Diagnóstico de Controles de Acceso Lógico a Archivos con Información PII y PCI Aplicaciones Core de las Áreas de Operaciones de una Entidad Financiera

Fredy A. Fernández y Ariel A. Martin

Especialización en Seguridad Informática

Universidad Piloto de Colombia, Bogotá, Cundinamarca,

Ing. Hellen Barbosa e Ing. Álvaro Escobar

Agosto 29, 2025

Contenido

pág.

Lista de Tablas

pág.

Lista de Figuras

pág.

Resumen

El presente proyecto tiene como objetivo diagnosticar los controles de acceso lógico a archivos que contienen información sensible (PII y PCI) en las aplicaciones Core de las áreas operativas de una entidad financiera. Esta información es crítica para la operación del banco y su protección es esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos.

El diagnóstico se realizó con base en estándares internacionales como ISO/IEC 27001:2022, ISO/IEC 27005:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia. Se identificaron brechas en la gestión de accesos, incluyendo accesos excesivos, falta de trazabilidad, ausencia de segregación de funciones y controles manuales sin respaldo tecnológico.

Como resultado, se propusieron controles compensatorios para mitigar los riesgos mientras se implementan soluciones definitivas. Estos incluyen revisiones periódicas de accesos, registro formal de solicitudes, definición clara de roles, monitoreo manual de logs y talleres de concientización.

Se diseñó un plan de implementación con fases, responsables y cronograma, acompañado de un presupuesto estimado, que cubre capacitación, consultoría, herramientas tecnológicas y auditoría interna.

La ejecución de este plan permitirá fortalecer la postura de seguridad del banco, reducir el riesgo de exposición de datos sensibles y asegurar el cumplimiento normativo, protegiendo la confianza de los clientes y la reputación institucional.

Abstract

This project aims to assess the effectiveness of logical access controls applied to files containing sensitive information specifically Personally Identifiable Information (PII) and Payment Card Industry (PCI) data within core applications used by the Operations areas of financial institution. These controls are critical to ensuring that only authorized users can access, modify, or interact with sensitive data, thereby reducing the risk of unauthorized access and data breaches.

The diagnostic was conducted based on internationally recognized standards and regulatory frameworks, including ISO/IEC 27001:2022, ISO/IEC 27005:2022, PCI DSS v4.0.1, and Colombia's External Circular 029 of 2014. The assessment revealed several gaps in access management, such as excessive privileges, lack of traceability, insufficient segregation of duties, and manual controls lacking technological support.

To mitigate these risks, compensatory controls were proposed, including periodic access reviews, formal access request tracking, clearly defined roles and responsibilities, manual log monitoring, and staff awareness training. A structured implementation plan was developed, detailing phases, responsibilities, and a budget estimate.

The project contributes to strengthening the bank's information security posture, ensuring regulatory compliance, and protecting customer trust by minimizing the exposure of sensitive data through unauthorized channels.

Introducción

En una entidad financiera, la gestión adecuada de los accesos a la información sensible es esencial para proteger los datos de los clientes, como información PII (Personally Identifiable Information) y PCI (Payment Card Industry), que se procesan en sistemas críticos como las aplicaciones Core de las áreas operativas. Los controles de acceso lógico son fundamentales para garantizar que solo los usuarios autorizados puedan visualizar, modificar o interactuar con esta información, reduciendo así el riesgo de accesos indebidos y fugas de datos.

Este proyecto tiene como objetivo realizar un diagnóstico de los controles de acceso lógico a archivos que contienen información PII y PCI, con el fin de prevenir accesos no autorizados y mitigar los riesgos de exposición de datos, resguardando los pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad.

El diagnóstico se fundamenta en estándares internacionales y normativos ampliamente reconocidos, como ISO/IEC 27001:2022, ISO/IEC 27005:2022, PCI DSS v4.0.1, y la Circular Externa 029 de 2014 emitida por la Superintendencia Financiera de Colombia. Estos marcos proporcionan lineamientos técnicos y metodológicos para evaluar, gestionar y tratar los riesgos asociados al acceso a información sensible.

Al finalizar el diagnóstico, se espera proponer el fortalecimiento de los controles de acceso lógico existentes, asegurando su eficacia y eficiencia en la protección de archivos críticos.

Esto incluye la identificación de los responsables de la información, quienes deben autorizar los accesos, así como mecanismos de monitoreo y trazabilidad que permitan registrar y auditar el uso de los datos, minimizando así los riesgos de exposición en canales no autorizados o mercados ilícitos.

Estas acciones contribuirán a prevenir sanciones legales, pérdidas económicas y daños reputacionales, fortaleciendo la confianza de los clientes y la postura de seguridad de la entidad frente a los desafíos actuales.

1. Definición del Problema

1.1 Planteamiento del Problema

En una entidad financiera en Colombia, gestiona grandes volúmenes de información confidencial como parte de sus operaciones, especialmente en la emisión y administración de tarjetas de crédito. Esta información incluye PII (*Personally Identifiable Information*) y PCI (*Payment Card Industry*), considerados activos críticos para la organización y almacenados en sus aplicaciones Core.

Actualmente, cerca del 10% del personal de planta en áreas operativas tiene acceso directo a esta información sensible. Sin embargo, los controles de acceso lógico implementados son mínimos y poco eficaces, lo que representa un riesgo significativo de fuga de información. Esta situación podría facilitar la exposición de datos en mercados ilícitos, generando consecuencias legales, pérdidas económicas y un deterioro de la reputación institucional.

La ocurrencia de incidentes de seguridad en el banco ha evidenciado la necesidad de fortalecer los mecanismos de control de acceso, especialmente en entornos donde se maneja información crítica. La falta de trazabilidad, la asignación de privilegios excesivos y la ausencia de revisiones periódicas agravan el riesgo de accesos no autorizados.

Ante este escenario, se hace necesario realizar un diagnóstico de los controles de acceso lógico aplicados a los archivos que contienen información PII y PCI en las aplicaciones Core del banco. Este diagnóstico debe estar alineado con los lineamientos establecidos por la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia, así como con los estándares internacionales ISO/IEC 27001:2022, ISO/IEC 27005:2022 y PCI DSS v4.0.1.

Este análisis permitirá identificar debilidades, establecer responsabilidades claras sobre la

autorización de accesos, y proponer acciones correctivas que fortalezcan la postura de seguridad de la entidad frente a los riesgos actuales.

1.2 Formulación del Problema

¿Qué tan eficaces y adecuados son los controles de acceso lógico implementados en las aplicaciones Core de las áreas de operaciones de una entidad financiera para proteger archivos que contienen información PII y PCI, conforme a los estándares ISO/IEC 27001:2022, ISO/IEC 27005:2022, PCI DSS v4.0.1 y la Circular Externa 029 de la Superintendencia Financiera de Colombia?

2. Justificación

En el contexto actual del sector financiero, la protección de la información sensible, como los datos PII (*Personally Identifiable Information*) y PCI (*Payment Card Industry*), se ha convertido en una prioridad estratégica para las entidades bancarias. En la entidad financiera, al gestionar grandes volúmenes de este tipo de información a través de sus aplicaciones Core, enfrenta riesgos significativos asociados al acceso no autorizado, especialmente en áreas operativas donde un porcentaje considerable del personal tiene acceso directo a estos datos.

En el banco se han presentado incidentes de seguridad que han generado impactos económicos y reputacionales relevantes, afectando la confianza de los clientes y aumentando las pérdidas financieras, al tener que asumir contra el estado de pérdidas y ganancias (P&G) los valores asociados a reclamaciones por fraudes en transacciones o compras no reconocidas. Las investigaciones internas han confirmado que muchas de estas transacciones no fueron realizadas por los clientes, lo que ha obligado a la entidad a asumir los montos reclamados.

La existencia de controles de acceso lógico mínimos y poco eficaces incrementa la probabilidad de fugas de información, lo que podría derivar en sanciones regulatorias, pérdidas económicas y un deterioro de la reputación institucional. En este sentido, el diagnóstico de los controles actuales se vuelve fundamental para identificar debilidades, establecer responsabilidades claras sobre la autorización de accesos y garantizar la trazabilidad del uso de la información.

Asimismo, se busca involucrar activamente a la alta gerencia en la gestión de estos riesgos, en concordancia con la política de seguridad de la información del banco, promoviendo la asignación clara de responsabilidades sobre la autorización de accesos, la implementación de mecanismos de trazabilidad y la alineación de los controles con la clasificación de la

información, con el fin de minimizar la exposición de datos en canales no autorizados y prevenir su divulgación indebida. Este diagnóstico no solo responde a una necesidad operativa, sino también a un compromiso institucional que permitirá a la entidad reducir su exposición al riesgo, mejorar su postura de seguridad y cumplir con los requisitos regulatorios y de auditoría, con la protección de los datos y el cumplimiento normativo.

Este proyecto se justifica en la necesidad de alinear los mecanismos de control de acceso con los estándares internacionales ISO/IEC 27001:2022, ISO/IEC 27005:2022 y PCI DSS v4.0.1, así como con los lineamientos regulatorios establecidos por la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia, fortaleciendo así la postura de seguridad de la entidad frente a los riesgos actuales.

3. Objetivos

3.1 Objetivo General

Diagnosticar los controles de acceso lógico implementados en las aplicaciones Core de una entidad financiera que gestionan archivos con información PII y PCI en las áreas de operaciones, con el fin de evaluar su eficacia, identificar brechas de seguridad y proponer mejoras alineadas con los estándares ISO/IEC 27001:2022, ISO/IEC 27005:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia.

