POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

MACROPROCESO

GESTIONAR EL RIESGO DE LA INFORMACIÓN

Aprobaciones	
Dueño de Proceso: Jairo Francisco González Matallana	Helber Alonso Melo Hernández
Cargo: Gerente de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad	**Cargo:** Vicepresidente de Riesgos

TABLA DE CONTENIDO

1. OBJETIVO GENERAL 3
2. ACCIONES Y HERRAMIENTAS 3
3. ALCANCE 3
4. ORGANIZACIÓN Y RESPONSABILIDADES 4
5. PRINCIPIOS 4
6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 5
7. POLÍTICAS INDIVIDUALES 5
7.1. ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD 5
7.2. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 5
7.3. SEGURIDAD DEL RECURSO HUMANO 6
7.4. GESTIÓN DE ACTIVOS DE INFORMACIÓN 6
7.5. GESTIÓN DE ACCESOS 7
7.6. CRIPTOGRAFÍA 7
7.7. SEGURIDAD FÍSICA Y AMBIENTAL 7
7.8. CULTURA EN SEGURIDAD Y CIBERSEGURIDAD 8
7.9. GESTIÓN DE AMENAZAS Y CIBERAMENAZAS 8
7.10. PROCESOS DE ADMINISTRACIÓN DE SISTEMAS E INFRAESTRUCTURA 8
7.11. SEGURIDAD EN TELECOMUNICACIONES 9
7.12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE 9
7.13. GESTIÓN DE TERCEROS 9
7.14. GESTIÓN DE INCIDENTES 10
7.15. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN CONTINUIDAD DE NEGOCIO 10
7.16. GESTIÓN DE CUMPLIMIENTO REGULATORIO 10
8. IMPLANTACIÓN Y PROGRAMACIÓN DE LAS POLÍTICAS 11
9. CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LAS POLÍTICAS 11
10. ADMINISTRACIÓN DE LAS POLÍTICAS Y PROCEDIMIENTO DE CAMBIO 11
11. EXCEPCIONES A LAS POLÍTICAS 11
12. ANEXO 1 – DESCRIPCIÓN DE ROLES Y RESPONSABILIDADES 12

CONTROL DE CAMBIOS 19

1. OBJETIVO GENERAL

Establecer los principios, lineamientos, responsabilidades y conductas para mantener un ambiente seguro de la información, mediante la definición de lineamientos enfocados a proteger la confidencialidad, integridad, disponibilidad y privacidad de la información y recursos informáticos del Banco, así como los mecanismos para defenderse y anticipar ataques que puedan comprometer la sostenibilidad del Banco, contribuyendo de esta forma a fortalecer la resiliencia organizacional.

Así mismo, definir el gobierno, políticas individuales y mecanismos de verificación y control que permitan su actualización y vigencia en el tiempo.

2. ACCIONES Y HERRAMIENTAS

Las acciones y herramientas que se tomarán para cumplir el objetivo general son:

- Definir las pautas para el acceso, uso y administración de la información y/o recursos informáticos del Banco, por parte los Usuarios (tales como, empleados directos o en misión, administradores, accionistas, revisoría fiscal), Consumidores Financieros, Terceros (proveedores y contratistas), Entes de Control, Entidades Relacionadas y Filiales del Banco.
- Definir las pautas para la administración de riesgos de Seguridad de la Información y Ciberseguridad, alineadas al marco de gestión de riesgo Corporativo y acorde con el apetito de riesgo definido por el Banco.
- Establecer los fundamentos para la definición y desarrollo del Sistema de Gestión de Seguridad de la Información y Ciberseguridad del Banco.
- Definir los lineamientos que se deben seguir para que la Alta Dirección del Banco se mantenga informada de los riesgos de Seguridad de la Información y Ciberseguridad y las acciones implementadas por los Responsables de la información para su tratamiento.
- Fomentar una cultura en Seguridad de la Información y Ciberseguridad en los Usuarios relacionados anteriormente.
- Proteger la imagen, los intereses y el buen nombre del Banco.

3. ALCANCE

La presente Política de Seguridad de la Información y Ciberseguridad define el marco base que guiará la implementación de cualquier directriz, sistema, proceso, procedimiento, y/o acción, relacionados con Seguridad de la Información y Ciberseguridad en el Banco.

Esta Política aplica para todos los niveles de la organización: Usuarios, Consumidores Financieros, Terceros, Entes de Control, Entidades Relacionadas y Filiales del Banco;

que acceden o hacen uso de la información y/o recursos informáticos del mismo. Adicionalmente, la presente Política aplica a toda la información creada, procesada, almacenada o utilizada en el soporte al Banco, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

Las definiciones propias contenidas en este documento, pueden consultarse en el documento anexo DE-058-0 Definiciones.

