BANCO PICHINCHA En confianza.	**Tipo de Macroproceso:** Estratégico	**Código:** PO-DR-SF-03
	Macroproceso: Administración del Riesgo	**Versión:** 1.0
	Procesos: Gestión de Seguridad de Información y Prevención de Fraudes	**Custodio:** Políticas y Relaciones Regulatorias
	Clasificación de la Información: ☐ Pública ☒ Interna ☐ Confidencial ☐ Estrictamente Confidencial	

Política General de Seguridad de la Información y Ciberseguridad

Aprobado por:	Firma de aprobación
Felipe Gomez Bustos **GERENTE DE CIBERSEGURIDAD**	
	Fecha de aprobación: 25/10/2022

CONTROL DE CAMBIOS

VERSIÓN	DETALLE	ELABORADO POR	FECHA DE APROBACIÓN VERSIÓN ANTERIOR	REVISADO POR
1.0	Cambio de nombre **Decia:** Política General de Seguridad de la información **Dice:** Política General de Seguridad de la Información y Ciberseguridad Revisión y actualización de contenido, incorporación de aspectos de ciberseguridad y responsabilidades de 3 líneas de responsabilidad.	Viviana Apolo Márquez **OFICIAL DE GESTIÓN DE RIESGOS DE SI** Paola Orbe **ADMINISTRADOR POLITICAS Y RELACIONES REGULATORIAS**	N/A	Katty Guamán **JEFE DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** Patricio Negrete **GERENTE DE OPERACIONES DE SEGURIDAD** Fernanda Béjarano **JEFE DE ASEGURAMIENTO DE LA CALIDAD DE SEGURIDAD DE LA INFORMACIÓN** Deisi Mosquera **GERENTE DE ARQUITECTURA DE SEGURIDAD** Javier Maldonado **JEFE SEGURIDAD INFORMACION CANALES** Patricio Enriquez Vargas **GERENTE POLITICAY RELACIONES REGULATORIAS** Paulina Guerra **GERENTE RIESGOS NO FINANCIEROS**

INDICE

1. Objetivo

Establecer las directrices y lineamientos aplicables para el Banco en materia de seguridad de la información y ciberseguridad enmarcados en el cumplimiento de las disposiciones normativas y en el marco de la adecuada administración integral de riesgos la cual adopta el esquema de las tres líneas de responsabilidad.

2. Alcance

El alcance de la presente política abarca todos los aspectos administrativos y organizacionales bajo los cuales el Banco diseña, implementa, opera y mejora el Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo en lo anterior el ámbito de ciberseguridad.

La presente política es aplicable a todos los colaboradores, personal externo, terceras partes proveedoras de productos y/o servicios, que acceden a las instalaciones y/o a los activos de información del Banco.

De igual forma, la presente política aplica a todos los activos de información del Banco en cualquiera de sus formas, medios de almacenamiento y distribución, ya sea física o digital.

3. Responsables

3.1 Del Cumplimiento

1. Directorio
2. Alta Gerencia
3. Comité de Seguridad de la Información
4. Gerencia de Ciberseguridad
5. Primera Línea de responsabilidad
6. Segunda Línea de responsabilidad
7. Tercera Línea de responsabilidad

✓ Directorio

Responsable de:

- Delegar un miembro del directorio que participe en las sesiones del Comité de Seguridad de la Información.
- Conocer, revisar y aprobar las resoluciones y acuerdos detallados en las actas del comité de seguridad de la información.
- Asegurar que la entidad cuente con recursos humanos, técnicos y económicos para la implementación del sistema de gestión de seguridad de la información y ciberseguridad.

✓ Alta Gerencia

Responsable de:

- Validar y aprobar los recursos humanos, técnicos y económicos para la implementación del sistema de gestión de seguridad de la información y ciberseguridad.
- Promover la mejora continua del Sistema de Gestión de seguridad (SGSI), e integrando dicho sistema con los procesos del Banco.
- Impulsar una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz de los riesgos de seguridad de la información y ciberseguridad.
- Impulsar la implementación de iniciativas para que toda la organización esté informada acerca de los principales lineamientos de la gestión de seguridad de la información y ciberseguridad, a través de los canales dispuestos por Banco Pichincha.
- Las demás que determine la junta general de accionistas, o que sean dispuestas por la Junta de Política y Regulación Monetaria y Financiera o la Superintendencia de Bancos respecto a Seguridad de la Información y Ciberseguridad.

