LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD APLICABLES A PROVEEDORES Y ALIADOS ESTRATÉGICOS DEL BANCO AGRARIO DE COLOMBIA

Este documento es una síntesis de referencia y está dirigido a proveedores y aliados estratégicos del Banco, para el cumplimiento de las obligaciones descritas en los **Lineamientos para la aplicación de la Política General de Seguridad de la Información y Ciberseguridad del Banco Agrario de Colombia.**

LINEAMIENTO 1 – Gestión de activos de información

1. Reglas para la gestión de los activos de información:

    a. Es responsabilidad de los colaboradores del Banco, entes reguladores y proveedores, que acceden a la información del BAC o de sus clientes y usuarios, atender las directrices establecidas en este documento para gestionar los activos de información a los cuales tienen acceso en desarrollo de sus funciones.

    b. Los colaboradores y proveedores no deben usar dispositivos personales (computadores, tabletas, teléfonos móviles, otros) en las áreas donde se ejecuten operaciones o transacciones bancarias. Los líderes de área deben hacer cumplir esta directriz.

2. Clasificación, etiquetado y disposición final de la información:

    a. La Vicepresidencia de Tecnología e Innovación, a través de sus gerencias, debe garantizar las medidas de seguridad necesarias para asegurar la disponibilidad y prevenir fugas, accesos y/o modificaciones no autorizadas de la información pública clasificada y pública reservada alojada en los servidores y servicios que se encuentren en la nube corporativa. Para los servicios de computación en la nube, el proveedor contractualmente debe certificar los controles que aseguran la protección y custodia de la información del Banco.

3. Derechos de autor:

    a. Los colaboradores del Banco, o proveedores que requieran utilizar información de libros, artículos, reportajes, documentos, registros comerciales, fotos, videos o audios, para elaborar documentos relacionados con sus funciones asignadas, lo podrán hacer dentro de lo permitido por la Ley de derechos de autor citando como referencia el sitio de donde fue tomada la información.

    b. Ningún colaborador del Banco (directo o indirecto), proveedor está autorizado para instalar software no autorizado o almacenar en su equipo de trabajo o en los activos que tiene asignados para el desarrollo de sus labores elementos multimedia tales como: fotos, vídeos o audios personales.

LINEAMIENTO 2 – Control de acceso lógico

a. Los colaboradores y proveedores que administran servicios en la red de datos corporativa, en los servicios de computación en la nube y/o en aplicaciones del Banco son los responsables de autorizar, verificar y actualizar los roles de acuerdo con la sensibilidad de la información que procesan, transmitan y/o almacenen y acorde con las actividades que desarrollen, según el procedimiento [Actualización de roles Core bancario y aplicativos externos].

b. Los colaboradores y proveedores del Banco, a los que se haya asignado usuarios de red con acceso a sistemas operativos y aplicaciones, deben asegurar la confidencialidad de las credenciales de acceso, que son personales e intransferibles, y en ninguna circunstancia deben prestarse, ni compartirse. Está prohibido utilizar las credenciales de acceso de otros usuarios para acceder a los sistemas de información del Banco.

c. La Vicepresidencia de Tecnología e Innovación a través de sus gerencias y los proveedores que administren activos tecnológicos en la red corporativa del BAC o en los servicios de computación en la nube, deben implementar y configurar en los recursos informáticos de (hardware y software) los registros de auditoría, para el seguimiento y control de las acciones que allí se desarrollen.

LINEAMIENTO 5 – Traslado de información.

a. Los colaboradores del Banco y proveedores que en el desarrollo de sus funciones administren información pública clasificada y/o pública reservada de o a cargo del Banco Agrario de Colombia, deberán mitigar los riesgos asociados a la pérdida de la confidencialidad, integridad, privacidad o disponibilidad de la información, máxime durante el tratamiento y transporte de esta por los sistemas de información; para tal fin, deben conocer y atender las Leyes de Transparencia (Ley 1712 de 2014), de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios), de Comercio Electrónico (Ley 527 d e 1999), de Habeas Data (Ley 1266 de 2008), de Servicios de Computación en la Nube (Circular Externa 005 de marzo de 2019), Requerimientos Mínimos para la Gestión de la Seguridad de la Información y Ciberseguridad (Circular Externa 007 de Junio de 2018) y cualquier otra norma que las modifique, sustituya y/o adicione.

b. Los colaboradores del Banco y proveedores deben velar por que el transporte de la información se gestione empleando canales de datos seguros (físicos o lógicos), que permitan brindar los niveles de confidencialidad, privacidad e integridad conforme al nivel de clasificación de la información.

c. Los colaboradores que gestionan la recepción o el transporte de información pública clasificada y pública reservada con proveedores, aliados estratégicos o gremios productivos deben formalizar con ellos el cumplimiento de los [Lineamientos de seguridad de la información y ciberseguridad del Banco] y la normatividad colombiana vigente, circular externa 042 de 2012 o la que la sustituya o modifique.

LINEAMIENTO 6 – Respaldo de la información.