4. ORGANIZACIÓN Y RESPONSABILIDADES

Los principales roles y responsabilidades de la Organización de Seguridad de la Información y Ciberseguridad se encuentran definidos en el Anexo 1 – Descripción de Roles y Responsabilidades, al final del presente documento.

5. PRINCIPIOS

Con el fin de dar cumplimiento a los objetivos del Banco, se han establecido como fundamentales los siguientes principios en los cuales se basa la Política de Seguridad de la Información y Ciberseguridad:

- **Principio estratégico:** La información es uno de los activos vitales para la operación del Banco y por lo tanto debe poseer un adecuado nivel de protección.
- **Principio de gobernabilidad:** Las faltas a las responsabilidades asignadas en la Política y Directrices de Seguridad de la Información y Ciberseguridad ocasionan sanciones de acuerdo con lo estipulado en la presente política.
- **Principio de confidencialidad:** La confidencialidad de la información del negocio debe ser mantenida acorde con las legislaciones, políticas y directrices definidas.
- **Principio de Integridad:** está relacionado con la precisión y completitud de la información, así como con su validez de acuerdo a las necesidades y expectativas del Banco.
- **Principio de disponibilidad:** la información esté disponible cuando sea requerida, así como los recursos y las capacidades necesarias asociadas.
- **Principio de privacidad:** es la necesidad de preservar y proteger los datos personales recopilados por el Banco, para que no sea accedida por un tercero crítico.
- **Principio de no repudio:** La realización de negocios electrónicos debe asegurar el establecimiento de logs y rastros de las transacciones, que le permitan al Banco resolver conflictos cuando una o algunas de las partes niegue su participación.
- **Principio de cumplimiento:** las políticas, directrices y procesos de Seguridad de la Información y Ciberseguridad deberán cumplir y estar alineados con los requerimientos de la normatividad aplicable al Banco.

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Política de Seguridad de la Información y Ciberseguridad: El Banco Popular es consciente que la información, independiente del medio en que se encuentre, es un activo vital y debe ser protegida para asegurar el correcto desarrollo de sus operaciones, por ello, declara su compromiso desde la Alta Dirección en el desarrollo de las habilidades, competencias y asignación de recursos técnicos y humanos necesarios para proteger su información y la de sus consumidores financieros, a través de la implementación de mecanismos y protocolos que permitan fortalecer sus capacidades para protegerse, resistir y reaccionar ante amenazas internas y/o amenazas en el ciberespacio, que puedan comprometer la confidencialidad, integridad, disponibilidad y privacidad de la información; todo ello, teniendo en cuenta la dimensión y el nivel de exposición al riesgo del Banco.

7. POLÍTICAS INDIVIDUALES

7.1. ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD

Política: La Alta Dirección velará por el desarrollo y mantenimiento del Sistema de Gestión de Seguridad de la información y Ciberseguridad del Banco, mediante la asignación dentro de los parámetros presupuestales de la Entidad, de los recursos necesarios para su ejecución y mantenimiento.

El Banco dispondrá de un Sistema de Gestión de Seguridad de Información y Ciberseguridad basado en prácticas líderes, que cumpla con la normatividad nacional e internacional alineado a la estrategia, objetivos y metas del Banco. Así mismo, dispondrá de los recursos adecuados para la operación, incluyendo la estructura encargada de definir, desarrollar y operar el Sistema, asignando funciones y responsabilidades para cada una de las partes relacionadas en el Anexo 1 y estableciendo el presupuesto para su correcto funcionamiento.

Anualmente se realizará un proceso de revisión y actualización a las políticas, directrices, sistema, procesos y procedimientos de Seguridad de la Información y Ciberseguridad el cual también realizará ante situaciones que lo ameriten, para mantenerlas actualizadas ante amenazas y Ciberamenazas que puedan afectar al Banco.

7.2. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Política: Los riesgos de Seguridad de la Información y Ciberseguridad a los que está expuesta la información y los activos de información del Banco deben ser identificados, analizados, evaluados y tratados de acuerdo con el valor de la información, probabilidad de ocurrencia e impacto.

La información y activos de información del Banco se protegerán con base en su criticidad y riesgos en que se puedan ver comprometidos; por lo tanto se contará con un

modelo de gestión de riesgos de Seguridad de la Información y Ciberseguridad, alineado con el marco de gestión de riesgos Corporativo, que permita identificar amenazas internas y amenazas en el Ciberespacio, determinar o actualizar el valor relativo de la información, valorar el nivel de riesgo a que está expuesta la información y determinar las acciones requeridas para su protección, de acuerdo con lo que defina la Junta Directiva.