✓ Comité de Seguridad de la Información

Responsable de:

- Evaluar, supervisar y apoyar el sistema de gestión de seguridad de la información y ciberseguridad.
- Revisar y aprobar las políticas, objetivos, procesos, procedimientos y metodologías de seguridad de la información y ciberseguridad.
- Aprobar los indicadores estratégicos de seguridad de la información y ciberseguridad, y conocer el resultado de los indicadores de monitoreo del cumplimiento y efectividad de los controles establecidos, según el alcance definido.
- Conocer y aprobar el resultado de la evaluación del desempeño del sistema de gestión de la seguridad de la información y ciberseguridad al menos una vez al año.
- Aprobar el plan de seguridad de la información y ciberseguridad.
- Conocer los resultados de auditorías relacionadas con controles de seguridad de información y ciberseguridad y las acciones a ejecutar para abordar los riesgos asociados.
- Comunicar las decisiones tomadas en las sesiones del Comité de Seguridad de la Información directamente al Directorio y mantener informada a la alta gerencia y al comité de administración integral de riesgos.

✓ Gerencia de Ciberseguridad

Responsable de:

- Definir la estrategia y el marco de seguridad de la información y ciberseguridad, alineada a la estrategia institucional.

- Definir y proponer para aprobación del Comité de Seguridad de la Información y del Directorio, las políticas, procesos, procedimientos y metodologías de seguridad de la información y ciberseguridad.
- Liderar el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información y ciberseguridad, involucrando a todas las áreas del Banco.
- Implementar los controles y acciones de mejora identificados y definidos en el plan anual de seguridad de la información y ciberseguridad.
- Establecer métricas para la medición del cumplimiento de la gestión de seguridad de la información y ciberseguridad.
- Evaluar, al menos una vez al año, el desempeño del sistema de gestión de la seguridad de la información y ciberseguridad e incluir las acciones de mejora en el plan anual.
- Reportar la gestión de seguridad de la información y ciberseguridad a la Alta Gerencia y el Directorio, a través del comité de seguridad de la información.

✓ **Primera Línea de responsabilidad**

- Establecer y mantener procesos adecuados para la gestión de operaciones y riesgos de seguridad y ciberseguridad (incluyendo el control interno).
- Implementar acciones preventivas y correctivas para hacer frente a las deficiencias o riesgos a los que se encuentran expuestos en materia de seguridad de la información y ciberseguridad.
- Cumplir con las disposiciones y requisitos establecidos por Ciberseguridad, al igual que las expectativas legales, reglamentarias y éticas.

✓ **Segunda Línea de responsabilidad**

Responsable de:

- Identificar cambios en el Apetito de Riesgo de Seguridad y Ciberseguridad y gestionarlos con la primera línea de responsabilidad
- Monitorear riesgos de Seguridad relacionados con el incumplimiento de leyes y regulaciones aplicables.
- Monitorear la implementación de prácticas efectivas de gestión de riesgos de seguridad de la información y ciberseguridad.
- Alertar de cambios regulatorios y de riesgos de ciberseguridad.

✓ **Tercera Línea de responsabilidad**

Responsable de:

- Evaluar objetiva e independientemente que las unidades y las actividades de la institución relacionadas con la gestión de la seguridad de la información y ciberseguridad cumplan con los lineamientos establecidos a nivel normativo.

- Verificar la eficacia de los controles implementados para mitigar el riesgo de seguridad de la información y ciberseguridad, en cada uno de sus factores y generar los informes respectivos que evidencien dicha labor.
- Revisar en forma periódica la efectividad del sistema de gestión de la seguridad de la información y ciberseguridad.

4. Políticas Generales

1. Banco Pichincha, por medio de su Directorio y Alta Gerencia, apoyará constantemente la implementación y mantenimiento de un sistema de gobierno corporativo, que permita la gestión oportuna relacionada con la seguridad de la información y ciberseguridad.

2. Banco Pichincha tendrá como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya, a fin de establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo el ámbito de ciberseguridad, en cumplimiento con las disposiciones legales, normativas y contractuales internas y externas.

3. La implementación de la función de seguridad de la información y ciberseguridad se establecerá, acorde al tamaño y complejidad de las operaciones del Banco, conformada como mínimo por: un Comité de Seguridad de la Información y Ciberseguridad, un oficial de seguridad de la información y un área independiente y especializada con el personal técnico calificado con la experiencia adecuada.

4. El Banco establecerá las responsabilidades y deberes relativos a la seguridad de la información y ciberseguridad, velará por su permanente actualización y vigencia, incluso después del cambio de funciones o de la terminación de la relación laboral, conforme con lo establecido en el acuerdo de confidencialidad y en virtud de su rol y responsabilidad de acuerdo a las funciones que desempeña.

