Comisión de Regulación de Comunicaciones

Política de Seguridad del Sistema de Gestión de Seguridad de la Información

La Comisión de Regulación de Comunicaciones como Unidad Administrativa Especial adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia, encargada de promover la libre y leal competencia y la inversión en el sector de las Tecnologías de la Información y las Comunicaciones, fundamentándose en un marco regulatorio convergente orientado a maximizar el bienestar social y la protección de los derechos de todos los usuarios colombianos y consciente de la importancia que la seguridad de la información tiene para el desarrollo de su función ha decido implementar un sistema de gestión de seguridad de la información, por lo que establece y suscribe la presente política.

La Política de Seguridad de la Información está encaminada a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware, el software y los servicios informáticos), la implementación del Sistema de Gestión de Seguridad de la Información, está encaminada a mejorar su seguridad, entendiéndola como la conservación de la confidencialidad e integridad de sus datos así como de los sistemas que la soportan y se compromete a implementar, apoyar y divulgar la presente política, así como los correspondientes procedimientos e instructivos de trabajo relacionados con el SGSI.

La Comisión de Regulación de Comunicaciones, para el cumplimiento de su misión, visión, objetivos estratégicos y valores institucionales, establece la función de Seguridad de la Información en la Entidad, con el fin de:

- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus usuarios y funcionarios.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos tecnológicos, así como la integridad y la confidencialidad de la información de la Entidad.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, pasantes, entre otros, de la CRC.
- Garantizar la continuidad del servicio frente a posibles incidentes.
- Garantizar la protección de derechos como el hábeas data.

Alcance/Aplicabilidad

La presente política aplica a toda la entidad, sus funcionarios, contratistas, terceros y pasantes de la CRC, en cuanto a los datos, los sistemas de información, el hardware y software que apoyan la gestión y el mantenimiento de los mismos.

El proceso iniciará por el Área de Gestión Tecnológica, el cual tiene como propósito en la entidad, gestionar eficaz y eficientemente los sistemas de información de la CRC para satisfacer los requerimientos de los clientes.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad de la presente política, se deben comprometer en un 100% con el cumplimiento de la misma.

A continuación se establecen los 14 parámetros de seguridad que soportan la política del SGSI de la Comisión de Regulación de Comunicaciones:

1. La CRC se compromete a definir, implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información dotándolo de aquellos medios y recursos que sean necesarios e instando a todo el personal para que asuma este compromiso, soportado en lineamientos claros alineados con las necesidades del negocio, y con los requerimientos regulatorios.

2. La CRC se compromete a integrar el SGSI con otros sistemas de gestión de la organización, compartiendo aquellos recursos que apliquen en beneficio de la optimización y buscando la mejora continua de la eficiencia y eficacia de la gestión de los procesos.

3. La CRC se compromete a implantar las medidas requeridas para la formación y concienciación del personal con la seguridad de la información

4. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas y pasantes.

5. La CRC se compromete a proteger la información generada, procesada o resguardada por los procesos internos, su infraestructura tecnológica y sus activos, del riesgo que se genera por los accesos otorgados a terceros.

6. La CRC protege la información creada, procesada, transmitida o resguardada por cada uno de sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a su uso incorrecto. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o que se encuentra bajo su custodia.

   La CRC garantiza el derecho de hábeas data de sus colaboradores y usuarios cuando sea encargada de tratar información o datos personales de los mismos, implementando normas de seguridad tendientes a impedir la adulteración, pérdida, destrucción o acceso no autorizado a los datos

7. La CRC se compromete a tomar las medidas necesarias para proteger su información de las amenazas que puedan ser originadas en fallas humanas o técnicas de su infraestructura.

8. La CRC se compromete a proteger sus instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

9. La CRC se compromete a controlar la operación de sus procesos internos, garantizando la seguridad de los recursos tecnológicos y las redes de datos.

10. La CRC se compromete a implementar controles de acceso a la información, sistemas y recursos de red.

11. La CRC garantiza que la seguridad es parte integral del ciclo de vida de los sistemas de información.

12. La CRC se compromete a mantener a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.

13. La CRC garantiza la disponibilidad de recursos tecnológicos para los procesos internos y la continuidad de la operación basado en el impacto que pueden generar los eventos de riesgo que lleguen a materializarse.

14. La CRC garantiza el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas, en materia de protección de la información.

Revisión de la Política

La revisión de la política del Sistema de Seguridad de la Información, se revisará anualmente o cuando haya una incidencia de seguridad, evento o cambio tecnológico que amerite su revisión.

CARLOS PABLO MÁRQUEZ ESCOBAR
Director Ejecutivo

Proyectado por: Sandra Salazar
Revisado por: Diana Wilches
Aprobado por: Zoila Vargas