

Versión: 1.0	POLÍTICA DE GESTIÓN DE SEGURIDAD DE PROVEEDORES - PUBLICA	
Vigente desde: 21/05/2026		



POLÍTICA DE GESTIÓN DE SEGURIDAD DE PROVEEDORES - PUBLICA
CODIGO: POL-0506

RUTA DE VALIDACIÓN		
FUNCIÓN	CARGO	UNIDAD
ELABORADO POR:	Analista de Procesos	Gerencia de Administración y Finanzas
REVISADO POR:	Consultor	Gerencia de Consultoría
APROBADO POR:	Gerente de Administración y Finanzas	Gerencia de Administración y Finanzas

Clasificación: Público

Página: 1 de 5

Nota: La información contenida en este documento es de propiedad de Assertiva y debe ser tratada de acuerdo con su nivel de confidencialidad. El uso no autorizado de la información contenida en este documento podrá ser sancionado.

Versión: 1.0	POLÍTICA DE GESTIÓN DE SEGURIDAD DE PROVEEDORES - PUBLICA	
Vigente desde: 21/05/2026		

1. Control de Cambios

Fecha	Aprobado por	Observación
21/05/2024	Gerente de Administración y Finanzas	versión inicial

Clasificación: Público

Página: 2 de 5

Nota: La información contenida en este documento es de propiedad de Assertiva y debe ser tratada de acuerdo con su nivel de confidencialidad. El uso no autorizado de la información contenida en este documento podrá ser sancionado.

Versión: 1.0	POLÍTICA DE GESTIÓN DE SEGURIDAD DE PROVEEDORES - PUBLICA	
Vigente desde: 21/05/2026		

Contenido

1. Control de Cambios	2
2. Política de Gestión de Proveedores y Seguridad de la Información	4
3. Compromiso con la seguridad.....	4
4. Gestión de proveedores	4
5. Responsabilidades de los proveedores	5
6. Cultura de concientización	5

Clasificación: Público

Página: 3 de 5

Nota: La información contenida en este documento es de propiedad de Assertiva y debe ser tratada de acuerdo con su nivel de confidencialidad. El uso no autorizado de la información contenida en este documento podrá ser sancionado.

Versión: 1.0	POLÍTICA DE GESTIÓN DE SEGURIDAD DE PROVEEDORES - PUBLICA	
Vigente desde: 21/05/2026		

2. Política de Gestión de Proveedores y Seguridad de la Información

En Assertiva reconocemos que nuestros proveedores y socios estratégicos desempeñan un rol fundamental en la entrega de servicios seguros y confiables. Por ello, mantenemos lineamientos orientados a proteger la confidencialidad, integridad y disponibilidad de la información compartida durante nuestras relaciones comerciales.

3. Compromiso con la seguridad

Assertiva exige que sus proveedores adopten prácticas adecuadas de seguridad de la información y protección de datos, alineadas con los riesgos asociados a los servicios o productos que entregan.

Nuestros procesos consideran:

- Evaluación de riesgos antes de contratar servicios o proveedores.
- Definición de requisitos de seguridad y confidencialidad en contratos y acuerdos.
- Monitoreo periódico del cumplimiento de condiciones de seguridad y niveles de servicio.
- Gestión de incidentes de seguridad de la información relacionados con terceros.
- Control de accesos y protección de los activos de información.
- Medidas de continuidad y recuperación ante contingencias.
- Gestión segura del término de contratos y devolución o eliminación de información.

4. Gestión de proveedores

Assertiva mantiene un proceso formal de gestión de proveedores que contempla:

- Clasificación de proveedores según criticidad y nivel de riesgo.
- Evaluaciones de seguridad para proveedores críticos.

Clasificación: Público

Página: 4 de 5

Nota: La información contenida en este documento es de propiedad de Assertiva y debe ser tratada de acuerdo con su nivel de confidencialidad. El uso no autorizado de la información contenida en este documento podrá ser sancionado.

Versión: 1.0	POLÍTICA DE GESTIÓN DE SEGURIDAD DE PROVEEDORES - PUBLICA	
Vigente desde: 21/05/2026		

- Revisión continua de cambios que puedan afectar la seguridad de los servicios.
- Mantenimiento de registros actualizados de proveedores y servicios asociados.

5. Responsabilidades de los proveedores

Los proveedores que trabajan con Assertiva deben:

- Cumplir las políticas y requisitos de seguridad aplicables.
- Proteger la información y activos a los que tengan acceso.
- Reportar oportunamente incidentes o eventos de seguridad.
- Mantener comunicación sobre cambios relevantes en los servicios prestados.

6. Cultura de concientización

Promovemos actividades de capacitación y concientización en seguridad de la información tanto para colaboradores internos como para terceros que interactúan con nuestros procesos y sistemas.

Clasificación: Público

Página: 5 de 5

Nota: La información contenida en este documento es de propiedad de Assertiva y debe ser tratada de acuerdo con su nivel de confidencialidad. El uso no autorizado de la información contenida en este documento podrá ser sancionado.