POLÍTICA Y MANUAL OPERATIVO

DE SEGURIDAD DE LA INFORMACIÓN

CLICK MÓVIL ISP

En cumplimiento del Artículo 5.1.2.3 de la Resolución CRC 6890 de 2022 y los estándares internacionales ISO/IEC 27000.

1. OBJETIVO

Establecer los lineamientos de seguridad de la información que permitan garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los servicios de telecomunicaciones y de la información procesada, transmitida o almacenada por CLICK MÓVIL ISP.

2. ALCANCE

Esta política aplica a la infraestructura tecnológica, procesos operativos, administrativos y técnicos asociados a la prestación de servicios, así como a todos los empleados, contratistas, proveedores y terceros que gestionen información en nombre de la empresa.

3. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- Confidencialidad: La información será accesible únicamente a personas autorizadas.
- Integridad: Se garantizará la exactitud, completitud y confiabilidad de la información.
- Disponibilidad: Los servicios y datos estarán disponibles para los usuarios legítimos en los tiempos requeridos.
- Legalidad y cumplimiento: Todas las prácticas se ajustarán a la normatividad de la CRC y demás autoridades competentes.
- Responsabilidad y trazabilidad: Toda acción sobre la información deberá ser atribuible, registrable y auditable.
- Mejora continua: El SGSI será revisado y actualizado periódicamente, fortaleciendo la seguridad frente a nuevos riesgos y amenazas.

4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

- Identificación, análisis y tratamiento de riesgos.
- Definición de controles administrativos, físicos, tecnológicos y organizacionales.
- Capacitación periódica en seguridad.
- Monitoreo continuo de vulnerabilidades y amenazas.
- Planes de contingencia, respaldo y recuperación.
- Auditorías internas y externas para validar cumplimiento

5. GESTIÓN DE INCIDENTES DE SEGURIDAD

Todo incidente debe ser identificado, documentado y gestionado según su severidad (Clase I-IV), garantizando contención, erradicación, recuperación y preservación de evidencias bajo cadena de custodia.

MANUAL OPERATIVO DE SEGURIDAD

GERENCIA GENERAL

- Aprobar y difundir la política de seguridad.
- Asignar recursos necesarios para el SGSI.
- Revisar informes de incidentes y vulnerabilidades.
- Autorizar planes de contingencia y continuidad.
- Coordinar con autoridades y auditorías externas

ÁREA TÉCNICA / NOC

- Monitorear red y sistemas críticos.
- Registrar y clasificar incidentes.
- Aplicar medidas de contención, erradicación y recuperación.
- Documentar acciones técnicas y conservar evidencias.
- Participar en simulacros y pruebas de recuperación.

ÁREA ADMINISTRATIVA Y LEGAL

- Recibir y consolidar reportes de incidentes.
- Notificar incidentes a la CRC y colCERT según plazos establecidos.
- Actualizar documentación normativa y contractual.
- Custodiar registros durante mínimo 1 año.
- Coordinar auditorías internas y externas

COLABORADORES

·Usar credenciales de manera segura.
·Reportar anomalías o incidentes al área técnica.
·Proteger información sensible y cumplir con procedimientos.
·Asistir a capacitaciones de ciberseguridad.
·Cumplir políticas de uso de dispositivos y redes corporativas.

PROVEEDORES Y ALIADOS

- Cumplir acuerdos de confidencialidad y seguridad.
- Notificar incidentes que afecten servicios subcontratados.
- Implementar medidas mínimas de seguridad en su infraestructura.
- Aceptar auditorías o verificaciones de CLICK MÓVIL ISP.

MAURICIO ALBERTO CUELLAR REYES
REPRESENTANTE LEGAL
SINERGIASOLUTION2019@GMAIL.COM
CEL. 3104571417