3.2 Objetivos Específicos

1) Identificar los archivos y sistemas que contienen información PII y PCI en las aplicaciones Core utilizadas por las áreas de operaciones de una entidad financiera.
2) Evaluar los controles de acceso lógico actualmente implementados sobre dichos archivos, considerando su eficacia, trazabilidad y alineación con las funciones del personal autorizado.
3) Verificar el nivel de cumplimiento de los controles de acceso lógico con respecto a los lineamientos establecidos por la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia, el estándar ISO/IEC 27001:2022 y PCI DSS v4.0.1.
4) Detectar brechas de seguridad y debilidades en los mecanismos de control que puedan facilitar accesos no autorizados o el uso indebido de información sensible.
5) Elaborar una matriz de riesgos asociados al acceso no autorizado a información

sensible, con base en la metodología de ISO/IEC 27005:2022.

6) Proponer un plan de tratamiento de riesgos que incluya acciones correctivas, responsables, plazos y mecanismos de seguimiento.

7) Proponer acciones de mejora y recomendaciones técnicas y administrativas para fortalecer los controles de acceso lógico, incluyendo la asignación de responsabilidades, la trazabilidad de accesos y la sensibilización del personal.

4. Hipótesis

Hi: Si se realiza un diagnóstico de los controles de acceso lógico implementados en las aplicaciones Core de una entidad financiera, que gestionan archivos con información PII y PCI en las áreas de operaciones, entonces será posible identificar brechas de seguridad, proponer mejoras que fortalezcan la protección de los datos sensibles, reducir el riesgo de accesos no autorizados y asegurar el cumplimiento de los estándares ISO/IEC 27001:2022, ISO/IEC 27005:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia.

H0: La realización de un diagnóstico detallado de los controles de acceso lógico implementados en las aplicaciones Core de una entidad financiera no permite identificar brechas de seguridad ni proponer mejoras significativas para la protección de los datos sensibles, ni contribuye a reducir el riesgo de accesos no autorizados ni a asegurar el cumplimiento de los estándares ISO/IEC 27001:2022, ISO/IEC 27005:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014.

Variable independiente: Diagnóstico de los controles de acceso lógico

Variable Dependiente: Fortalecer de la protección de la información PII y PCI

5. Alcance y limitaciones

5.1 Alcance

Este proyecto se enfoca en diagnosticar los controles de acceso lógico implementados en las aplicaciones Core de una entidad financiera, específicamente en aquellas utilizadas por las áreas de operaciones que gestionan archivos con información sensible clasificada como PII y PCI. El diagnóstico se realizará con base en los lineamientos establecidos por la norma ISO/IEC 27001:2022, ISO/IEC 2005:2022, ISO/IEC 27005:2022, el estándar PCI DSS v4.0.1 y la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia.

El proyecto contempla:

- Entrevistas con áreas operativas, TI y seguridad de la información.
- Revisión de políticas, procedimientos y matrices de acceso vigentes.
- Evaluación de controles de acceso lógico en aplicaciones Core que gestionan información sensible (PII y PCI).
- Análisis de trazabilidad y registros de auditoría para identificar accesos indebidos o no autorizados.
- Identificación de brechas frente a estándares internacionales:

  - ISO/IEC 27001:2022

  - PCI DSS v4.0.1
- Identificación de riesgos asociados frente al estándar internacional ISO/IEC 27005:2022
- Revisión del cumplimiento normativo con la Circular Externa 029 de 2014 de la

Superintendencia Financiera de Colombia.

- Propuesta de recomendaciones para fortalecer los controles de acceso, incluyendo:
  - Asignación de responsabilidades
  - Clasificación de información
  - Mecanismos de trazabilidad
- Elaboración de informe final con hallazgos, riesgos, recomendaciones y plan de acción.

5.2 Limitaciones del Proyecto

- Alcance funcional restringido: El diagnóstico se limita a las áreas de operaciones del Banco y no incluye otras áreas como tecnología, comercial o jurídica.
- No incluye la implementación de controles, solo su diagnóstico y recomendaciones.
- No contempla aplicaciones fuera del alcance definido (por ejemplo, sistemas satélites o de terceros).
- Acceso a la información: La disponibilidad de documentación interna, registros de acceso y entrevistas con personal con experiencia, puede estar sujeta a restricciones de confidencialidad o políticas internas.
- La calidad del diagnóstico dependerá de la disponibilidad y veracidad de la información proporcionada por las áreas responsables.
- No se evaluarán aspectos físicos o de infraestructura (como controles de acceso físico o seguridad perimetral).
- Tiempo y recursos: El análisis se realizará en un periodo determinado, lo que puede

limitar la profundidad del diagnóstico en ciertos sistemas o procesos.

- Cambios en el entorno normativo: El proyecto se basa en la normativa vigente al momento del estudio; futuras actualizaciones regulatorias podrían requerir ajustes posteriores.

6. Marco Teórico

6.1 Marco Teórico

6.1.1 Control de Acceso Lógico

El control de acceso lógico se refiere a los mecanismos técnicos y administrativos que regulan quién puede acceder a sistemas, aplicaciones y archivos digitales dentro de una organización. Su propósito es garantizar que solo usuarios autorizados puedan interactuar con información sensible, como datos personales o financieros.

Existen distintos tipos de controles de acceso:

- Administrativos: políticas, procedimientos, capacitaciones y revisiones de antecedentes.
- Físicos: control de ingreso a instalaciones mediante dispositivos biométricos o tarjetas.
- Lógicos o técnicos: autenticación mediante contraseñas, tokens, biometría, y gestión de privilegios en sistemas informáticos (Rouse, 2021)

El control de acceso lógico es fundamental para prevenir el uso indebido de información crítica, especialmente en sectores como el financiero, donde la exposición de datos puede generar pérdidas económicas y sanciones legales.

6.1.2 Protección de Información PII y PCI

La información personal identificable (PII) incluye datos como nombres, números de identificación, direcciones y cualquier otro elemento que permita identificar a una persona. Por su parte, la información de tarjetas de pago (PCI) comprende datos como el número de tarjeta, fecha de vencimiento y código de seguridad. La protección de estos datos es esencial para evitar

fraudes, robo de identidad y comercialización ilegal en mercados ilícitos (NIST, 2010).

6.1.3 Norma ISO/IEC 27001:2022

La norma ISO/IEC 27001:2022 establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo es proteger los activos de información mediante un enfoque basado en riesgos. El Anexo A de la norma incluye 93 controles agrupados en cuatro categorías: organizacionales, de personas, físicos y tecnológicos. (SO/IEC 27001, 2022)

Entre los controles más relevantes para este proyecto se encuentran:

A.5.15: Control de acceso.

- A.8.12: Prevención de fugas de datos.
- A.8.16: Actividades de monitoreo.
- A.5.30: Preparación de las TIC para la continuidad del negocio.

6.1.4 ISO/IEC 27005:2022

La norma ISO/IEC 27005:2022 proporciona directrices para la gestión de riesgos de seguridad de la información, y está diseñada para apoyar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO/IEC 27001. Esta norma no prescribe una metodología específica, sino que ofrece un marco estructurado para identificar, evaluar, tratar, monitorear y comunicar los riesgos de seguridad de la información. (SGS Academy, 2023)

6.1.5 Estándar PCI DSS v4.0.1

El estándar PCI DSS (Payment Card Industry Data Security Standard) establece requisitos para proteger los datos de tarjetas de pago. Las versiones más recientes, como la v4.0.1, refuerzan la autenticación multifactor, la gestión de privilegios y el monitoreo continuo

de accesos (PCI, 2023)

Los requisitos 7 y 8 del estándar son especialmente relevantes:

- Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de conocer.
- Requisito 8: Identificar y autenticar el acceso a los componentes del sistema

6.1.6 Circular Externa 029 de 2014 – Superintendencia Financiera de Colombia

Esta circular establece los lineamientos para la gestión de riesgos de seguridad de la información en entidades vigiladas. Exige la implementación de controles de acceso, trazabilidad, segregación de funciones y monitoreo de actividades. Además, promueve la asignación de responsabilidades claras y la adopción de buenas prácticas internacionales (Circular Básica C.E 029, 2014).

6.2 Marco Referencial

Una entidad financiera con amplia trayectoria en el sector bancario colombiano ha evolucionado significativamente desde su constitución en la década de 1960. A lo largo de su historia, ha experimentado procesos de expansión, fusiones estratégicas y alianzas internacionales que han fortalecido su presencia en el mercado nacional y regional.

Durante sus primeras décadas, la entidad consolidó su operación mediante adquisiciones y la creación de unidades especializadas en financiación de vivienda, lo que le permitió diversificar su portafolio de servicios. En los años noventa, se formalizó una fusión entre su sociedad financiera y una corporación de ahorro y vivienda, dando lugar a una estructura bancaria más robusta y orientada a la atención integral de clientes personales y empresariales.

En la primera década del siglo XXI, la entidad buscó alianzas estratégicas con actores

internacionales del sector financiero, lo que derivó en el lanzamiento de productos innovadores enfocados en la inclusión financiera de segmentos tradicionalmente desatendidos. Estas iniciativas contribuyeron a ampliar su cobertura y posicionamiento en el mercado colombiano.

