Banco de la República
Colombia

14 de septiembre de 2020

CERTIFICA QUE:

EL Banco de la República cuenta con un Sistema de Gestión de Seguridad de la Información – SGSI (Certificado ISO27001:2013) el cual está conformado por las políticas, los estándares (técnicos y generales de seguridad de la información), la arquitectura computacional, los procesos y procedimientos, la estructura organizacional y los mecanismos de verificación y control. El SGSI tiene como propósito garantizar que los riesgos de la seguridad de la información y los riesgos de ciberseguridad son conocidos, asumidos, gestionados y mitigados por el Banco de forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios que se producen en el entorno y en la tecnología.

Las Políticas de Seguridad de la Información y de Ciberseguridad son parte fundamental del SGSI y contienen directrices que enmarcan la actuación de todos los empleados, funcionarios y contratistas del Banco de la República respecto al asunto. Estas tienen por objeto:

a. Establecer directrices generales relacionadas con seguridad de la información y ciberseguridad.
b. Ser un medio de divulgación para comunicar los lineamientos establecidos por la Administración del Banco de la República respecto a la seguridad de la información y la ciberseguridad, generando cultura y compromiso en todos los niveles de la organización.
c. Establecer y comunicar la responsabilidad y autoridad sobre el manejo de la seguridad de la información y la ciberseguridad del Banco.
d. Orientar el debido cuidado y la debida diligencia en la gestión de la seguridad de la información y la ciberseguridad.
e. Establecer un orden y marco de actuación en temas de seguridad de la información y ciberseguridad, para todas las personas que presten sus servicios al Banco de la República.
f. Garantizar la confiabilidad, imagen y credibilidad del Banco de la República con sus empleados, clientes y con la sociedad en general.
g. Definir un lenguaje común sobre la seguridad de la información y la ciberseguridad dentro de la organización.

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

P1. **Sistema de Gestión de la Seguridad de la información (SGSI);** El Banco debe contar con un Sistema de Gestión de la Seguridad de la Información (SGSI) que apoye una adecuada gestión de riesgos. Dicho Sistema soportará la debida protección de la información a partir de principios universalmente aceptados de seguridad de la información (Confidencialidad, Integridad, Disponibilidad).

P2. **Valoración y Protección de la Información**; El Banco debe valorar la información desde el punto de vista de seguridad y acorde a esto determinar los mecanismos de protección adecuados.

P3. **Arquitecturas Aprobadas de Seguridad**; El Banco desde las etapas iniciales de los proyectos, debe incluir la evaluación de aspectos relacionados con la arquitectura de seguridad y seguir los lineamientos establecidos al respecto.

P4. **Atención de Incidentes de Seguridad**; El Banco debe atender los incidentes relacionados con la seguridad de la información y la ciberseguridad.

P5. **Buen uso de los recursos tecnológicos;** El Banco debe implementar los mecanismos para vigilar y promover el buen uso de los recursos tecnológicos. Las personas que presten sus servicios al Banco deben seguir los lineamientos de seguridad de la información y hacer buen uso de dichos recursos.

P6. **Buen uso de los activos de información**; El Banco debe implementar los mecanismos para vigilar y promover el buen uso de la información. Las personas que presten sus servicios al Banco deben conocer la clasificación desde el punto de vista de seguridad de la información a su cargo y acorde a esto seguir las recomendaciones de esta política.

P7. **Control de acceso;** El Banco debe implementar controles de acceso (físicos y lógicos) para que la información corporativa se encuentre debidamente protegida. Así mismo, debe tener mecanismos para seguimiento de actividades sobre la información o recursos de tecnología.

P8. **Operación;** El Banco debe implementar mecanismos y procedimientos para mitigar los riesgos asociados a la gestión de la información en los procesos que soportan la operación del negocio.

P9. **Operación Plataforma;** El Banco debe implementar mecanismos y procedimientos para mitigar los riesgos asociados a la administración de la plataforma tecnológica que soporta la operación del negocio.

P10. **Ciberseguridad;** El Banco implementará un programa de ciberseguridad alineado con mejores prácticas y la Política Nacional de Ciberseguridad. Dicho programa buscará el mejoramiento continuo de su postura de seguridad y aumentar su resiliencia.

LUIS FRANCISCO RIVAS DUEÑAS
Subgerente
Subgerencia General de Servicios Corporativos