5. El Banco desarrollará, implementará y mejorará una metodología de gestión de riesgos de seguridad de la información y ciberseguridad, la cual considerará las definiciones de apetito y tolerancia de riesgo aplicables a la materia.

6. Se definirán los procedimientos necesarios para el control y monitoreo de los servicios contratados y del cumplimiento de las definiciones y requisitos en materia de seguridad de la información y ciberseguridad, estableciéndolos formalmente por medio de cláusulas en el respectivo contrato.

7. El Banco deberá identificar y gestionar los riesgos de seguridad de la información y ciberseguridad asociados a la contratación de servicios de infraestructura, plataforma o software incluyendo la computación en la nube, y dar cumplimiento a las disposiciones normativas aplicables.

8. Se coordinará la ejecución de auditorías externas orientadas a evaluar la gestión de seguridad de la información y ciberseguridad, por lo menos una vez al año, o cuando la situación lo amerite.

9. El Banco contratará anualmente con las compañías de seguro privado pólizas de los ramos autorizados por el organismo de control, ante la posible materialización de ciberriesgos de acuerdo a lo señalado en la norma de control para la gestión del riesgo.

10. Las políticas, procesos, procedimientos y metodologías de seguridad de la información y ciberseguridad, así como la estrategia y el marco de ciberseguridad deberán ser revisados, al menos una vez al año, o cuando se produzcan cambios significativos para su posterior aprobación en las instancias formales ya definidas en el Banco.

11. El Banco velará por la permanente concienciación y generación de una cultura de seguridad de la información y ciberseguridad en colaborares y terceros.

12. Los lineamientos contemplados en este documento, están sujetos al cumplimiento de la Norma de Control para la Gestión del Riesgo Operativo, por tanto, es responsabilidad de los dueños de los procesos la oportuna identificación de riesgos e implementación de controles, así como de notificar a la Unidad de Riesgo Operativo para su adecuado seguimiento y monitoreo de manera que permitan minimizar la ocurrencia de posibles eventos de riesgo operativo.

5. Documentos relacionados

- Política de cumplimiento de la seguridad de la información
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos Pblicos de Riesgos Polticas/Política de Cumplimiento de Seguridad de la Información.pdf

- Política de escritorios y pantallas limpias
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos Pblicos de Riesgos Polticas/Política de escritorios y pantallas limpias.pdf

- Política para la asignación, reemplazo, uso y disposición de dispositivos de usuario final

- Política de seguridad de la información para la gestión del talento humano
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos%20Pblicos%20de%20Riesgos%20Polticas/Poli%cc%81tica%20de%20seguridad%20de%20la%20informacio%cc%81n%20para%20la%20gestio%cc%81n%20del%20talento%20humano.pdf

- Política de organización interna de seguridad de la información
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos%20Pblicos%20de%20Riesgos%20Polticas/Poli%cc%81tica%20de%20organizacio%cc%81n%20interna%20de%20seguridad%20de%20la%20informacio%cc%81n.pdf

- Política de seguridad de información para el trabajo remoto/teletrabajo
  https://pichinchanetbp.bpichincha.com/docs/politicas/Historial%20de%20Documentos%20de%20Riesgos%20Polticas/P%C3%BAblico_Pol%C3%ADtica%20de%20seguridad%20de%20informaci%C3%B3n%20para%20el%20trabajo%20remoto%20teletrabajo_v1_0.pdf

- Política de Gestión de Activos de Información
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos%20Pblicos%20de%20Riesgos%20Polticas/Pol%C3%ADtica%20de%20gesti%C3%B3n%20de%20activos%20de%20informaci%C3%B3n.pdf

- Política de Seguridad de Ia Información para la Gestión de Accesos
  https://pichinchanetbp.bpichincha.com/docs/politicas/Historial%20de%20Documentos%20de%20Riesgos%20Polticas/P%C3%BAblico_Pol%C3%ADtica%20de%20seguridad%20de%20Ia%20informaci%C3%B3n%20para%20la%20gesti%C3%B3n%20de%20accesos_v1_0.pdf

- Política de SI para el uso de controles criptográficos
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos%20Pblicos%20de%20Riesgos%20Polticas/Pol%C3%ADtica%20de%20SI%20para%20el%20uso%20de%20controles%20criptogr%C3%A1ficos.pdf

- Política de seguridad física y ambiental
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos%20Pblicos%20de%20Riesgos%20Polticas/Pol%C3%ADtica%20de%20Seguridad%20F%C3%ADsica%20y%20Ambiental.pdf

  Política de Gestión del Desarrollo, Adquisición y Mantenimiento de Software
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos%20Pblicos%20de%20Riesgos%20Polticas/Pol%C3%ADtica%20de%20SI%20para%20la%20adquisici%C3%B3n,%20desarrollo%20y%20mantenimiento%20de%20sistemas.pdf