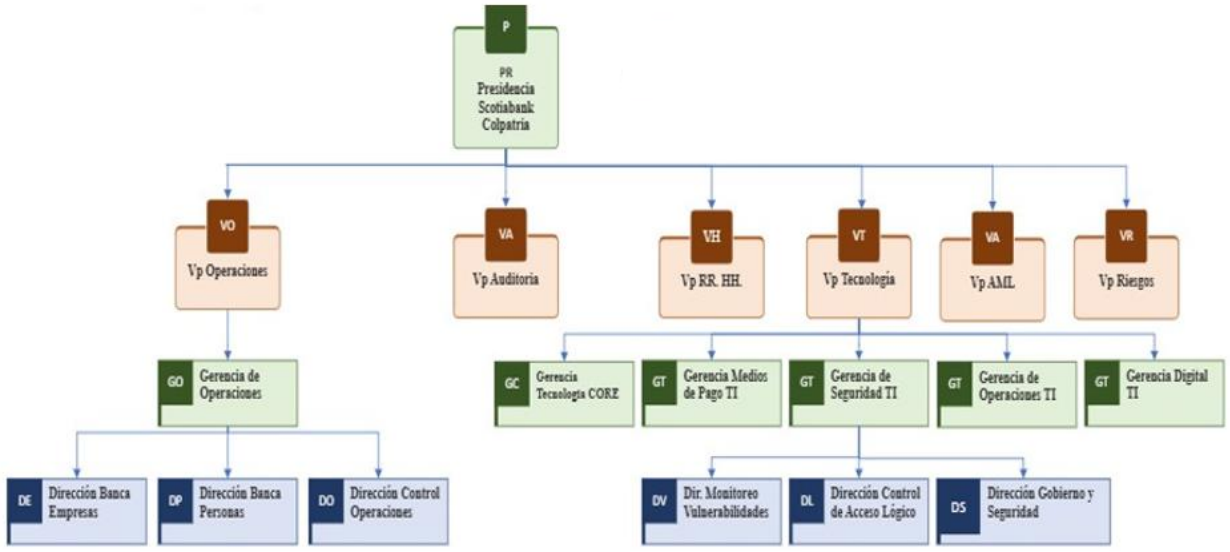
Posteriormente, se concretó una nueva alianza con un grupo financiero global con presencia en América Latina, lo que permitió fortalecer su capacidad operativa, tecnológica y comercial. Esta integración facilitó la adquisición de operaciones locales de banca personal de otra entidad internacional, consolidando así una marca renovada con enfoque regional y respaldo global.

Actualmente, la entidad cuenta con una red de más de 90 oficinas distribuidas en más de 20 ciudades del país, complementada por una infraestructura tecnológica que incluye cajeros automáticos propios y en convenio. Su equipo humano está conformado por más de 5.000 colaboradores, organizados en una estructura corporativa que incluye presidencia, vicepresidencias funcionales y gerencias especializadas.

La entidad se distingue por ofrecer soluciones financieras innovadoras, productos adaptados a las necesidades del mercado colombiano y servicios de inteligencia comercial para empresas locales e internacionales. Gracias al respaldo de su grupo estratégico internacional, proporciona herramientas financieras alineadas con las dinámicas del entorno global, manteniendo un enfoque de crecimiento sostenible, cumplimiento normativo y transformación digital.

Figura 1

Organigrama de la entidad financiera



Nota. El organigrama presentado incluye únicamente las áreas correspondientes al alcance del proyecto, seleccionadas entre las 15 Vicepresidencias que actualmente conforman la estructura organizacional del Banco. Elaboración propia.

7. Diseño Metodológico

7.1 Enfoque Metodológico

El proyecto adopta un enfoque cualitativo y cuantitativo (mixto), ya que combina el análisis documental y normativo con la recolección y evaluación de datos técnicos sobre los accesos lógicos en las aplicaciones Core del Banco. Este enfoque permite comprender tanto el contexto organizacional como la efectividad de los controles implementados.

7.2 Tipo de Estudio

Se trata de un estudio descriptivo y diagnóstico, orientado a identificar el estado actual de los controles de acceso lógico, sus debilidades y los riesgos asociados, con el fin de proponer acciones de mejora alineadas con estándares internacionales y normativas locales.

7.3 Métodos y Técnicas de Recolección de Información

Entrevistas semiestructuradas: con responsables de seguridad de la información, administradores de sistemas y áreas operativas.

Identificación de aplicaciones Core y archivos: servidores, Bases de Datos, archivos y tablas.

Revisión documental: análisis de políticas, procedimientos, líneas base y manuales de seguridad.

Revisión técnica de accesos: extracción y análisis de datos sobre cuentas activas, roles,

privilegios, matrices de acceso y trazabilidad en las aplicaciones Core.

Evaluación normativa: comparación de los controles actuales frente a los requisitos de ISO/IEC 27001:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014.

7.4 Instrumentos

Lista de chequeo del cumplimiento normativo.

Matriz de riesgos basada en ISO/IEC 27005:2022.

Mapa de calor de riesgos para priorización visual.

Plan de tratamiento de riesgos con responsables, plazos y estado de implementación.

7.5 Población y Muestra

7.5.1 Población objetivo

Funcionarios de las áreas de operaciones con acceso a información PII y PCI.

7.5.2 Muestra

Selección representativa del 10% del personal operativo con acceso lógico a las aplicaciones Core.

7.6 Fases del Proyecto

7.6.1 Cronograma de actividades

Como parte de la planificación del diagnóstico de controles de acceso lógico, se establece

un cronograma de actividades que define las fases del proyecto, los responsables asignados, la duración estimada de cada tarea y las fechas de ejecución. Este cronograma permite asegurar una gestión eficiente del tiempo, la coordinación entre equipos y el cumplimiento de los entregables establecidos. El cronograma contempla las siguientes etapas (ver tabla 1)

Tabla 1.

Cronograma de actividades.

Actividad	Duración (días)	Responsable	Fecha Inicio	Fecha Fin
1.1 Definición del alcance del diagnóstico	3	Líder de Seguridad de la Información	24/06/2025	26/06/2025
1.2 Identificación de stakeholders	2	Gerente de Proyecto	27/06/2025	1/07/2025
1.3 Revisión documental	3	Seguridad de la Información	2/07/2025	4/07/2025
1.4 Planificación del cronograma	2	Gerente de Proyecto	7/07/2025	8/07/2025
2.1 Levantamiento de información	5	Consultor de Seguridad / Equipos Técnicos	9/07/2025	15/07/2025
2.2 Evaluación de controles	7	Consultor de Seguridad	16/07/2025	24/07/2025
2.3 Validación de hallazgos	3	Líder de Seguridad / Stakeholders	25/07/2025	29/07/2025
3.1 Diseño de controles compensatorios	4	Consultor de Seguridad	30/07/2025	4/08/2025
3.2 Asignación de responsabilidades	2	Alta Gerencia / Seguridad de la Información	5/08/2025	6/08/2025
3.3 Plan de implementación	3	Gerente de Proyecto / Seguridad de la Información	8/08/2025	12/08/2025
4.1 Presentación de informe final	2	Consultor de Seguridad / Gerente de Proyecto	13/08/2025	14/08/2025
4.2 Socialización con stakeholders	2	Gerente de Proyecto / Alta Dirección		
4.3 Seguimiento post-diagnóstico	3	Seguridad de la Información / Auditoría Interna		

Nota. Este cronograma sirve como base para el seguimiento del proyecto y la asignación de recursos, facilitando la identificación de desviaciones y la toma de decisiones oportunas. Elaboración propia.

7.6.2 Entrevistas semiestructuradas

Como parte del proceso de levantamiento de información y validación de hallazgos, se llevaron a cabo entrevistas semiestructuradas con los equipos responsables de la seguridad de la información, control de acceso, tecnología y áreas de negocio (tabla 2 y 3) Estas sesiones permitieron:

- Recopilar información clave sobre la gestión de accesos, perfiles y privilegios en las aplicaciones incluidas en el alcance del diagnóstico.
- Validar hallazgos preliminares con los responsables funcionales y técnicos.
- Identificar riesgos operativos y de cumplimiento asociados a la asignación de accesos indebidos o excesivos.
- Promover el consenso sobre los controles compensatorios y las recomendaciones propuestas.
- Fortalecer la colaboración integral, asegurando que las soluciones propuestas sean viables, sostenibles y alineadas con los objetivos del negocio.
- La participación de los distintos equipos permitió enriquecer el análisis y garantizar que las medidas correctivas propuestas respondan a las necesidades reales de la organización.

Tabla 2.

Usuarios y perfiles en las aplicaciones Core del Banco al mes de junio de 2025

Aplicación	Funcionarios planta	Usuarios en app	Total Usr activos	Total Usr inactivos	Total rol App	Total perfil App	Total Funcionario Gc Op	Total Usr Gc Op	Usr Auta Archivo Crítico Gc Op
Core banco	5193	3852	3350	502	1588	383	581	577	58
Core tarjetas	5193	1471	1467	4	51	36	581	457	58
Crm	5193	3268	3054	214	398	72	581	223	58
Originador	5193	1914	1793	121	230	10	581	223	58

Nota. La tabla muestra las aplicaciones identificadas en el alcance del proyecto, junto con las cantidades de funcionarios y usuarios por aplicación, estado, cantidad de perfiles y autorizados a archivos críticos. Elaboración propia

Tabla 3.

