

Política general de Seguridad de la Información

En la Cámara de Comercio de Bogotá la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes. La Cámara de Comercio de Bogotá es consciente del valor de la información, independiente de cual sea su forma, origen o fecha de generación, razón por la cual existe un compromiso expreso por la protección y cuidado de la misma, con el fin de asegurar a sus clientes, accionistas, empleados y contratistas, que la información se maneja en condiciones de seguridad adecuadas.

La Seguridad de la Información en la Cámara de Comercio de Bogotá, tiene como objetivo proteger la información de una gran variedad de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el riesgo, reducir los impactos por incidentes de seguridad, generar oportunidades de negocio y para dar cumplimiento legal, contractual y regulatorio; el debido cuidado en el manejo de la información, permitirá a la Cámara de Comercio de Bogotá mantener relaciones de confianza con sus clientes actuales y futuros.

Los principios de seguridad para el manejo de la información se tienen en cuenta en la Cámara de Comercio de Bogotá, los cuales son los exigidos por la Ley y las buenas prácticas de seguridad: la confidencialidad, la integridad, la disponibilidad y el no repudio; también se tienen en cuenta los principios de calidad en el manejo de la información como son: la efectividad, la eficiencia y la confiabilidad.

La protección de la información requiere de un proceso integral de gestión del riesgo que identifique, clasifique y defina los propietarios de los activos de información de acuerdo con su sensibilidad y criticidad; liste y analice las amenazas y vulnerabilidades de los activos y evalúe la probabilidad de ocurrencia e impacto en términos de la pérdida de la confidencialidad, integridad y disponibilidad, para determinar el nivel de riesgo existente; posteriormente se decide la opción de tratamiento del riesgo (mitigar, transferir, aceptar, evitar) más adecuada para la organización, con el fin de llevar el riesgo a un nivel aceptable y finalmente se implementan actividades de monitoreo que permiten medir la eficacia de los controles implementados para generar oportunidades de mejora.

La Cámara de Comercio de Bogotá proporciona los recursos que permiten implementar un Gobierno de Seguridad de la Información alineado a los requisitos de Ley, contractuales, reglamentarios y a las necesidades de distintas áreas de la organización. Así mismo facilita los medios para la educación, formación y concientización en materia de seguridad de la información.

Todos los funcionarios de la Cámara de Comercio de Bogotá son responsables del manejo de la información en condiciones de seguridad, el cumplimiento de las políticas y de los controles implementados por la organización, así como de detectar las oportunidades de mejora, reportar incidentes de seguridad e implementar las acciones correctivas o preventivas a que haya lugar, para asegurar un proceso permanente de mejora en la Gestión de la Seguridad de la Información.

El Comité de Buen Gobierno, Riesgos y Auditoria conformado por miembros de Junta Directiva, Presidencia y Vicepresidencia, como representantes de la Alta Gerencia aprueban esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información en la Entidad. Así mismo verificarán el cumplimiento de las actividades de planeación, implementación, seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

Es responsabilidad de la Coordinación de Planeación e Innovación – Seguridad de la Información de la Cámara de Comercio de Bogotá velar por el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos, procedimientos, instructivos y formatos específicos alineados al estándar internacional ISO 27001 y sus normas derivadas además de los otros marcos generalmente aceptados como: COBIT, ITIL, NIST, ASNZ y DRII, así como liderar la implementación de los controles exigidos por la Ley y la Regulación Vigente.