1. Comunicado

Política general seguridad de la información

La Política de Seguridad de la Información de IdeasFractal SAS en el sector turístico tiene como principal objetivo salvaguardar datos sensibles y activos de información en sus procesos. En este sentido, se comprometen a implementar, mantener y mejorar la seguridad de la información, haciendo énfasis en la gestión de riesgos y el cumplimiento del estándar PCI DSS para transacciones con tarjetas de pago. Un aspecto crucial de esta política es la creación de una cultura organizacional centrada en la seguridad y la privacidad.

Las directrices establecidas comprenden la definición y revisión periódica de políticas de seguridad, la creación de un programa PCI DSS destinado a fomentar la seguridad informática, así como la responsabilidad de todos los usuarios de cumplir con las políticas establecidas.

Los objetivos clave de esta política son el fortalecimiento de la seguridad de la información, la implementación de controles físicos y lógicos, la protección de datos personales y la mejora de la gestión de la seguridad informática. Se promueven programas de formación y se busca instaurar una cultura organizacional enfocada en la seguridad de la información.

Es importante destacar que esta política se aplica de manera integral a todos los niveles de la organización, incluyendo tanto a usuarios internos como externos, así como a toda la información de la empresa. Los principios fundamentales de seguridad informática abordados son la confidencialidad, la disponibilidad y la integridad de la información.

Es imperativo resaltar que el cumplimiento de esta política es de carácter obligatorio para todos los empleados, contratistas y cualquier persona que tenga acceso a los activos de información de la organización.

Establece un compromiso de dirección para garantizar la seguridad de la información, lo que incluye la revisión periódica de la política, su divulgación y la asignación de recursos adecuados. Adicionalmente, la política se somete a una revisión anual y se incorpora en los contratos celebrados con empleados y contratistas. Se realiza anualmente una auditoría de ciberseguridad para evaluar la efectividad de las medidas implementadas.

En esta política, se definen claramente los roles y responsabilidades, destacando al Director de Tecnología de la Información como el principal responsable de la política, así como al Director del Proyecto PCI DSS para la implementación de políticas específicas. Además, se detallan otros roles esenciales, como propietarios, custodios y usuarios de información. Se asignan responsabilidades específicas para la gestión de activos de información, el uso de información por terceros y se establecen sanciones por incumplimiento.

En resumen, esta política aborda de manera integral la identificación de amenazas, vulnerabilidades y la importancia de establecer controles adecuados. Además, define los tipos de activos y roles y responsabilidades relacionados con la administración de la seguridad de la información.