El Banco contará con un proceso de revisión y actualización de la gestión de riesgos de Seguridad de la Información y Ciberseguridad, para adecuarlo frente a las amenazas que surjan en el uso, desarrollo o creación de nuevas tecnologías (Riesgos Emergentes).

7.3. SEGURIDAD DEL RECURSO HUMANO

Política: El Banco proveerá los mecanismos necesarios para asegurar que los empleados cumplan con sus responsabilidades en Seguridad de la Información y Ciberseguridad desde su ingreso hasta su retiro.

El Banco verificará los antecedentes de sus empleados y terceros críticos relacionados en forma previa a su contratación, e igualmente se incluirá dentro de los contratos las cláusulas que especifiquen las obligaciones referidas al manejo y cuidado de la información del Banco.

Adicionalmente, dependiendo del rol que vaya a desempeñar el empleado o tercero crítico, se especificarán dentro de sus funciones, las responsabilidades correspondientes a la Seguridad de la Información y Ciberseguridad y el cumplimiento de lo establecido en el Código de Ética y Conducta del Banco.

7.4. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Política: La información, independiente del medio en que se encuentre, es un activo vital para la operación del Banco y por tanto deberá ser clasificada y protegida según su importancia y valor y administrada adecuadamente para asegurar su integridad, disponibilidad, confidencialidad y privacidad.

El Banco definirá una metodología de gestión de activos de la información para realizar la identificación, inventario, clasificación, asignación y valoración de la misma, definiendo los Responsables de los activos de información quienes velarán por su correcta protección de acuerdo con los lineamientos definidos por el Banco.

Los activos de información se clasificarán y tratarán de acuerdo con su naturaleza, ubicación e impacto, así mismo, se implementarán controles que permitan tratar posibles amenazas, de acuerdo con su criticidad y valor para el Banco.

7.5. GESTIÓN DE ACCESOS

Política: El uso de la información del Banco será controlado para prevenir accesos no autorizados. Los privilegios de acceso a la información serán mantenidos en concordancia con las necesidades de las áreas los riesgos identificados, limitando el acceso a los empleados solamente a la información requerida de acuerdo con sus funciones.

Se establecerán mecanismos de control de acceso físico y lógico para asegurar que los activos de información se mantengan protegidos de una manera consistente con su valor para el Banco y estableciendo medidas para tratar los riesgos de pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información.

El Banco contará con una metodología de gestión del ciclo de vida de administración de usuarios, garantizando que cada empleado o tercero crítico del Banco tenga un único usuario de acceso, el cual contará con las restricciones y permisos previamente definidos por su superior inmediato. El acceso a los recursos del Banco se enmarcará dentro de las premisas de necesidad de conocer y menor privilegio posible.

7.6. CRIPTOGRAFÍA

Política: El Banco utilizará sistemas lógicos o físicos para el aseguramiento de la confidencialidad e integridad de la información, por medio de controles criptográficos como claves o llaves criptográficas, firmas digitales, certificados y/o algoritmos de cifrado.

Para el almacenamiento y/o transmisión de información sensible, se establecerá el uso de controles criptográficos con el fin de asegurar la información, evaluando y disponiendo de los mecanismos tecnológicos requeridos en cada caso.

7.7. SEGURIDAD FÍSICA Y AMBIENTAL

Política: Todas las áreas físicas del negocio tendrán un nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas. La información sensible se mantendrá en lugares con acceso restringido cuando no sea utilizada.

La seguridad física del Banco se basará en perímetros y áreas seguras, las cuales serán protegidas por medio de controles circundantes apropiados.

La infraestructura tecnológica propia del Banco o administrada por un tercero, contará con mecanismos de seguridad físicos y ambientales para prevenir su exposición, daño o pérdida, así como eventos de seguridad que puedan causar interrupción a las actividades del mismo.

7.8. CULTURA EN SEGURIDAD Y CIBERSEGURIDAD

Política: El Banco desarrollará programas de capacitación y concientización con el fin de proporcionar instrucción suficiente a sus empleados, usuarios y terceros críticos para adoptar una cultura en Seguridad de la Información y Ciberseguridad.

El Banco contará con un programa permanente de capacitación y concientización que permitirá a los empleados, usuarios y terceros críticos estar informados acerca de sus responsabilidades frente a la Seguridad de la Información y Ciberseguridad, así como las amenazas y Ciberamenazas que puedan afectar al Banco. Dicho programa incluirá ejercicios de pruebas enfocados a los diferentes niveles de la organización con el fin de medir el nivel de concientización alcanzado, generando indicadores para medir su efectividad.

Los empleados del Banco participarán en las actividades definidas en el programa, así como las charlas de actualización desarrolladas anualmente y se implementarán medidas para informar a los consumidores financieros sobre las recomendaciones de Seguridad de la Información y Ciberseguridad para la protección de su información.