Entrevistas a las áreas involucradas en el levantamiento

Área	Nombre del Participante	Rol	Fecha	Aplicaciones que utiliza	Tipo de Acceso (Lectura, Escritura, Admin, etc.)	Observaciones	Brechas Identificadas	Recomendaciones al Participante
Gc Seguridad TI / Dir de Seguridad	Juan Felipe Tabares Silgado	Gerente de Seguridad Informática (CISO)	9/07/2025	N/A	N/A	Socialización y presentación del alcance del proyecto, autoriza realizar el levantamiento de información.	N/A	Limitar el levantamiento de información con los líderes de cada una de las áreas de operaciones, ofuscar la información para no comprometer información sensible.
Gc Seguridad TI / Dir Gobierno de seguridad y Consultoría	Carlos Andrés Rodríguez Ayala	Ingeniero II Consultoría	9/07/2025	N/A	N/A	Consultor de seguridad comparte los estándar, Políticas y procedimientos de seguridad.	Falta de socialización de los estándares y políticas con las áreas de operaciones.	Se debe socializar los estándares, políticas, manuales y línea base de seguridad a las áreas de negocio del Banco en especial al área de operaciones quienes manipulan información sensible para la compañía.
Gc Seguridad TI / Dir Control de Acceso Lógico	Luis Carlos Pérez Sosa	Ingeniero I Control de Acceso Lógico	9/07/2025	Core banco core tarjetas crm originador	Admin	Administrador de seguridad de las aplicaciones Core, comparte el Manual de gestión de usuarios y lista de usuarios y perfiles en las aplicaciones junto con las últimas certificaciones realizadas. Comparte los parámetros de seguridad de las contraseñas en cada una de las aplicaciones.	Desconoce los estándares y políticas de seguridad. Las últimas certificaciones tienen un periodo superior a un año. Los parámetros de seguridad de las aplicaciones no cumplen de acuerdo al estándar de seguridad. No cuentan con una bitácora de archivos críticos autorizados a las áreas de operaciones. Tiene salida de correo externo.	Se debe realizar un cronograma de certificación de las aplicaciones, identificar y reportar a los dueños de las aplicaciones el resultado de estas certificaciones. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe implementar un plan de trabajo para poder revisar, identificar y configurar los parámetros de seguridad de contraseña en las aplicaciones. Se debe implementar una bitácora de archivos sensibles y poder tener identificados los usuarios que se encuentran autorizados a estos archivos, de igual forma realizar una certificación periódica de estas autorizaciones.
Gc Tecnología / Dir Soporte Core Bancario	Nidia Yela Vélez	Director IT Core Bancario	10/07/2025	Core banco	Admin	Administrador de la aplicación Core Banco, comparte arquitectura de la aplicación Core Banco, comparte lista de archivos y librerías que almacena información Transaccional con información PII y PCI.	No se generan logs de acceso sobre todos los archivos PII y PCI que almacenan este tipo de información. Tiene salida de correo externo.	Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información.
Gc Infraestructura TI / Dir Core Bancario	Marisol Avendaño Gómez	Ingeniero II Infraestructura	10/07/2025	Core banco	Admin	Administrador de Infraestructura Core Banco, comparte información como direccionamiento y configuración de los servidores, certificados digitales instalados.	Los parámetros de seguridad de contraseña no cumplen con el estándar de seguridad y la línea base de acuerdo con lo reportado por Gobierno y Consultoría de seguridad. Tiene salida de correo externo.	Se debe revisar y reconfigurar los parámetros de seguridad de contraseña en la aplicación para cumplir el estándar y línea base de seguridad. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información.
Gc Tecnología / Dir Core Tarjetas	Yenith Hernández Rodríguez	Ingeniero II Core Tarjetas y Procesos de Automatización	11/07/2025	Core tarjetas	Admin	Administrador de la aplicación Core Tarjetas, comparte arquitectura de la aplicación, comparte lista de Base de Datos y Tablas que almacena información	No se generan logs de acceso sobre todas las tablas que almacenan información PII y PCI. Tiene salida de correo externo.	Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información.

Área	Nombre del Participante	Rol	Fecha	Aplicaciones que utiliza	Tipo de Acceso (Lectura, Escritura, Admin, etc.)	Observaciones	Brechas Identificadas	Recomendaciones al Participante
Gc Tecnología / Dir CRM y Ventas	Daniel Palanco Guerrero	Ingeniero II CRM y Ventas	11/07/2025	Crm	Admin	Administrador de la aplicación CRM, comparte arquitectura de la aplicación, comparte lista de Base de Datos y Tablas que almacena información Transaccional con información PII.	No se generan logs de acceso sobre todas las tablas que almacenan información PII. Tiene salida de correo externo.	Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información.
Gc CRM / Dir Campañas	Janeth Guacaneme	Profesional I CRM	11/07/2025	Core banco crm	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para CRM y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del CORE BANCO mediante herramienta de WRKQRY.	Accede a archivos PII sin MFA, no registra logs de uso de archivos Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información de CRM.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Ingeniería de Confiabilidad / Dir de Ventas	Jeimmy Huertas Camacho	Ingeniera I Tecnología Digital	14/07/2025	Originador	Admin	Administrador de la aplicación ORIGINADOR, comparte arquitectura de la aplicación, comparte lista de Base de Datos y Tablas que almacena información Transaccional con información PII y PCI.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Originador.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Operaciones / Dir Banca Empresas	Claudia Lorena Bermudez	Director de Operaciones Banca Empresas	14/07/2025	Core banco core tarjetas	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para Core Tarjetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco y Core Tarjetas.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Operaciones / Dir Banca Empresas	Nancy Montana García	Profesional Back Office & Servicios Empresariales	14/07/2025	Core banco core tarjetas	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para Core Tarjetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco y Core Tarjetas.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.

Área	Nombre del Participante	Rol	Fecha	Aplicaciones que utiliza	Tipo de Acceso (Lectura, Escritura, Admin, etc.)	Observaciones	Brechas Identificadas	Recomendaciones al Participante
Gc Operaciones / Dir Banca Empresas	Carolina Téllez Ojeda	Profesional de Servicios Documentales Pasivo	14/07/2025	Core banco core tarjetas	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para Core Tarjetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco y Core Tarjetas.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Operaciones / Dir Banca Empresas	Yadira García Suarez	Profesional de Servicios Documentales Pyme	14/07/2025	Core banco core tarjetas	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para Core Tarjetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco y Core Tarjetas.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Operaciones / Dir Banca Empresas	Liliana Martínez Bello	profesional de Servicios Documentales Empresas	14/07/2025	Core banco core tarjetas	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para Core Tarjetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco y Core Tarjetas.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Operaciones / Dir Banca Personas	Carlos Perilla Torres	Director de Operaciones Banca Personas	15/07/2025	Core banco core tarjetas crm originador	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para CRM, Originador, Core Tarjetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco, CRM, Originador y Core Tarjetas.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Operaciones / Dir Banca Personas	Edward Forero Rojas	Profesional Tarjeta Crédito y Débito	15/07/2025	Core banco core tarjetas crm originador	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para CRM, Originador, Core Tarjetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas. Base de seguridad. Se debe identificar y socializar el responsable de

Área	Nombre del Participante	Rol	Fecha	Aplicaciones que utiliza	Tipo de Acceso (Lectura, Escritura, Admin, etc.)	Observaciones	Brechas Identificadas	Recomendaciones al Participante
Gc Operaciones / Dir Banca Personas	Julio Soto Parra	Profesional Ciclo de Vida	15/07/2025	Core banco core tarjetas crm originador	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para CRM, Originador, Core Tarjetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Banco, CRM, Originador y Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco, CRM, Originador y Core Tarjetas.	la aplicación para autorizar accesos a los archivos Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Operaciones / Dir Banca Personas	Maria Lucia Carvajal	Profesional de originación y entrega	15/07/2025	Core banco core tarjetas crm originador	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para CRM, Originador, Core Tarjetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco, CRM, Originador y Core Tarjetas.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Operaciones / Dir Banca Personas	Paola Pinzón Gomez	Profesional Hipotecario	15/07/2025	Core banco crm originador	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para Originador, CRM y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco, CRM y Originador.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.
Gc Operaciones / Dir Control de Operaciones	Jose de Jesus Blanco Marin	Profesional Control de Operaciones	15/07/2025	Core banco core tarjetas crm	Lectura, Escritura, Reportes, Operación	Funcionario solo accede a las aplicaciones desde Intranet para Originador, Core Trajetas y cliente para el Core Banco. Realiza ejecuciones de consulta sobre archivos del Core Banco mediante herramienta de WRKQRY.	Accede a archivos PII y PCI sin MFA, no registra logs de uso de archivos. Tiene salida de correo externo. No conoce la clasificación de la información. Desconoce el responsable de la información del Core Banco, Core Tarjetas y CRM.	Se debe implementar (MFA). Se debe revisar y reconfigurar las reglas de monitoreo y entrega de eventos al SIEM. Se debe restringir la salida de correo externo con el fin de minimizar el riesgo de fuga de información. Se debe capacitar e informar los estándares, políticas, manuales y líneas Base de seguridad. Se debe identificar y socializar el responsable de la aplicación para autorizar accesos a los archivos con información sensible.

Nota. La tabla muestra el consolidado de las entrevistas realizadas, con la justificación, hallazgo y recomendaciones. Elaboración propia.

