DOCUMENTO DE APOYO

LINEAMIENTO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En la Cámara de Comercio de Medellín para Antioquia trabajamos para que las empresas e instituciones sociales y culturales de la región crezcan, siendo un aliado en su desarrollo. Por esta razón implementamos los procesos, las prácticas y estructura requeridos para cumplir con nuestras funciones delegadas y otras iniciativas de desarrollo empresarial con altos estándares de seguridad y manejo de datos e información.

La CCMA en su direccionamiento estratégico, establece el sistema de seguridad de la información con los siguientes objetivos:

• Diseñar los procesos y entregar las herramientas tecnológicas e informáticas que garanticen la disponibilidad, integridad y confidencialidad de la información; así como la continuidad operativa de la organización.
• Minimizar la ocurrencia y recurrencia de incidentes y eventos que puedan afectar los pilares de la seguridad de la información.
• Promover el desarrollo de una cultura del manejo seguro de la información.

Para su funcionamiento, el sistema de gestión de seguridad de la información define criterios claros frente al manejo de los diferentes mecanismos de gestión de la confidencialidad, integridad y disponibilidad de los activos de información y se compromete a satisfacer las necesidades de sus grupos de interés mediante:

- La prestación de servicios de calidad, pertinentes y oportunos soportados en tecnología, cuyas políticas de implementación y desarrollo obedezcan a criterios y estándares para el adecuado manejo y cuidado de la información.
- La disposición y administración de los recursos necesarios y pertinentes para alcanzar una cobertura integral de los aspectos relativos a la seguridad informática y ciberseguridad.
- El establecimiento de los criterios para la recolección, almacenamiento, uso, circulación y supresión de los datos personales tratados por la CÁMARA en desarrollo de su objeto social y garantizar en todo momento los derechos de habeas de data, la privacidad y la seguridad de los datos de los titulares de información personal.
- La gestión de los riesgos alrededor de los activos de información y los activos secundarios o aplicaciones y mecanismos mediante los cuales se le de tratamiento y uso a la misma.
- La definición e implementación de planes de contingencia y respuesta a emergencias para cuidar, recuperar y activar la información requerida para asegurar la continuidad del negocio.
- La definición de procesos continuos de verificación, evaluación y pruebas de funcionamiento de las políticas y lineamientos de seguridad de la información.
- Y, el cumplimiento de los requisitos legales y la gestión de acciones de mejora continua aplicando las metodologías establecidas por la Organización.

Así mismo se asignan responsabilidades generales y específicas para la gestión de la seguridad de la información:

- ✓ **Alta dirección:** Es responsable de:
  - Aprobar la política y realizar seguimiento al desempeño y definiciones del sistema de gestión en intervalos planificados.
  - Proporcionar los recursos necesarios para establecer, implementar, operar, realizar seguimiento, mantener y mejorar el sistema de gestión.

- ✓ **Líder del SG-SI (Equipo de Tecnología):** Es responsable de:
    - Definir los procesos, lineamientos, directrices y documentos de apoyo del sistema de gestión en lo relativo a la Seguridad de la Información de acuerdo con los estándares normativos y legislación aplicable.
    - Identificar, evaluar y monitorear los riesgos y controles del sistema de gestión – Seguridad de la Información.
    - Monitorear el desempeño del sistema de gestión - Seguridad de la Información.
    - Identificar e implementar acciones de mejora continua del sistema de gestión – Seguridad de la Información.
    - Atender los procesos de auditorías del sistema de gestión – Seguridad de la Información.
    -
- ✓ **Colaboradores o usuarios CCMA:** Son responsables de:
    - Cumplir con las políticas y lineamientos definidos dentro el sistema de gestión para garantizar la integridad, disponibilidad y confidencialidad de la información.
    - Monitorear las situaciones de riesgos y reportar los eventos de seguridad de la información en forma oportuna siguiendo el procedimiento establecido.
    - Reportar las debilidades observadas o sospechadas en los sistemas o servicios con el objetivo de evitar incidentes de seguridad de la información.
    - Usar adecuadamente las bases de datos de personas y/empresas cumpliendo con los derechos de habeas de data.

- ✓ **Proveedores:** Son responsables de:
    - Cumplir con las políticas, procesos, lineamientos y documentos de apoyo definidos dentro del sistema de gestión para garantizar la integridad, disponibilidad y confidencialidad de la información.
    - Asegurar la confidencialidad, integridad y disponibilidad de sus activos de información en los servicios prestados.
    - Reportar los eventos de seguridad de la información en forma oportuna siguiendo el procedimiento establecido.
    - Reportar las debilidades observadas o sospechadas en los sistemas o servicios con el objetivo de evitar incidentes de seguridad de la información.