7.9. GESTIÓN DE AMENAZAS Y CIBERAMENAZAS

Política: El Banco dispondrá de los recursos necesarios para implementar un programa de gestión de amenazas y ciberamenazas que puedan impactar la confidencialidad, integridad, disponibilidad y privacidad de la información del Banco.

El Banco contará con un procedimiento de revisión periódica de amenazas internas y ciberamenazas que puedan afectar sus activos de información e implementará planes de identificación, anticipación, remediación inmediata y defensa, priorizando de acuerdo a su nivel de criticidad para el Banco.

7.10. PROCESOS DE ADMINISTRACIÓN DE SISTEMAS E INFRAESTRUCTURA

Política: El Banco administrará y gestionará sus sistemas e infraestructura tecnológica bajo estándares de seguridad y prácticas líderes, implementando directrices y procedimientos que le permitan llevar a los responsables un debido control y aseguramiento.

Las áreas encargadas de administrar la información y recursos tecnológicos del Banco, implementarán procesos y procedimientos para administrar los de sistemas e infraestructura, teniendo en cuenta (i) lineamientos de Seguridad de la Información y Ciberseguridad que contemplen las actividades de monitoreo y gestión oportuna de amenazas, (ii) registros de las acciones ejecutadas por los usuarios y/o administradores, (iii) control de cambios a las plataformas, (iv) establecimiento e implementación de controles en Seguridad de la Información y Ciberseguridad en proyectos y (v) respaldo de información y seguimiento al uso de recursos; con el objetivo de asegurar el desempeño requerido de los sistemas y las plataformas que los soportan.

7.11. SEGURIDAD EN TELECOMUNICACIONES

Política: Las conexiones de red internas y externas del Banco se autenticarán para prevenir que la información sea accedida por personal no autorizado. Igualmente, las conexiones de red contarán con controles que le permitan su protección.

El uso de medios y canales de comunicación se regirán por las directrices de Seguridad de la Información y Ciberseguridad definidas por el Banco y sujetos a evaluación periódica.

La arquitectura de seguridad de la información de las redes del Banco, incluirá el uso de controles de red basados en monitoreo, segmentación, cifrado, bloqueo y limitación de sistemas remotos.

7.12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE

Política: Las adquisiciones, desarrollos, mantenimientos y cambios en las plataformas o sistemas de información del Banco contemplarán e implementarán los requerimientos de Seguridad de la Información y Ciberseguridad. En el caso de no cumplir con los requerimientos mínimos exigidos, se establecerán controles complementarios que mitiguen los riesgos identificados.

El desarrollo de los proyectos e iniciativas tecnológicas del Banco contarán, desde sus fases iniciales, con un análisis de Riesgos de Seguridad de la Información y Ciberseguridad. Dichos requerimientos se implementarán y probarán previo a su paso a operación. El nivel de seguridad de un sistema no se verá disminuido por las modificaciones o actualizaciones realizadas.

La adopción de tecnologías emergentes (v.gr., computación en la nube) cumplirá con evaluaciones de Seguridad de la Información y Ciberseguridad, en donde se identifiquen los riesgos para el Banco en la adopción de estas tecnologías y se definan controles mínimos que den cumplimiento a las directrices de Seguridad de la Información y Ciberseguridad y a las regulaciones existentes.

7.13. GESTIÓN DE TERCEROS

Política: El Banco dentro de su proceso de contratación de bienes y/o servicios con terceros, realizará un proceso de evaluación de Riesgos de Seguridad de la Información y Ciberseguridad de los terceros.

El Banco contará con una metodología de evaluación de riesgos y ciberiesgos de los terceros, identificando los terceros críticos para Seguridad de la Información y Ciberseguridad y estableciendo planes de acción para los riesgos que estén por fuera del nivel de riesgo aceptado por el Banco.

Los empleados del Banco responsables de los contratos con terceros monitorearán regularmente el cumplimiento de los controles de seguridad de la información y ciberseguridad de los terceros a cargo de cada una de las dependencias del Banco.

Se definirán en conjunto con los terceros, canales y protocolos de comunicación que le permitan conocer y gestionar de manera efectiva y rápida el estado de los servicios recibidos, así como los mecanismos para dar respuesta conjunta a incidentes de seguridad que comprometan la información del Banco.

7.14. GESTIÓN DE INCIDENTES

Política: El Banco establecerá un procedimiento de gestión de incidentes de Seguridad de la Información y Ciberseguridad con el fin de dar respuesta a las amenazas y ciberamenazas que puedan comprometer la información del Banco.

El Banco dispondrá de los recursos necesarios para brindar un apropiado monitoreo, detección y gestión de incidentes de Seguridad de la Información y Ciberseguridad, estableciendo procedimientos para el monitoreo de eventos, identificación, respuesta, notificación, recuperación y reanudación.