7.6.3 Identificación de aplicaciones Core

Se identifican las aplicaciones Core incluidas dentro del alcance del proyecto, relacionando para cada una de ellas su respectiva infraestructura tecnológica. Esta información incluye el sistema operativo y su versión, el motor de base de datos utilizado, el direccionamiento IP asignado y la segmentación de red correspondiente.

La tabla 4 permite establecer el entorno técnico sobre el cual se gestionan los accesos y se aplican los controles de seguridad.

Tabla 4.

Infraestructura de aplicaciones Core

Aplicación	Ambiente	Nombre Servidor Hastíame	Sistema Operativo	Motor Base de Datos	Tipo	IP	Puerto	Segmento de RED
Core banco	Producción	COBNS000	I Series IBM v 7.4	DB2 for i 7 7.4	APP	10.10.25.101	992	PCI
Core banco	Contingencia	COBNS001	I Series IBM v 7.4	DB2 for i 7 7.4	APP	10.14.38.96	992	PCI
Core tarjetas	Producción	bsbcaptarj01	Linux RedHat Enterprise 8.9	N/A	APP Nodo1	10.10.25.210	5012,5013,5014	PCI
Core tarjetas	Producción	bsbcaptarj02	Linux RedHat Enterprise 8.9	N/A	APP Nodo2	10.10.25.211	5012,5013,5014	PCI
Core tarjetas	Producción	bsbcdptarj01	Linux RedHat Enterprise 8.9	Oracle DB 19c	DB Nodo1	10.10.24.112	5012,5013,5014	PCI
Core tarjetas	Producción	bsbcdptarj02	Linux RedHat Enterprise 8.9	Oracle DB 19c	DB Nodo2	10.10.24.113	5012,5013,5014	PCI
Core tarjetas	Contingencia	bsbcactarj01	Linux RedHat Enterprise 8.9	N/A	APP	10.14.175.217	5012,5013,5014	PCI
Core tarjetas	Contingencia	bsbcdctarj01	Linux RedHat Enterprise 8.9	Oracle DB 19c	DB	10.14.175.223	5012,5013,5014	PCI
CRM	Producción	bsbcapcrm01	Linux RedHat Enterprise 8.9	N/A	APP Nodo1	10.12.33.95	2328,2329,2330	NO PCI
CRM	Producción	bsbcapcrm02	Linux RedHat Enterprise 8.9	N/A	APP Nodo2	10.12.33.96	2328,2329,2330	NO PCI
CRM	Producción	bsbcdpcrm01	Linux RedHat Enterprise 8.9	Oracle DB 19c	DB Nodo1	10.12.18.95	2328,2329,2330	NO PCI
CRM	Producción	bsbcdpcrm02	Linux RedHat Enterprise 8.9	Oracle DB 19c	DB Nodo2	10.12.18.96	2328,2329,2330	NO PCI
CRM	Contingencia	bsbcaccrm01	Linux RedHat Enterprise 8.9	N/A	APP	10.13.53.20	2328,2329,2330	NO PCI
CRM	Contingencia	bsbcdccrm01	Linux RedHat Enterprise 8.9	Oracle DB 19c	DB	10.13.53.25	2328,2329,2330	NO PCI
Originador	Producción	bsbcapori01	Windows Server 2016 10.0.14393	N/A	APP Nodo1	10.10.25.111	3351,3352,3353	PCI
Originador	Producción	bsbcapori02	Windows Server 2016 10.0.14393	N/A	APP Nodo2	10.10.25.112	3351,3352,3353	PCI
Originador	Producción	bsbcdpori01	Windows Server 2016 10.0.14393	SQL Server 2016 13.0.7029.3	DB Nodo1	10.10.24.111	3351,3352,3353	PCI
Originador	Producción	bsbcdpori02	Windows Server 2016 10.0.14393	SQL Server 2016 13.0.7029.3	DB Nodo2	10.10.24.112	3351,3352,3353	PCI
Originador	Contingencia	bsbcacori01	Windows Server 2016 10.0.14393	N/A	APP	10.14.38.111	3351,3352,3353	PCI
Originador	Contingencia	bsbcdcori01	Windows Server 2016 10.0.14393	SQL Server 2016 13.0.7029.3	DB	10.14.38.112	3351,3352,3353	PCI

Nota. La tabla muestra las características de los servidores por aplicación y ambientes en el que procesa y almacenan información sensible (PII y PCI). Elaboración propia.

7.6.4 Identificación archivos críticos que contienen información PII y PCI en aplicaciones Core

Se realiza el proceso de identificación de archivos críticos que contienen información sensible, específicamente datos de información personal (PII) y datos de tarjetas de pago (PCI), dentro de las aplicaciones Core incluidas en el alcance del proyecto.

Para ello, se lleva a cabo un análisis conjunto con los equipos responsables de la aplicación de parte de TI, seguridad de la información y de las áreas operativas, con el fin de determinar qué archivos, bases de datos o estructuras de almacenamiento contienen este tipo de información. El objetivo es establecer un inventario claro que permita aplicar controles de protección, trazabilidad y monitoreo adecuados.

Durante este ejercicio, se identifican archivos que contienen datos como nombres completos, números de identificación, direcciones, números de cuenta, información de tarjetas de crédito, entre otros. Esta información es clasificada como crítica y se documenta en una matriz que incluye el nombre del archivo, la aplicación asociada, el tipo de información contenida, los controles de acceso aplicados, frecuencia de uso y en observaciones los campos que contiene el archivo o tabla identificada.

7.6.4.1 Core Banco. Como parte del proceso de identificación de archivos críticos que contienen información sensible (PII y PCI), en la tabla 5, se relacionan los archivos identificados junto con la estructura de datos dentro de esta aplicación, que almacena, procesa y transmite información PII y PCI, considerados de alto riesgo.

Tabla 5.

Identificación de archivos Core Banco

Archivo N°	Librería	Nombre del archivo	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
AR01	BSBDCRM01	DCRM010	Personas	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Fecha de Nacimiento, Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento, Código Postal, Teléfono de Oficina, Teléfono Celular, Segmento, Estado del cliente, Profesión, Estrato, Sexo, Estado Civil, Cargo, Código CIIU, Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos, NIT de la Empresa, Nombre de la Empresa)
AR02	BSBDCRM01	DCRM011	Personas_ext	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Identificación, Número de identificación, Lugar de Nacimiento, Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Nivel Educativo, Número de Hijos, Personas a cargo, Origen de Fondos, Clasificación Riesgo, Nombre de Referencias, Teléfono de referencias, Parentesco, Ingresos, Egresos, Sueldo)
AR03	BSBDCRM01	DCRM013	Empresas	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Nombre de la empresa, NIT de la empresa, correo electrónico del representante legal de la empresa, Dirección de la empresa, Barrio, Ciudad, Segmento, Actividad económica de la empresa)
AR04	BSBDCRM01	DCRM017	Productos	PII/PCI	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Productos, Línea de productos, subproductos, número de productos, Portafolio, Dirección principal, Barrio, Ciudad, Departamento, email, Nombre completo, tipo de documento, documento de cliente)
AR05	BSBDCRM01	DCRM069	Cliente-segmento	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Documento cliente, NIT Empresa, Tipo de documento, Tipo de cliente, Segmento, Nombre completo, Razon social)
AR06	BSBDCRM01	DCRM1229	Informacion financiera persona natural	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Documento cliente, Tipo de documento, Ciudad de expedición de documento, Departamento, País, Ciudad de residencia, Barrio de Residencia, Departamento de residencia, País de residencia Fecha de expedición de documento, País de Nacionalidad, PEP, Ciudad de nacimiento, Departamento de Nacimiento, Decalra Impuesto, Dirección, Teléfono, Correo electrónico, Actividad económica, Cargo Ocupación, Código CIIU, Total Activos, Total Pasivos, Total Patrimonio, Total Ingresos, Total Egresos, Origen de Fondos, Otro origen de fondos, Nombre Completo, fecha de nacimiento, Dirección de Oficina, Ciudad de Oficina, Ingresos validados)
AR07	BSBDCRM01	DCRM1230	Informacion financiera persona juridica	PII/PCI	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Nombre Razón social, Nombre Comercial, Tipo de identificación, Número de Identificación, Fecha de Constitución, País de Constitución, Tipo de empresa, Cotiza en Bolsa, Dirección 39esidenci de la empresa, País de la empresa, Departamento, Ciudad, Teléfono principal, correo electrónico de contacto, Actividad económica, Código CIIU, Ventas anuales, Sucursales en otro país, Realiza Transacción en Moneda Extranjera, Tipo de producto, Número de producto, Entidad del producto, Ciudad, País, Moneda, tiene clientes en el exterior, país del cliente, Remesas Giros Mensual, Origen de fondos, Destino Origen de Fondos, Otros orígenes de fondos, Total ingresos, Total Egresos, Total Activos, Total Pasivos, Total Patrimonio, Segmento)
AR08	BSBDCRM01	DCRM1232	Direcciones principales	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Documento, Número de documento, Dirección principal, Barrio, Ciudad, Departamento, Código Postal, Estado de la Dirección)