- Política de SI aplicada en la gestión de terceros
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos%20Pblicos%20de%20Riesgos%20Polticas/Pol%C3%ADtica%20de%20SI%20aplicada%20a%20la%20gesti%C3%B3n%20de%20terceros.pdf

- Política de Gestión de Incidentes de Ciberegurídad
  https://pichinchanetbp.bpichincha.com/docs/politicas/Historial%20de%20Documentos%20de%20Riesgos%20Polticas/P%C3%BAblico_Pol%C3%ADtica%20de%20gesti%C3%B3n%20de%20incidentes%20de%20seguridad%20de%20la%20informaci%C3%B3n_v1_0.pdf

- Política de redes y comunicaciones
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos Pblicos de Riesgos Polticas/Politica de redes y comunicaciones.pdf

- Política de operación de TI
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos Pblicos de Riesgos Polticas/Política de Operación de TI.pdf

- Política para la implementación de servicios tecnológicos en la nube
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos Pblicos de Riesgos Polticas/Política para la implementación de servicios tecnológicos en la nube.pdf

- Política de Gestión de Activos Tecnológicos
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos Pblicos de Riesgos Polticas/Política de Gestión de Activos Tecnológicos.pdf

- Política de seguridad de datos e información

- Política de gobierno de datos
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos Pblicos de Riesgos Polticas/Politica Gobierno de Datos.pdf

- Política para la Administración de Riesgo Operativo
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos Pblicos de Riesgos Polticas/Política para la administración de Riesgo Operativo.pdf

- Política de Gestión de Límites de Apetito de Riesgo
  https://pichinchanetbp.bpichincha.com/docs/politicas/Documentos Pblicos de Riesgos Polticas/Política de gestión de límites de apetito de riesgo.pdf

- Metodología de gestión de riesgos de seguridad de la información

- Metodología de evaluación de criticidad, sensibilidad y accionabilidad.

- Metodología de clasificación de información.

- Metodología de seguridad en terceros

6. Glosario

- **Seguridad de la información**: es el conjunto de medidas y técnicas que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información; incluyen aspectos relacionados con la seguridad informática y la ciberseguridad.

- **Confidencialidad:** es el atributo de que solo el personal autorizado acceda a la información preestablecida.

- **Integridad**: es el atributo de mantener la totalidad y exactitud de la información y de los métodos de procesamiento.

- **Disponibilidad**: es el atributo de que los usuarios autorizados tengan acceso a la información cada vez que lo requieran a través de los medios que satisfagan sus necesidades.

- **SGSI**: Sistema de Gestión de Seguridad de la Información.

- **Ciberseguridad**: conjunto de medidas de protección de la infraestructura tecnológica y de la información, a través del tratamiento de las amenazas que ponen en riesgo la información procesada por los diferentes componentes tecnológicos interconectados.

- **Esquema de tres líneas de responsabilidad**: es un modelo de control y gestión de riesgos que brinda apoyo al órgano de gobierno del Banco, estableciendo una estructura y procesos eficaces para poder alcanzar los objetivos y mitigar los riesgos a los que se encuentra expuesto.

- **Primera línea de responsabilidad**: rol asignado a las áreas del negocio y operativas, responsables del diseño y evaluación de sus controles y la implementación de acciones preventivas y correctivas para hacer frente a las deficiencias de personas, procesos y tecnología de la información. Para efectos de esta política, las funciones de seguridad informática y de ciberseguridad forman parte de la primera línea de responsabilidad.

- **Segunda línea de responsabilidad:** áreas especializadas que tienen la función de monitorear y hacer contraposición de los controles diseñados y evaluados en la primera línea y el monitoreo de la evolución de los riesgos de seguridad de la información y ciberseguridad. Para efectos de esta política, la función de seguridad de la información forma parte de la segunda línea de responsabilidad.

- **Tercera línea de responsabilidad:** rol asignado a Auditoría Interna, cuya función es asegurar de forma independiente y objetiva, las prácticas del gobierno y de la administración de riesgos operativos en cada línea de responsabilidad.

- **Oficial de Seguridad de la Información (CISO):** Rol asignado al Gerente de Ciberseguridad de Banco Pichincha.

- **Ciberriesgos:** Parte de la gestión global del riesgo que se centra exclusivamente en el riesgo que se manifiesta en el dominio ciber (Entornos de información interconectados).
- **Apetito de Riesgo:** es una ponderación de alto nivel de cuánto riesgo la administración del Banco está dispuesta a aceptar en el logro de la misión y visión.