El Banco informará de forma oportuna a sus partes interesadas cuando se materialice un incidente de Seguridad de la Información y Ciberseguridad que afecten la confidencialidad, integridad, disponibilidad y/o privacidad de la información del Banco o sus consumidores financieros.

7.15. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN CONTINUIDAD DE NEGOCIO

Política: La continuidad de los procesos de Seguridad de la Información y Ciberseguridad estará incluida en los procesos de gestión de la continuidad de negocio, en todas sus fases.

El Banco implementará aspectos de seguridad de la información y ciberseguridad en sus procesos de gestión de continuidad de negocio, asegurando que los niveles de protección, en caso de activación de la contingencia, sean iguales o mayores a los niveles definidos en la operación normal.

El Banco incluirá en sus procesos de pruebas de continuidad de negocio, ejercicios que simulen la materialización de ataques cibernéticos que permitan evaluar la capacidad su respuesta.

7.16. GESTIÓN DE CUMPLIMIENTO REGULATORIO

Política: *Las políticas, directrices, procesos y procedimientos de Seguridad de la Información y Ciberseguridad del Banco estarán acordes con el cumplimiento de las leyes y regulaciones locales e internacionales.*

El Banco dispondrá de procedimientos para la revisión, identificación, documentación y cumplimiento de la legislación y requisitos legales que le aplican en Seguridad de la Información y Ciberseguridad. Estos requerimientos se incluirán en el desarrollo del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, tomando las

acciones específicas para mantener alineado permanentemente al Banco con tales disposiciones.

8. IMPLANTACIÓN Y PROGRAMACIÓN DE LAS POLÍTICAS

La política de Seguridad de la Información y Ciberseguridad involucra el desarrollo e implantación de un programa de Seguridad de la Información y Ciberseguridad integrado a la operación del Banco. Para lograr los objetivos establecidos en este documento, las presentes Políticas anticipan y autorizan el desarrollo de directrices, procedimientos detallados y otras medidas administrativas; así como el desarrollo o la adquisición de los mecanismos preventivos y reactivos, herramientas de software y otras técnicas de protección.

9. CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LAS POLÍTICAS

El cumplimiento de las políticas con sus respectivas directrices, es obligatorio para Usuarios, Consumidores Financieros, Terceros, Entes de Control, Entidades Relacionadas y Filiales del Banco Popular; siempre que accedan o hagan uso de la información del Banco. Cada parte interesada debe entender su rol y asumir sus responsabilidades respecto a la gestión de los riesgos en seguridad de la información y ciberseguridad, manteniendo un ambiente de control adecuado para sus procesos.

Cualquier incumplimiento de esta política que comprometa la confidencialidad, integridad, disponibilidad y/o privacidad de la información, dará lugar a las acciones administrativas internas del caso de acuerdo con lo establecido en la Convención Colectiva y en el Reglamento Interno de Trabajo del Banco, sin perjuicio de las acciones judiciales pertinentes.

10. ADMINISTRACIÓN DE LAS POLÍTICAS Y PROCEDIMIENTO DE CAMBIO

Para asegurar la sostenibilidad de la Política de Seguridad de la Información y Ciberseguridad, la misma será objeto de una revisión anual y de las revisiones periódicas que se requieran por razón de cambios estructurales y tecnológicos que afecten al Banco o de modificaciones normativas, de acuerdo con las responsabilidades establecidas.

Cualquier parte interesada puede identificar la necesidad de modificar la Política de Seguridad de la Información y Ciberseguridad, para lo cual seguirá el procedimiento de actualización definido por el Banco.

11. EXCEPCIONES A LAS POLÍTICAS

No se tienen excepciones a las presentes Políticas.

12. ANEXO 1 – DESCRIPCIÓN DE ROLES Y RESPONSABILIDADES

JUNTA DIRECTIVA

- Estudiar y aprobar la política Seguridad de la Información y Ciberseguridad, según propuesta presentada por la Vicepresidencia de Riesgos.
- Estudiar y aprobar el apetito de riesgo del Banco, según propuesta presentada por la Vicepresidencia de Riesgos.
- Considerar los informes que le presente el Oficial de Seguridad de la Información y Ciberseguridad sobre los resultados de la evaluación de efectividad del programa de seguridad de la información y ciberseguridad, propuestas de mejora en materias de Ciberseguridad y resumen de los incidentes que afectaron al Banco.
- Estudiar y aprobar los recursos que se requieran para el adecuado funcionamiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad dentro de los parámetros presupuestales aprobados por las misma Junta cada año y previo concepto favorable del Presidente del Banco.
- Participar en programas de concientización y capacitación en temas de Seguridad de la Información y Ciberseguridad.