Archivo N°	Librería	Nombre del archivo	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
AR09	BSBDCRM01	DCRM1233	Cumplimiento personas expuestas públicamente	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Documento, Número de documento, PEP)
AR10	BSBDCRM01	DCRM1234	Cumplimiento empresas	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Documento, Número de documento, Calificación de Riesgo Cliente)
AR11	BSBDCRM01	DCRM1237	Partes asociadas locales	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Documento, Número de documento, Nombre Completo, Fecha de Nacimiento, Lugar de Nacimiento, correo electrónico, Teléfono principal, Teléfono laboral, Dirección de correspondencia, PEP, Familiar PEP)
AR12	BSBDCRM01	DCRM1238	Partes asociadas extranjeras	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Documento, Número de documento, Nombre Completo, Cargo ocupación, Código CIIU, Teléfono principal, Teléfono laboral, Dirección de correspondencia, Total Ingresos, Total Egresos, Total Activos, Total Pasivos, Operación ME)
AR13	BSBDCRM01	DCRM1250	Cargue riesgo local	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Documento, Número de documento, Calificación de riesgo local, Fecha Calificación)
AR14	BSBDCRM01	DCRM1251	Rechazos cargue riesgo local	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Documento, Número de documento, Motivo Rechazo)
AR15	BSBDCRM01	DCRM1257	Empresas extranjeras	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Otro Tipo de Documento, Número de documento, Nombre completo, País de Nacimiento, País de dirección, Departamento, Ciudad, Dirección principal)
AR16	BSBDCRM01	DCRM1258	Personas extranjeras	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Otro Tipo de Documento, Número de documento, Nombre completo, País de expedición, Fecha de Nacimiento, País de Nacimiento, PEP, País de dirección, Departamento, Ciudad, Dirección principal)
AR17	BSBDCRM01	DCRM2025	Clientes historico	PII	Gerencia de CRM	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Documento, Número de documento, Nombre completo, Fecha expedición documento, Lugar de expedición, Nacionalidad, Fecha de Nacimiento, País de Nacimiento, Sexo, Estado Civil, Personas a Cargo, Nivel educativo, Profesión, Dirección de residencia, Barrio, Ciudad, Departamento, Tipo de Vivienda, Estrato, Teléfono de residencia, número de celular, e-mail de contacto, Tiempo de residencia, Actividad-ocupación, Código CIIU, NIT de la Empresa, Nombre de la Empresa, antigüedad en la empresa, Relación con la empresa, Actividad económica de la empresa, Cargo actual, Dirección de Oficina, Barrio, Ciudad, Departamento, Teléfono, Sueldo, Comisiones, Honorarios, Arrendamientos, Otros ingresos, Total ingresos, Descripción Otros Ingresos, Arriendo-Cuota Hipoteca, préstamo Nómina, Gastos Familiares, Cuota Tarjeta Cred, Cuota otros prestamos, Total Egresos, Total Activos, Total Pasivo, Total Patrimonio, Nombre completo de referencias, Ciudad Referencias, Teléfono referencias, Parentescos, Origen de Fondos, Fecha de Vinculación)
AR18	BSBDTAR01	DTAR001	Contrato	PII/PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, cupo de tarjeta, saldo utilizado, saldo disponible, saldo disponible compra, saldo disponible avance, Número de identificación titular, tipo de documento, nombre completo de cliente, estado de contrato, límite de cupo para avances, grupo de liquidación, número de beneficiarios, Fecha de alta contrato, Fecha de Baja, Motivo de Baja)
AR19	BSBDTAR01	DTAR002	Contrato b	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, Producto, subproducto, fecha de alta, código condición económica, grupo de liquidación, número de beneficiarios, código de bloqueo, fecha del último bloqueo, situación del contrato Impagado, saldo impagado, importe cobrado y aplicado, intereses corrientes, intereses de mora, fecha última aplicación, total de puntos, puntos periodo anterior, punto generados en último corte, puntos redimidos, puntos vencidos, puntos a vencer, fecha vencimiento de puntos, calificación interna, calificación endeudamiento, tipo

Archivo N°	Librería	Nombre del archivo	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
									de moneda, cartera castigada, saldo castigado, fecha último rediferido, fecha de refinanciación, valor refinanciación, indicador pago primera cuota, fecha primera compra, fecha cambio de cupo, tipo cambio de cupo, cupo anterior, cupo nuevo,valor acumulado de IVA)
AR20	BSBDTAR01	DTAR003	Contrato c	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, fecha inicio de mora, número días en mora, número de cuotas en mora, altura de mora, valor de mora, saldo total otros conceptos, saldo a favor, Total pagos última factura, Valor devolución IVA, valor último pago, fecha último pago, fecha última facturación, saldos, cupo disponible, comisiones, intereses, reversos)
AR21	BSBDTAR01	DTAR004	Contrato d	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, Capital, comisiones última facturación, intereses última facturación, impuestos última facturación, Honorarios, intereses de mora, avance en el periodo, compras en el periodo, pago mínimo, pago total, número de cuotas pagadas, plazo de la deuda, fecha del último extracto, fecha de liquidación, fecha próximo vencimiento)
AR22	BSBDTAR01	DTAR005	Tarjeta a	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, PAN de la tarjeta en claro, número de plástico, franquicia, tipo de tarjeta, fehca alta tarjeta, estado tarjeta, bloqueo, fecha caducidad tarjeta, fecha último reenvío renovación, titular o beneficiario, no renovación, fecha próximo cobro cuota, nombre estampado, fecha de baja, motivo de baja, fecha último uso, comentario de bloqueo, fecha último bloqueo)
AR23	BSBDTAR01	DTAR006	Tarjeta b	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, Motivo de reexpedición, fecha de reexpedición, nombre en plástico, cupo de tarjeta)
AR24	BSBDTAR01	DTAR008	Movimiento a	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, Tipo de la factura, descripción tipo de la factura, fecha de la factura, número de referencia de la factura, PAN de la tarjeta en claro, código de la moneda de la operación, número de autorización, código de comercio, nombre de comercio reducido, código de actividad, fecha contable de la operación, tipo de franquicia, fecha de liquidación, número de cuotas de la compra, saldos pendientes de diferir, cuotas pendientes de facturación)
AR25	BSBDPLA01	DPLA001	Plasticos	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, PAN de la tarjeta en claro, número de plástico, franquicia, tipo de tarjeta, fehca alta tarjeta, estado tarjeta, bloqueo, fecha caducidad tarjeta, fecha último reenvío renovación, titular o beneficiario, no renovación, fecha próximo cobro cuota, nombre estampado, fecha de baja, motivo de baja, fecha último uso, comentario de bloqueo, fecha último bloqueo)
AR26	BSBDPLA01	DPLA003	Personas	PII	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Documento cliente, Tipo de documento, Ciudad de expedición de documento, Departamento, País, Ciudad de residencia, Barrio de Residencia, Departamento de residencia, País de residencia Fecha de expedición de documento, Pais de Nacionalidad, PEP, Ciudad de nacimiento, Departamento de Nacimiento, Decalra Impuesto, Dirección, Teléfono, Correo electrónico, Actividad económica, Cargo Ocupación, Código CIIU, Total Activos, Total Pasivos, Total Patrimonio, Total Ingresos, Total Egresos, Origen de Fondos, Otro origen de fondos, Nombre Completo, fecha de nacimiento, Dirección de Oficina, Ciudad de Oficina, Ingresos validados)
AR27	BSBDPLA01	DPLA011	Contrato	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, cupo de tarjeta, saldo utilizado, saldo disponible, saldo disponible compra, saldo disponible avance, Número de identificación titular, tipo de documento, nombre completo de cliente, estado de contrato, límite de cupo para avances, grupo de liquidación, número de beneficiarios, Fecha de alta contrato, Fecha de Baja, Motivo de Baja)
AR28	BSBDPLA01	DPLA012	Plastico a	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, PAN de la tarjeta en claro, número de plástico, franquicia, tipo de tarjeta, fehca alta tarjeta, estado tarjeta, bloqueo, fecha caducidad tarjeta, fecha último reenvío renovación,

Archivo N°	Librería	Nombre del archivo	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
									titular o beneficiario, no renovación, fecha próximo cobro cuota, nombre estampado, fecha de baja, motivo de baja, fecha último uso, comentario de bloqueo, fecha último bloqueo)
AR29	BSBDPLA01	DPLA013	Plastico b	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Número de contrato, Motivo de reexpedición, fecha de reexpedición, nombre en plástico, cupo de tarjeta)
AR30	BSBDPLA01	DPLA014	Realce	PII/PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Código Entidad, Motivo de expedición, fecha de expedición, nombre en plástico, cupo de tarjeta, Número de documento, Fecha de emisión, Fecha de entrega, Currier, Dirección de correspondencia, Barrio, Ciudad de correspondencia, Nombre completo de cliente)
AR31	BSBDEXT01	DEXT001	Personas	PII	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Documento cliente, Tipo de documento, Ciudad de expedición de documento, Departamento, País, Ciudad de residencia, Barrio de Residencia, Departamento de residencia, País de 42esidencia Fecha de expedición de documento, Pais de Nacionalidad, Ciudad de nacimiento, Departamento de Nacimiento, Dirección, Teléfono, Correo electrónico)
AR32	BSBDEXT01	DEXT002	Tipo de cliente	PII	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Documento cliente, NIT Empresa, Tipo de documento, Tipo de cliente, Segmento, Nombre completo, Razon social)
AR33	BSBDEXT01	DEXT011	Extracto	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Documento cliente, Tipo de documento, Tipo de Producto, Número de producto, Ciudad de residencia, Barrio de Residencia, Departamento de residencia, País de residencia, Dirección, Teléfono, Correo electrónico, saldo de producto, fecha de pago, fecha de corte, intereses corrientes, intereses de mora, valor pago mínimo, valor pago total, valor pago diferido, detalle de compra)
AR34	BSBDEXT01	DEXT012	Saldos y cupos	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (Tipo de Producto, Número de producto, saldo de producto, fecha de pago, fecha de corte, intereses corrientes, intereses de mora, valor pago mínimo, valor pago total, valor pago diferido, detalle de compra)
AR35	BSBDEXT01	DEXT018	Curriers	PCI	Gerencia de Operaciones Tarjetas	CORE BANCO	Contraseña, Roles, Perfiles	Diario	Archivo contiene información (NIT Currier, Nombre de empresa, Documento cliente, Tipo de documento, Tipo de Producto, Número de producto, Ciudad de residencia, Barrio de Residencia, Departamento de residencia, País de residencia, Dirección, Teléfono, Correo electrónico)

Nota. La tabla muestra los archivos y el detalle de los campos que fueron identificacos, donde se almacena información sensible (PII y PCI) en la aplicación Core Banco. Elaboración propia.

