen acceso a la información de la empresa, ya sea directa o indirectamente, incluyendo proveedores de servicios de tecnología de la información, hardware, software, servicios en la nube, consultores externos, y cualquier otro proveedor que maneje, procese o almacene información sensible de la empresa.

3. DEFINICIONES

- **Proveedor:** Cualquier entidad externa que proporciona bienes o servicios.
- **Activos de Información:** Todo tipo de información que tiene valor para la empresa, incluyendo datos electrónicos, documentos físicos, propiedad intelectual, y cualquier otro tipo de información confidencial.
- **Incidente de Seguridad:** Cualquier evento que resulte en la pérdida, alteración, divulgación no autorizada, o acceso a la información de la empresa.

4. PRINCIPIOS GENERALES

- a) Los proveedores deben firmar un acuerdo de confidencialidad como requisito indispensable antes de iniciar cualquier relación comercial con AutenTIC. Este acuerdo de confidencialidad establece claramente las obligaciones del proveedor en cuanto a la protección, uso y divulgación de la información sensible y propietaria a la que puedan tener acceso durante el curso de la relación comercial. Además, especifica las consecuencias legales en caso de incumplimiento, asegurando que la información de la empresa esté protegida no solo durante la vigencia del contrato, sino también después de su finalización. La firma de este acuerdo subraya el compromiso del proveedor con las mejores prácticas de seguridad de la información y fortalece la relación de confianza y colaboración entre ambas partes. Igualmente, el proveedor debe asegurar que el acuerdo y cualquier lineamiento de seguridad de la información sean comunicados y aplicados a sus empleados y a terceros involucrados en el desarrollo de la relación contractual con AutenTIC.
- b) Resguardar la confidencialidad, integridad, disponibilidad y privacidad de la información perteneciente a la empresa, así como la de sus clientes y terceros, cuando los servicios contratados lo requieran; siempre que sea generada, almacenada o procesada en el marco del desarrollo de la relación contractual que lo vincule con AutenTIC.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON PROVEEDORES	CÓDIGO	SIG-PL-4
		VERSIÓN	5
		FECHA	29/08/2024
		CLASIFICACIÓN	Uso Público


- c) Todos los proveedores se evaluarán con respecto a sus capacidades y prácticas de seguridad de la información. Para esto se requiere que posean directrices, reglas y/o pautas de Seguridad de la Información en su organización; estas deben ser elaboradas y mantenidas al día en función de los riesgos que puedan afectar a la organización.
- d) La información compartida con proveedores debe ser clasificada de acuerdo con la política de clasificación de la información de AutenTIC, y solo se debe proporcionar el acceso necesario para cumplir con las obligaciones contractuales.
- e) Los proveedores deben implementar controles adecuados para proteger la información, alineados con las mejores prácticas de seguridad.
- f) La disponibilidad de la información se ajustará a los términos estipulados en el contrato, oferta u orden de compra correspondiente. Si no se cuenta con un acuerdo específico de nivel de servicio, el proveedor deberá garantizar que la información esté disponible cuando sea requerida, actuando con la mayor atención y cuidado.
- g) Los controles de acceso, tanto técnicos como operacionales, que los proveedores deben seguir, deben estar debidamente documentados y aprobados, y ser conocidos por ambas partes involucradas.
- h) Cuando se produzcan cambios en el servicio, AutenTIC definirá y comunicará los ajustes realizados o previstos en relación con los acuerdos contractuales iniciales, conforme a lo establecido en el Manual de Selección, Evaluación y Reevaluación de Proveedores.

4.1. Monitoreo y Revisión Continua:

- AutenTIC realizará revisiones periódicas del desempeño de los proveedores en términos de seguridad de la información. Esto incluirá auditorías, revisiones de cumplimiento y evaluaciones de riesgos.
- Cualquier incumplimiento de los requisitos de seguridad por parte de un proveedor será evaluado y podrá resultar en la terminación del contrato o en la implementación de medidas correctivas.

4.2. Gestión de Incidentes de Seguridad:

- Los proveedores deben notificar inmediatamente a AutenTIC en caso de cualquier incidente de seguridad que pueda afectar la información de la empresa.
- Los proveedores deben colaborar en la investigación y resolución de incidentes de seguridad, incluyendo la provisión de acceso a registros y documentación relevante.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON PROVEEDORES	CÓDIGO	SIG-PL-4
		VERSIÓN	5
		FECHA	29/08/2024
		CLASIFICACIÓN	Uso Público

5. CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

- a. Los proveedores clasificados como críticos que subcontraten servicios relacionados con la tecnología de la información y comunicación deben garantizar que los requisitos y buenas prácticas de seguridad adoptados por AutenTIC se apliquen igualmente a los terceros que participen directamente en la prestación de estos servicios.
- b. Para cada adquisición de software y hardware, el departamento técnico, junto con el Oficial de Seguridad de la Información, debe definir los requisitos de seguridad conforme al procedimiento de compras establecido.
- c. Debe garantizarse que la infraestructura y los servicios ofrecidos dispongan de mecanismos de seguridad efectivos para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

6. PROHIBICIONES:


- a) **Uso de Software No Autorizado:** Se prohíbe estrictamente el uso de software, herramientas, o servicios que no hayan sido aprobados previamente por AutenTIC dentro del contexto de la relación contractual.
- b) **Subcontratación No Autorizada:** Los proveedores no pueden subcontratar servicios o componentes clave sin la autorización previa y por escrito de AutenTIC, especialmente en la cadena de suministro de TIC.
- c) **Transferencia No Autorizada de Información:** Está prohibido compartir, transferir o divulgar información de AutenTIC a terceros no autorizados, sin importar el contexto.
- d) **Uso Inapropiado de la Información:** Queda prohibido el uso de la información de la empresa por parte de los proveedores para fines distintos a los acordados en el contrato.

7. VIGENCIA

Esta política será sometida a revisión y aprobación con una frecuencia anual o a cambios que puedan afectar su propósito, será revisada por el Oficial de Seguridad de la Información o quien designe la Dirección y será aprobada por la Dirección General.



LUIS MIGUEL GONZÁLEZ ULLOA
 Director General

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON PROVEEDORES	CÓDIGO	SIG-PL-4
		VERSIÓN	5
		FECHA	29/08/2024
		CLASIFICACIÓN	Uso Público

CONTROL DE VERSIONES Y CAMBIOS

Versión	Fecha Aprobación	Nota de Cambio
1	19/02/2021	Versión inicial
2	10/05/2021	Se ejecutan correcciones según notas de auditoría de certificación
3	24/07/2022	Revisión del documento
4	10/06/2023	Actualización de política uso de correo electrónico
5	29/08/2024	<ul style="list-style-type: none"> • Se separaron estos lineamientos de los proveedores de la política del documento general. • Se modificó toda la política • Se asignó la codificación.



Documento No.
fad73728-14d1-4aa7-89a8-9b462dbe33ad

Creado el:
29/08/2024 06:11 p. m.

Este documento es la representación de un documento original en formato electrónico. Para validar el estado actual del documento ingrese a: consulta.autenticsign.comy/o escanee el código QR.



Este documento está firmado electrónicamente, de conformidad con los estándares internacionales de firma en tanto es un documento auténtico, íntegro y disponible para consulta en línea.

4 Páginas