ALTA DIRECCIÓN

- Asegurar la implementación de las estrategias y políticas aprobadas por la Junta Directiva en relación con la Seguridad de la Información y Ciberseguridad.
- Promover el desarrollo de proyectos y/o iniciativas que busquen mejorar los niveles de Seguridad de la Información y Ciberseguridad del Banco.
- Evaluar y proponer los recursos financieros y humanos requeridos para el desarrollo y mantenimiento de las políticas, directrices, procesos y procedimientos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, dentro de la dimensión y nivel de exposición al riesgo del Banco e igualmente en el marco presupuestal correspondiente.
- Participar en programas de concientización y divulgación de temas de Seguridad de la Información y Ciberseguridad.
- Cumplir con las políticas de Seguridad de la Información y Ciberseguridad del Banco.

COMITÉ CORPORATIVO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

- Definir principios, directrices y lineamientos corporativos, entendiendo Banco y sus Filiales, de seguridad de la información y ciberseguridad en función de los objetivos de negocio del Grupo.
- Establecer posición frente a la gestión de riesgos de Seguridad de la Información y Ciberseguridad, a nivel Corporativo.

- Coordinar acciones preventivas y correctivas para el manejo de crisis generadas por los eventos relacionados con los incidentes que afectan la Seguridad de la Información y Ciberseguridad.
- Adelantar investigaciones y mantenerse permanentemente actualizados en forma especializada sobre las nuevas tecnologías de Seguridad de la Información y Ciberseguridad.

COMITÉ DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD DEL BANCO

- Aprobar la estrategia y modelo de Seguridad de la Información y Ciberseguridad, en función de los objetivos del Banco y con base en los lineamientos corporativos.
- Evaluar de forma continua las estrategias, programas y Sistema de Gestión de Seguridad de la Información y Ciberseguridad.
- Fomentar el desarrollo y capacitación de la Unidad de Seguridad de la Información y Ciberseguridad en el Banco.
- Revisar los resultados de los indicadores del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, así como tomar acciones correctivas en caso de ser requerido.

COMITÉ DE AUDITORIA

- revisar y recomendar para aprobación de la Junta Directiva la Política de Seguridad de la Información y Ciberseguridad.

VICEPRESIDENTE DE RIESGOS

- Presentar para aprobación de la Junta Directiva, la política Seguridad de la Información y Ciberseguridad, previo concepto favorable del Presidente.
- Velar por que se implementen las estrategias y políticas aprobadas por la Junta Directiva en relación con la Seguridad de la Información y Ciberseguridad.
- Proponer para aprobación de la Junta Directiva, el apetito de riesgo del Banco, previo concepto favorable del Presidente.
- Disponer de los recursos asignados al área de Seguridad de Información y Ciberseguridad para propender por el adecuado funcionamiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, de conformidad con lo autorizado por la Junta Directiva.
- Apoyar el desarrollo de proyectos y/o iniciativas que busquen optimizar los niveles de Seguridad de la Información y Ciberseguridad del Banco.
- Monitorear, controlar y reportar el resultado de la gestión de riesgos de Seguridad de la Información y Ciberseguridad a la Alta Dirección.

OFICIAL DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

- Diseñar, desarrollar, implementar y actualizar el Sistema de Gestión de Seguridad de la Información y Ciberseguridad en línea con los requerimientos y directrices del Banco.
- Definir lineamientos y políticas para proteger la información de acuerdo con el valor o criticidad definido por los Responsables.
- Asesorar a la Alta Dirección y Junta Directiva en temas que considere necesarios sobre Seguridad de la Información y Ciberseguridad, para que aquellas puedan hacer seguimiento y tomar las decisiones adecuadas.
- Proponer la estructura organizacional requerida para el desarrollo del Modelo de Seguridad de la Información y Ciberseguridad.
- Diseñar y desarrollar indicadores de gestión claros, objetivos y verificables que reflejen el desempeño del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.
- Diseñar y desarrollar el programa de concientización del Banco.
- Comunicar a los Entes de Control y otras partes interesadas los incidentes de Seguridad de la Información y Ciberseguridad, sus impactos y las acciones de remediación tomadas.