7.6.4.2 Core Tarjetas. Como parte del proceso de identificación de archivos críticos que contienen información sensible (PII y PCI), se realiza un análisis específico sobre la aplicación Core Tarjetas.

Durante la revisión, se identifican tablas que contienen información como nombres de titulares, números de tarjeta, códigos de

seguridad (CVV), fechas de vencimiento, historiales de transacciones y datos de contacto como se muestra en la tabla 6.

Tabla 6.

Identificación de tablas en bases de datos Core tarjetas

Archivo N°	Base de Datos	Esquema	Nombre de Tabla	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
AR36	TARPRO1 / TARPRO2	Cliente	Tar_Cliente	Información de clientes	PII	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	iene información (Nombre completo de clientes, Tipo de ificación, Número de identificación, correo electrónico nal y corporativo, Fecha de Nacimiento, Dirección de encia, Dirección de Oficina, Dirección de Correspondencia, o, Ciudad, Departamento, Código Postal, Teléfono de Oficina, ono Celular, Segmento, Estado del cliente, Profesión, Estrato, , Estado Civil, Cargo, Código CIIU, Fecha de ingreso a la a empresa, Tipo de Actividad, Tipo de Contrato, Tipo de io, Total de Ingresos, Rango de Ingresos, Total Egresos, NIT Empresa, Nombre de la Empresa)
AR37	TARPRO1 / TARPRO2	Cliente	Tar_Benefi	Información de beneficiarios o amparados	PII	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Fecha de Nacimiento, Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento, Código Postal, Teléfono de Oficina, Teléfono Celular, Segmento, Estado del cliente, Profesión, Estrato, Sexo, Estado Civil, Cargo, Código CIIU, Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos, NIT de la Empresa, Nombre de la Empresa)
AR38	TARPRO1 / TARPRO2	Producto	Tar_Contrat	Información de número de contrato y PAN en claro	PII/PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, PAN de la tarjeta en claro, número de plástico, franquicia, tipo de tarjeta, fehca alta tarjeta, estado tarjeta, bloqueo, fecha caducidad tarjeta, fecha último reenvío renovación, titular o beneficiario, no renovación, fecha próximo cobro cuota, nombre estampado, fecha de baja, motivo de baja, fecha último uso, comentario de bloqueo, fecha último bloqueo)
AR39	TARPRO1 / TARPRO2	Producto	Tar_Expedic	Información reexpedición de tarjeta	PII/PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, Motivo de reexpedición, fecha de reexpedición, nombre en plástico, cupo de tarjeta)
AR40	TARPRO1 / TARPRO2	Producto	Tar_Transacc	Información de Transacciones	PII/PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, Producto, subproducto, fecha de alta, código condición económica, grupo de liquidación, número de beneficiarios, código de bloqueo, fecha del último bloqueo, situación del contrato Impagado, saldo impagado, importe cobrado y aplicado, intereses corrientes, intereses de mora, fecha última aplicación, total de puntos, puntos periodo anterior, punto generados en último corte, puntos redimidos, puntos vencidos, puntos a vencer, fecha vencimiento de puntos, calificación interna, calificación endeudamiento, tipo de moneda, cartera castigada, saldo castigado, fecha último rediferido, fecha de refinanciación, valor refinanciación, indicador pago primera cuota, fecha primera compra, fecha

Archivo N°	Base de Datos	Esquema	Nombre de Tabla	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
										cambio de cupo, tipo cambio de cupo, cupo anterior, cupo nuevo, valor acumulado de IVA)
AR41	TARPRO1 / TARPRO2	Producto	Tar_Cta_tarj	Información de Tarjeta	PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, PAN de la tarjeta en claro, número de plástico, franquicia, tipo de tarjeta, fehca alta tarjeta, estado tarjeta, bloqueo, fecha caducidad tarjeta, fecha último reenvío renovación, titular o beneficiario, no renovación, fecha próximo cobro cuota, nombre estampado, fecha de baja, motivo de baja, fecha último uso, comentario de bloqueo, fecha último bloqueo)
AR42	TARPRO1 / TARPRO2	Producto	Tar_Franqui	Información de Franquicias	PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, PAN de la tarjeta en claro, número de plástico, franquicia, tipo de tarjeta, fehca alta tarjeta, estado tarjeta, bloqueo, fecha caducidad tarjeta, fecha último reenvío renovación, titular o beneficiario, no renovación, fecha próximo cobro cuota, nombre estampado, fecha de baja, motivo de baja, fecha último uso, comentario de bloqueo, fecha último bloqueo)
AR43	TARPRO1 / TARPRO2	Extractos	Tar_Cliente	Información de clientes	PII	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Fecha de Nacimiento, Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento, Código Postal, Teléfono de Oficina, Teléfono Celular, Segmento, Estado del cliente,Profesión, Estrato, Sexo, Estado Civil, Cargo, Código CIIU, Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos, NIT de la Empresa, Nombre de la Empresa)
AR44	TARPRO1 / TARPRO2	Extractos	Tar_Benefi	Información de beneficiarios o amparados	PII	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Fecha de Nacimiento, Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento, Código Postal, Teléfono de Oficina, Teléfono Celular, Segmento, Estado del cliente, Profesión, Estrato, Sexo, Estado Civil, Cargo, Código CIIU, Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos, NIT de la Empresa, Nombre de la Empresa)
AR45	TARPRO1 / TARPRO2	Extractos	Tar_Cupos	Información de cupos y saldos	PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, Capital, comisiones última facturación, intereses última facturación, impuestos última facturación, Honorarios, intereses de mora, avance en el periodo, compras en el periodo, pago mínimo, pago total, número de cuotas pagadas, plazo de la deuda, fecha del último extracto, fecha de liquidación, fecha próximo vencimiento)
AR46	TARPRO1 / TARPRO2	Extractos	Tar_Cuota	Información de saldos a pagar y facturación	PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, fecha inicio de mora, número días en mora, número de cuotas en mora, altura de mora, valor de mora, saldo total otros conceptos, saldo a favor, Total pagos última factura, Valor devolución IVA, valor último pago, fecha último pago, fecha última facturación, saldos, cupo disponible, comisiones, intereses, reversos)
AR47	TARPRO1 / TARPRO2	Extractos	Tar_Fechas	Información de fechas de pago	PCI	Gerencia de Operaciones	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, PAN de la tarjeta en claro, número de plástico, franquicia,

Archivo N°	Base de Datos	Esquema	Nombre de Tabla	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
						Tarjetas				tipo de tarjeta, fecha alta tarjeta, estado tarjeta, bloqueo, fecha caducidad tarjeta, fecha último reenvío renovación, titular o beneficiario, no renovación, fecha próximo cobro cuota, nombre estampado, fecha de baja, motivo de baja, fecha último uso, comentario de bloqueo, fecha último bloqueo)
AR48	TARPRO1 / TARPRO2	Extractos	Tar_Comercio	Información de comercios	PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, Tipo de la factura, descripción tipo de la factura, fecha de la factura, número de referencia de la factura, PAN de la tarjeta en claro, código de la moneda de la operación, número de autorización, código de comercio, nombre de comercio reducido, código de actividad, fecha contable de la operación, tipo de franquicia, fecha de liquidación, número de cuotas de la compra, saldos pendientes de diferir, cuotas pendientes de facturación)
AR49	TARPRO1 / TARPRO2	Contabilidad	Tar_Comision	Información de comisiones generadas y pagadas	PII/PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, Capital, comisiones última facturación, intereses última facturación, impuestos última facturación, Honorarios, intereses de mora, avance en el periodo, compras en el periodo, pago mínimo, pago total, número de cuotas pagadas, plazo de la deuda, fecha del último extracto, fecha de liquidación, fecha próximo vencimiento)
AR50	TARPRO1 / TARPRO2	Contabilidad	Tar_Impuesto	Información de impuestos	PII/PCI	Gerencia de Operaciones Tarjetas	CORE TARJETAS	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, Capital, comisiones última facturación, intereses última facturación, impuestos última facturación, Honorarios, intereses de mora, avance en el periodo, compras en el periodo, pago mínimo, pago total, número de cuotas pagadas, plazo de la deuda, fecha del último extracto, fecha de liquidación, fecha próximo vencimiento)

Nota. La tabla muestra las tablas y el detalle de los campos que fueron identificacos, donde se almacena información sensible (PII y PCI) en la aplicación Core Tarjetas. Elaboración propia.

