POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INNOVATION TELECOMUNICACIONES SAS

El proveedor se compromete a proteger la información durante todo su ciclo de vida, adoptando medidas administrativas, técnicas y organizacionales orientadas a prevenir su pérdida, alteración, eliminación, divulgación, acceso, uso o tratamiento no autorizado.

Para ello, implementará controles de seguridad acordes con su operación y con los riesgos identificados, procurando preservar la **confidencialidad, integridad y disponibilidad de la información**, así como prevenir, detectar, gestionar y atender oportunamente los eventos e incidentes que puedan afectar los sistemas, redes, infraestructura tecnológica o información bajo su responsabilidad.

¿Cómo cumplir con la Política de Seguridad de la Información?

1. **Protección de la información:** Proteger la información para preservar su confidencialidad, integridad y disponibilidad durante todo su ciclo de vida.

2. **Seguridad de la infraestructura tecnológica:** Implementar y mantener herramientas, controles y mecanismos de seguridad que permitan conservar un nivel adecuado de protección de los sistemas, redes, equipos e infraestructura tecnológica.

3. **Control y monitoreo:** Controlar y monitorear las actividades realizadas mediante los sistemas y recursos tecnológicos, con el propósito de identificar y prevenir situaciones que puedan afectar negativamente la información o la infraestructura.

4. **Gestión de accesos:** Establecer mecanismos para controlar el acceso a sistemas, redes, equipos e información, procurando que únicamente tengan acceso las personas debidamente autorizadas.

5. **Gestión de incidentes de seguridad:** Identificar, reportar, gestionar y atender oportunamente los eventos o incidentes de seguridad de la información, adoptando las acciones necesarias para mitigar sus efectos y evitar su recurrencia.

6. **Respaldo y recuperación de información:** Implementar mecanismos de respaldo y recuperación de la información que permitan garantizar su disponibilidad y continuidad frente a fallas, pérdidas o incidentes.

7. **Cumplimiento de políticas y controles:** Verificar periódicamente la aplicación y cumplimiento de las políticas, procedimientos y requisitos establecidos en materia de seguridad de la información.

8. **Seguridad de proveedores y terceros:** Controlar y supervisar, de acuerdo con el nivel de riesgo aplicable, las actividades realizadas por proveedores, contratistas y terceros que tengan acceso a información, sistemas o infraestructura tecnológica.

9. **Uso adecuado de los recursos tecnológicos:** Promover el uso responsable y autorizado de los equipos, sistemas, redes, cuentas, credenciales y demás recursos tecnológicos dispuestos para el desarrollo de las actividades.

10. **Cultura de seguridad:** Promover actividades de información, capacitación y sensibilización dirigidas al personal, orientadas a fortalecer la cultura de seguridad de la información y prevenir riesgos asociados al factor humano.

11. **Mejoramiento continuo:** Revisar y actualizar periódicamente las medidas de seguridad implementadas, teniendo en cuenta los riesgos identificados, los cambios tecnológicos, los incidentes presentados y las necesidades de la organización.

FIN DEL DOCUMENTO