UNIDAD DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

- Desarrollar, implementar, actualizar y verificar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad en línea con los requerimientos del Banco.
- Desarrollar y mantener las directrices, los procedimientos y los estándares de Seguridad de la Información y Ciberseguridad.
- Desarrollar, implementar y controlar el Programa de Manejo de Incidentes de seguridad de información y Ciberseguridad.
- Participar en los proyectos que manipulen activos críticos de información definidos por el Responsable de la información, para asegurarse que se apliquen lineamientos definidos de Seguridad de la Información y Ciberseguridad.
- Definir la estrategia de las pruebas de Seguridad de la Información y Ciberseguridad en las aplicaciones o sistemas.
- Evaluar los riesgos en cuanto a la Seguridad de la Información y Ciberseguridad en aplicativos, productos, sistemas operativos, herramientas y redes, según requerimiento del Responsable de la información.
- Realizar pruebas de efectividad a los controles implementados y tomar las medidas necesarias para asegurar su cumplimiento.
- Investigar sobre nuevas formas, productos y servicios de protección informática, que permitan la identificación y desarrollo de iniciativas para fortalecer los niveles de seguridad del Banco.
- Ejecutar revisiones de seguridad a los terceros críticos del Banco para evaluar el grado de cumplimiento de las políticas, directrices de seguridad.

- Revisar el cumplimiento de los lineamientos y directrices de Seguridad de la Información y Ciberseguridad por parte de las diferentes áreas del Banco.
- Definir y ejecutar el programa de concientización y capacitaciones que recibirán regularmente las partes interesadas del Banco, en temas relacionados con seguridad de la información y ciberseguridad y mantenerlos actualizados sobre las nuevas ciberamenazas.

RESPONSABLES DE LA INFORMACIÓN

- Identificar, evaluar, tratar y conocer los riesgos a que podría estar expuesta su información y velar por que se provean los mecanismos necesarios para que estos riesgos se mitiguen a niveles aceptables considerando la relación costo-beneficio para su área.
- Clasificar los activos de información de acuerdo con su criticidad.
- Definir los requerimientos de seguridad de sus activos de información en relación con su confidencialidad, integridad, disponibilidad y privacidad.

Adicionalmente debe definir, entre otros:

  - ¿Quién puede utilizarlo?
  - ¿Qué pueden hacer los usuarios - lectura, escritura, modificación?
  - ¿Bajo qué circunstancias pueden hacerlo?
  - Condiciones para utilizarlo (aprobación escrita, un área específica, etc.)

- Efectuar la auto-evaluación de la correcta ejecución de los controles requeridos sobre los activos de información bajo su responsabilidad, con el apoyo de las áreas correspondientes.

ADMINISTRADORES DE RECURSOS TECNOLÓGICOS

- Aplicar y mantener los estándares de seguridad en los recursos informáticos de su responsabilidad, acorde con los lineamientos y directrices de seguridad de la información y ciberseguridad del Banco y bajo la autorización del Responsable de la información correspondiente.
- Apoyar la implementación de las herramientas de Seguridad de la plataforma bajo su responsabilidad.
- Velar por que los controles de seguridad a los recursos informáticos bajo la autorización del Responsable de la información de la misma se mantengan en el tiempo.
- Monitorear, registrar e informar los eventos de intrusión o uso malicioso de los recursos informáticos de su responsabilidad y reportarlos al Responsable de la información y al Oficial de Seguridad de la Información y Ciberseguridad.

LÍDER DE SEGURIDAD FÍSICA

- Diseñar, desarrollar, implementar, mantener y controlar un programa de seguridad física que incluya la protección de áreas que almacenen información crítica

- Mantener una comunicación directa y efectiva con el área de Seguridad de la Información, participando en investigaciones donde los activos físicos estén comprometidos.

LÍDER DE CAPACITACION

- Apoyar al Líder de Seguridad de la Información y Ciberseguridad en la implantación y desarrollo del Programa de Concientización.
- Generar indicadores que permitan medir, evaluar y tomar acciones para la gestión del Programa de Concientización.

LÍDER DE TALENTO HUMANO

- Apoyar al Líder de Seguridad de la Información y Ciberseguridad en el programa de manejo de incidentes de Seguridad de la Información y Ciberseguridad y evaluación de riesgos.
- Dirigir las acciones administrativas internas establecidas en el Banco por incumplimiento de las políticas de seguridad de la información y ciberseguridad, y/o las judiciales que de acuerdo con las normas aplicables sean necesarias, con el apoyo del Asesor Legal y demás estamentos del banco que se consideren pertinentes.
- Realizar la modificación de los contratos de trabajo de personal y del reglamento interno de trabajo para que incluyan responsabilidades de seguridad de la información y ciberseguridad.

ASESOR LEGAL

- Asesorar en el cumplimiento de las normas legales locales y/o internacionales que afecten al Banco en materia de seguridad de la Información y ciberseguridad.
- Brindar apoyo y asesoramiento para que el Sistema de Gestión de Seguridad de la Información y Ciberseguridad del Banco esté dentro del marco legal correspondiente y cuente con el sustento legal que formalice y haga viable su aplicación.
- Comunicar al Director de Seguridad del Banco cuando se adviertan cambios o novedades en la legislación que afecten la vigencia o haga necesarios ajustes al Sistema de Gestión de Seguridad de la Información y Ciberseguridad del Banco.
- Asesorar al Banco en la implementación o adopción de normas en materia de seguridad de la información y/o ciberseguridad.