1. Información estructurada:

    a. Las áreas que adelanten procesos de contratación deben asegurar que se incluya contractualmente con los proveedores, la obligación de contar con procedimientos y herramientas tecnológicas para realizar copias de respaldo a la información que se almacenará en las instalaciones externas al Banco, de acuerdo con lo establecido en el lineamiento de [Relaciones con los Proveedores].

LINEAMIENTO 7 – Seguridad de las operaciones y comunicaciones.

1. Software malicioso:

Los colaboradores, proveedores que utilicen los recursos tecnológicos del Banco, deben acatar las siguientes recomendaciones:

    a. Ejecutar el software de antivirus, antispyware, antispam y antimalware sobre los archivos y/o documentos abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen de cuentas de correo electrónico desconocidas.

    b. Validar que los archivos adjuntos en los correos electrónicos, descargados de internet o copiados desde cualquier medio de almacenamiento, provienen de fuentes conocidas.

    c. Notificar de manera inmediata a la Gerencia de Ciberseguridad sobre alguna infección por software malicioso a través del buzón incidentes.seguridad@bancoagrario.gov.co, quienes gestionarán las medidas de control correspondientes.

2. Gestión de Incidentes de seguridad de la Información y Ciberseguridad.

Los colaboradores, aliados estratégicos y proveedores a través del supervisor del contrato deben:

- Notificar a la Gerencia de Ciberseguridad y Riesgo Operativo, a través del medio que esta defina, los incidentes identificados, la pérdida, fuga o divulgación no autorizada de información pública clasificada o pública reservada.

3. Continuidad del negocio:

El Banco facilitará los recursos que se requieran para proporcionar una respuesta efectiva de colaboradores y procesos, en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de la operación critica del negocio. Para las aplicaciones en la nube, contractualmente la responsabilidad le compete al proveedor garantizar la ejecución exitosa de los planes de continuidad, para lo cual el Banco solicitará la respectiva certificación.

4. Manejo de medios de almacenamiento. (USB, CD, cintas, discos extraíbles):

La Vicepresidencia de Tecnología e Innovación debe implementar herramientas para la detección y contención de código malicioso que puedan ser ejecutados desde los medios de almacenamiento extraíbles y afecten la confidencialidad, disponibilidad e integridad de la información. Los proveedores de servicios en la nube deben cumplir con este requerimiento.

LINEAMIENTO 10 – Puesto de trabajo seguro, pantalla limpia

1. Puesto de trabajo seguro:

    a. Los colaboradores, aliados estratégicos y proveedores son responsables de custodiar la información pública clasificada y pública reservada, a cargo del Banco, durante y fuera de la jornada laboral o en su ausencia temporal del puesto de trabajo, en periodos de las vacaciones, en incapacidades o cualquier otra novedad que genere un ausentismo de forma tal, que no sea consultada o accedida por personas no autorizadas.

    b. Los colaboradores, aliados estratégicos y proveedores deben garantizar la preservación y custodia de los documentos físicos o medios magnéticos, (por ejemplo, medios removibles) que contengan información catalogada como pública clasificada o pública reservada, en los lugares definidos por el Banco.

    c. Los colaboradores, aliados estratégicos y proveedores son responsables de preservar, cuidar y velar por el buen funcionamiento de los equipos de cómputo, puestos de trabajo y archivadores que les han sido asignados para la custodia de documentos con información de o a cargo del Banco.

2. Pantalla limpia:

Los colaboradores, aliados estratégicos y proveedores deben cerrar y/o bloquear la sesión de acceso al equipo de cómputo asignado (escritorio o portátil), o los servicios en red cada vez que se ausenten de su puesto de trabajo y/o una vez finalizada la sesión de uso, con el fin de evitar acceso no autorizado a la información.

3. Impresoras.

Los colaboradores, aliados estratégicos y proveedores que, en ejercicio de sus funciones, impriman información catalogada como pública clasificada o pública reservada en impresoras, fotocopiadoras o escáner, tienen la responsabilidad de retirar los documentos inmediatamente al momento de reproducirlos.

LINEAMIENTO 12 – Servicios de red.

1. Servicio Correo Electrónico.

Los colaboradores, aliados estratégicos y/o proveedores que utilicen el servicio de correo electrónico corporativo, son responsables de acatar las directrices sobre el uso adecuado y protección de la información de propiedad o a cargo del Banco.

a. El servicio de correo electrónico corporativo se utilizará para enviar y recibir mensajes relacionados con las tareas propias del rol designado en el Banco para cada cargo; no se debe enviar información pública clasificada o pública reservada a correos electrónicos personales. En caso de ser necesario se solicitará la autorización al propietario de la información en el Banco.

b. Los siguientes usos del correo electrónico corporativo son considerados como inadecuados y se gestionarán como incidentes de seguridad de la información, atendiendo el procedimiento [Gestión de eventos e incidentes]:

