Política de Seguridad de la Información para la Relación con Proveedores

Esta política establece los requisitos de seguridad de la información que deben cumplir los proveedores, suministradores, colaboradores, partes interesadas, canales de ventas y distribución que tengan acceso a información de MANIPULAE SL. El objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información, minimizando los riesgos de seguridad.

Todos los productos y servicios adquiridos a terceros deberán cumplir con los requisitos de ciberseguridad definidos por MANIPULAE SL, los cuales serán coherentes con nuestras políticas internas de gestión. Estos requisitos se extenderán a toda la cadena de suministro.

La organización garantizará el cumplimiento de las normativas legales aplicables relacionadas con la protección de datos y la seguridad de la información, incluyendo, entre otras, el Reglamento General de Protección de Datos (RGPD), la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), y la legislación sobre derechos de propiedad intelectual. Estas normativas serán incorporadas en los procesos y prácticas internas, asegurando su correcta aplicación y cumplimiento en todas las actividades de la organización.

Las condiciones específicas que podrían conllevar la terminación del contrato, incluyendo aquellas relacionadas con la seguridad de la información, pueden incluir las siguientes:

1. Incumplimiento de las medidas de seguridad acordadas.
2. Gestión inadecuada de incidentes de seguridad.
3. Falta de cumplimiento de normativas legales aplicables.
4. Retrasos o fallos críticos en la prestación del servicio.
5. Negativa a someterse a auditorías de seguridad.
6. Ausencia de certificaciones exigidas en el contrato.
7. Filtración o uso indebido de información confidencial.
8. Inacción ante hallazgos críticos o recomendaciones de mejora.

El contrato incluirá garantías claras para proteger los intereses de la organización reflejadas en el Anexo SLA en aquellos proveedores considerados críticos para la organización.

Los contratos establecerán las responsabilidades de cada parte en seguridad, especificando penalizaciones por incumplimiento. Se detallará quién gestiona el acceso a información sensible, realiza copias de seguridad, monitorea registros de actividad y mantiene los sistemas de seguridad como antimalware, firewalls y cifrado.

La organización implementará medidas para garantizar la seguridad de la información en toda la cadena de suministro, exigiendo a los proveedores y socios comerciales el cumplimiento de estándares de seguridad equivalentes a los de la empresa. Esto incluirá la evaluación regular de riesgos asociados, la formalización de acuerdos contractuales con cláusulas específicas de protección de información y el monitoreo continuo de las prácticas de seguridad de los terceros involucrados. Además, se fomentará una comunicación efectiva con los proveedores para responder oportunamente a incidentes y garantizar la integridad de la información compartida.

Aprobada por Dirección