COLABORADORES

- Aplicar los lineamientos definidos por el área de Seguridad de la Información y Ciberseguridad que garanticen la protección de la información del Banco.
- Identificar posibles riesgos de Seguridad de la Información y Ciberseguridad e informar a los Responsables de la Información y al área de Seguridad.

- Manejar la información del Banco a su cargo de acuerdo con los niveles de criticidad definidos.
- Utilizar los activos de información exclusivamente para la realización de las labores permitidas dentro y/o fuera del Banco.
- Preservar la seguridad de la información utilizada en el desarrollo de sus funciones.
- Participar en los programas de concientización y capacitación en temas de seguridad de la información y ciberseguridad.
- Y las demás responsabilidades que se consignen en los manuales de funciones.
- No uses tu dirección de correo corporativo, en la inscripción de servicios o promociones con terceros desconocidos, puedes ser víctima de phishing o de algún tipo de malware
- Todos los empleados del banco, sin importar el nivel jerárquico, y/o terceros tienen la obligación y responsabilidad de informar y/o alertar sobre la posible ocurrencia de un incidente de Seguridad de la Información y/o Ciberseguridad…!Si detectas un incidente de seguridad de la información, repórtalo de inmediato a través del Correo electrónico **segurinfo@bancopopular.com.co**

LÍDER DE LA OFICINA DE GOBIERNO DE DATOS O (CDO)

- Conocer y tener en cuenta los principios, políticas y directrices de seguridad de la información y ciberseguridad para el establecimiento de la misión, visión, metas de corto, mediano y largo plazo del gobierno de información.
- Apoyar a los líderes de dominio en la implementación de los controles y responsabilidades definidos por seguridad de la información y ciberseguridad, garantizando la alineación con las políticas.

LÍDER DE SEGURIDAD INFORMÁTICA

- Implementar los mecanismos y controles para resguardar y proteger la información y recursos informáticos de acuerdo con el valor dado por los Responsables de la información y siguiendo los lineamientos emitidos por seguridad de la información y ciberseguridad.
- Administrar y operar las herramientas de Seguridad del Banco.
- Administrar el nivel de seguridad de las aplicaciones basado en la autorización que le otorgue el Responsable de la información.
- Monitorear, registrar, resolver e informar eventos de intrusión o uso malicioso de los recursos informáticos, reportándolos al Responsable de la información y al Director de Seguridad de la Información del Banco.
- Aplicar y mantener los estándares de Seguridad de las plataformas bajo su custodia.

TERCEROS RELACIONADOS CON EL BANCO

- Implementar los lineamientos y directrices definidas por la Unidad de Seguridad de la Información y Ciberseguridad en el desarrollo de los servicios prestados al Banco.
- Establecer un ambiente de control para los riesgos de seguridad de la información y ciberseguridad que afecten los activos de información del Banco.
- Establecer mecanismos de comunicación y coordinación con el Banco, ante la materialización de incidentes de seguridad de la información y ciberseguridad.
- Participar en los programas de concientización y divulgación del Banco en temas de seguridad de la información y ciberseguridad.

CONTROL DE CAMBIOS

HISTORIAL		
# VERSIÓN	**FECHA PUBLICACIÓN**	**DESCRIPCIÓN DEL CAMBIO**
1	15/01/2021	Se crea el documento como reemplazo de la política PO-058-0 Política de seguridad de la información y ciberseguridad.
2	21/09/2021	Se actualiza el documento Política de Seguridad de la Información y Ciberseguridad por cambio de nombre de la Gerencia Oficial Corporativo de Riesgo CRO a la Gerencia Integral de Riesgos
3	17/01/2023	Se actualiza el documento Política de Seguridad de la Información y Ciberseguridad ajustando lo siguiente: •En una de las responsabilidades de los administradores de recursos tecnológicos, se cambia “Director de Seguridad de la Información” por “Oficial de Seguridad de la Información y Ciberseguridad”. •En las responsabilidades de los COLABORADORES, se incluye una especifica relacionada con el reporte de eventos o incidentes, por los canales establecidos al interior del Banco.
4	26/02/2024	Se actualiza Política de Seguridad de la Información y Ciberseguridad, así: • En el numeral 12.ANEXO 1 – DESCRIPCIÓN DE ROLES Y RESPONSABILIDADES, incluyendo el rol de COMITÉ DE AUDITORIA para dar cumplimiento a la circular 008 (Según lo aprobado en Acta de Junta No. 2772, página 11) • Se ajusta el cargo Gerente Integral de Riesgos a Vicepresidente de Riesgos, según el último organigrama aprobado.