- Enviar correos masivos (cadenas de correo) con cualquiera de los siguientes contenidos: político, religioso, servicio social, discriminatorios, publicitario o pornográficos.
- Enviar o intercambiar mensajes con contenido que atente contra la ética o contra la integridad moral de las personas, la imagen del Banco Agrario de Colombia o de otras entidades; contra las regulaciones o normas sujetas de cumplimiento por el Banco.
- Crear, almacenar o intercambiar mensajes que violen las leyes que protegen: los derechos de autor, las normas sobre seguridad de la información y ciberseguridad y la protección de datos personales.
- Suplantar la identidad de otro usuario para revisar, crear, enviar, alterar o borrar mensajes utilizando la cuenta de correo del usuario suplantado.
- Utilizar cuentas de correo diferentes de la corporativa para el envío o recepción, de información de tipo pública clasificada y/o pública reservada del Banco Agrario de Colombia.

2. Uso de Internet:

Es responsabilidad de los colaboradores, aliados estratégicos y proveedores con acceso al servicio de navegación en Internet, utilizarlo adecuadamente, atendiendo las disposiciones de navegación definidas por el Banco:

a. Los colaboradores, aliados estratégicos y proveedores del Banco que divulguen información pública clasificada o pública reservada en redes sociales a la que tienen acceso en ejercicio de sus funciones, son responsables a título personal y en consecuencia podrán adelantarse acciones legales y administrativas en su contra.

b. Las siguientes acciones de navegación en Internet en la red corporativa del Banco, no

están autorizadas y pueden catalogarse como un incidente de seguridad de la información y se gestionarán de acuerdo con el procedimiento [Gestión de eventos e incidentes]:

- Acceder a sitios de juegos o apuestas en línea, webcam, páginas pornográficas u ofensivas.
- Descargar o distribuir películas, videos, música, audios, Streaming, salvo excepciones autorizadas.
- Utilizar software o servicios de mensajería instantánea (chat) y redes sociales no autorizadas.
- Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.
- Compartir en sitios web no autorizados la información catalogada como pública clasificada y/o pública reservada del Banco.
- Alterar la configuración de los equipos de cómputo para acceder a páginas no autorizadas.

LINEAMIENTO 13 – Relación con los proveedores.

Alcance: El lineamiento registra los controles y los criterios de seguridad de la información, ciberseguridad y protección de datos de obligatorio cumplimiento contractual para los aliados estratégicos y proveedores y/o Terceros Receptores de datos en el marco de las finanzas abiertas con quienes se transfiera, trasmita, intercambie, almacene, procese y transporte información (pública, pública clasificada o pública reservada) en forma física o digital del Banco.

- Los proveedores, aliados estratégicos y subcontratistas, deben cumplir con las leyes, normativas y regulación colombiana asociada con la protección de la información, presentar las certificaciones correspondientes y procedimientos que evidencien el manejo seguro de la información y la atención de la ciberseguridad. Los supervisores de contratos del BANCO deben velar porque estas obligaciones se incluyan como anexo y/o parte integral del servicio contratado y que puedan ser verificadas en cualquier momento por la Gerencia de Riesgo Operativo. Para los terceros receptores de datos (TRD) en el marco de las finanzas abiertas, la Gerencia encargada de su administración debe solicitar a la Gerencia de Riego Operativo la verificación de los requisitos de seguridad y ciberseguridad, previo a su vinculación y debe exigir en los acuerdos contractuales el cumplimiento de los requisitos de seguridad y ciberseguridad establecidos en la Circular Externa 004 de 2024 emitida por la Superintendencia Financiera de Colombia.

- La Vicepresidencia Jurídica a través de la gerencia que designe en coordinación con la Gerencia de Compras y Contratación de la Vicepresidencia Administrativa, debe incluir cláusulas de confidencialidad en los contratos y acuerdos de servicio donde se intercambie información pública clasificada o pública reservada, comprometiendo al proveedor, sus empleados y a los subcontratistas (si los hubiere) a guardar absoluta reserva sobre la información a la que tengan acceso (acorde al servicio contratado) y establecer la calidad de encargado y/o custodio temporal de datos personales según lo establecido en la Ley 1581

de 2012 y sus decretos reglamentarios. Para los Terceros Receptores de Datos la Gerencia designada de su administración deberá asegurar la inclusión de estos requisitos.

- La Gerencia de Riesgo Operativo realiza visitas de seguimiento a los proveedores y/o subcontratistas que procesan información clasificada y reservada, incluidos los terceros receptores de datos en el marco de las finanzas abiertas, acorde con lo establecido en el procedimiento de Análisis de Riesgos de Seguridad de la Información, para verificar el cumplimiento de los controles de seguridad de la información y ciberseguridad con base en la Norma técnica NTC-ISO-IEC 27001 y la norma PCI DSS y/o normatividad aplicable de acuerdo con el objeto del contrato incluido el cumplimiento de los planes de continuidad del negocio.
-

Nota: Cualquier duda o inquietud sobre el presente documento, favor canalizarla a través del supervisor del contrato, o responsable del convenio o acuerdo. Designado por el Banco