7.6.4.3 CRM. Como parte del proceso de identificación de archivos críticos que contienen información sensible (PII), se realiza un análisis puntual sobre la aplicación CRM. En esta revisión se evidencian tablas de base de datos que almacenan información demográfica e identificable de los clientes, utilizada para la gestión comercial, atención y seguimiento de servicios. A continuación, se detallan los campos identificados en la tabla 7.

Tabla 7.

Identificación de tablas en bases de datos CMR

Archivo N°	Base de Datos	Esquema	Nombre de Tabla	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
AR51	CRMPRO1 / CRMPRO2	Cliente	C_CLIENT	Tabla principal información de clientes	PII	Gerencia de CRM	CRM	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Fecha de Nacimiento, Teléfono de Oficina, Teléfono Celular, Segmento, Estado del cliente, Profesión, Estrato, Sexo, Estado Civil, Cargo, Código CIIU)
AR52	CRMPRO1 / CRMPRO2	Cliente	C_ADDRESS1	Direcciones	PII	Gerencia de CRM	CRM	Contraseña, Roles, Perfiles	Diario	Contiene información (Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento)
AR53	CRMPRO1 / CRMPRO2	Cliente	C_ADDR_CLI	Direcciones con clientes	PII	Gerencia de CRM	CRM	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Fecha de Nacimiento, Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento, Código Postal)
AR54	CRMPRO1 / CRMPRO2	Cliente	C_PHONE_CL	Teléfonos clientes	PII	Gerencia de CRM	CRM	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Teléfono de Oficina, Teléfono Celular)
AR55	CRMPRO1 / CRMPRO2	Cliente	C_CLIENT_E	Tabla extendida de campos de clientes	PII	Gerencia de CRM	CRM	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento, Código Postal, Teléfono de Oficina, Teléfono Celular, Segmento, Estado del cliente, Profesión, Estrato, Sexo, Estado Civil, Cargo, Código CIIU, Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos)
AR56	CRMPRO1 / CRMPRO2	Cliente	C_CLIEN_FN	Tabla extendida de campos de clientes	PII	Gerencia de CRM	CRM	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Fecha de Nacimiento, Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento, Código Postal)
AR57	CRMPRO1 / CRMPRO2	Cliente	C_CLI_FNMX	Tabla información Financiera	PII	Gerencia de CRM	CRM	Contraseña, Roles, Perfiles	Diario	Contiene Información (Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos, NIT de la Empresa, Nombre de la Empresa

Nota. La tabla muestra las tablas y el detalle de los campos que fueron identificacos, donde se almacena información sensible (PII y PCI) en la aplicación CRM. Elaboración propia.

7.6.4.4 Originador. Como parte del proceso de identificación de archivos críticos que contienen información sensible (PII), se realiza un análisis específico sobre la aplicación Originador, utilizada para la gestión y procesamiento de solicitudes de productos financieros.

Durante la revisión, se identifican estructuras de datos y tablas de base de datos que almacenan información personal de los clientes, capturada durante el proceso de originación. Esta información incluye datos como nombres completos, números de identificación, datos de contacto, información laboral, referencias personales y detalles financieros, los cuales son utilizados para la evaluación y aprobación de productos.

A continuación, en la tabla 8, se lista la información relevante contenida en las bases de datos:

Tabla 8.

Identificación de tablas en bases de datos Originador

Archivo N°	Base de Datos	Esquema	Nombre de Tabla	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
AR58	ORIPRO1 / ORIOPRO2	Cliente	O_cliente	Información de clientes	PII	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal y corporativo, Fecha de Nacimiento, Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento, Código Postal, Teléfono de Oficina, Teléfono Celular, Segmento, Estado del cliente, Profesión, Estrato, Sexo, Estado Civil, Cargo, Código CIIU, Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos, NIT de la Empresa, Nombre de la Empresa)
AR59	ORIPRO1 / ORIOPRO2	Cliente	O_direcci	Información de ubicación y contacto clientes	PII	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Dirección de residencia, Dirección de Oficina, Dirección de Correspondencia, Barrio, Ciudad, Departamento)
AR60	ORIPRO1 / ORIOPRO2	Producto	O_Pasivo	Información Productos de cuentas, CDT, AFC	PII	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de producto, estado de producto, bloqueo, fecha de bloqueo, titular – relacionado, renovación, fecha de cancelación, Fecha de apertura, motivo de cancelación, fecha último uso, comentario de bloqueo, fecha último bloqueo)
AR61	ORIPRO1 / ORIOPRO2	Producto	O_Activo	Información Productos de crédito	PII	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de Producto, fecha de alta de producto, código condición económica, grupo de liquidación, aplicado, intereses corrientes, intereses de mora, fecha última aplicación, calificación interna, calificación endeudamiento, tipo de moneda, cartera castigada, saldo castigado, indicador pago primera cuota)
AR62	ORIPRO1 / ORIOPRO2	Producto	O_Tarjeta	Información Producto de crédito y débito	PII/PCI	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, Número de contrato, PAN de la tarjeta en claro, número de plástico, franquicia, tipo de tarjeta, fecha alta tarjeta, estado tarjeta, bloqueo, fecha caducidad tarjeta, fecha último reenvío renovación, titular o beneficiario, no renovación, fecha próximo cobro cuota, nombre estampado, fecha de baja, motivo de baja, fecha último uso, comentario de bloqueo, fecha último bloqueo)

Archivo N°	Base de Datos	Esquema	Nombre de Tabla	Descripción del archivo	Tipo de información (PII / PCI)	Propietario	Sistema asociado	Controles de acceso aplicados	Frecuencia de uso	Observaciones
AR63	ORIPRO1 / ORIOPRO2	Producto	O_Pagare	Información de garantias	PII	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Código Entidad, número de producto, Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal, montos, dirección de correspondencia, fecha de vencimiento)
AR64	ORIPRO1 / ORIOPRO2	Riesgo	O_Experian	Información central de riesgo	PII	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, Fecha de Nacimiento, CIIU, Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos)
AR65	ORIPRO1 / ORIOPRO2	Riesgo	O_Cifin	Información central de riesgo	PII/PCI	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, Fecha de Nacimiento, CIIU, Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos)
AR66	ORIPRO1 / ORIOPRO2	Riesgo	O_Reconoce	Información de Biometría	PII	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, correo electrónico personal, Fecha de Nacimiento, Dirección de residencia, Barrio, Ciudad, Departamento, Código Postal, Teléfono principal, Teléfono Celular)
AR67	ORIPRO1 / ORIOPRO2	Riesgo	O_Bureau	Información centralizada	PII/PCI	Gerencia de Productos y Soluciones Digitales	Originador	Contraseña, Roles, Perfiles	Diario	Contiene información (Nombre completo de clientes, Tipo de Identificación, Número de identificación, Fecha de Nacimiento, CIIU, Fecha de ingreso a la última empresa, Tipo de Actividad, Tipo de Contrato, Tipo de Salario, Total de Ingresos, Rango de Ingresos, Total Egresos)

Nota. La tabla muestra las tablas y el detalle de los campos que fueron identificacos, donde se almacena información sensible (PII y PCI) en la aplicación Originador. Elaboración propia.

7.6.5 Revisión de Políticas, Procedimientos y Matrices de Acceso Vigentes

Se realiza una revisión integral de las políticas, procedimientos y matrices de acceso vigentes en las aplicaciones críticas, con el fin de verificar su alineación con los principios de seguridad de la información, mínimo privilegio, necesidad de conocer y cumplimiento normativo.

7.6.5.1 Políticas de seguridad de la información. Se realiza la entrevista y solicitud formal de documentación al equipo de Gobierno de Consultoría de Seguridad del Banco, con el objetivo de obtener los estándares, políticas y líneas base que orientan los lineamientos de seguridad utilizados como guía para la implementación en las aplicaciones incluidas en el alcance del proyecto. Como resultado, se recibe documentación que permite evaluar si los controles definidos están actualizados y alineados con los marcos normativos ISO/IEC 27001:2022 y PCI DSS v4.0.1. Esta documentación incluye políticas de seguridad, procedimientos operativos y matrices de acceso que establecen criterios para la gestión de usuarios, perfiles y privilegios. Adicionalmente, se realiza una entrevista y solicitud formal de documentación al equipo de Control de Acceso del Banco, enfocada en los manuales y procedimientos relacionados con la gestión de usuarios y perfiles. Como respuesta, se recibe el Manual de Gestión de Usuarios y Perfiles, el cual sirve como base para la revisión de la gestión de accesos en las aplicaciones Core.

Durante esta revisión, se identifica que la documentación contempla lineamientos que incorporan los principios de mínimo privilegio, necesidad de saber y segregación de funciones, así como prácticas de certificación periódica de accesos. Estos elementos contribuyen a fortalecer la seguridad lógica y el cumplimiento regulatorio. Los hallazgos identificados se documentan en la matriz documental, la cual se presenta en la tabla 9

Tabla 9.

Marco de gobierno de seguridad

Tipo de Documento	Nombre del Documento	Fecha de Emisión	Última Actualización	Estado	Brechas Identificadas	Recomendación	Responsable
Estándar	Protección de Datos	30/10/2023	11/10/2023	Vigente	Falta de capacitación. Acceso o divulgación no autorizada. Envío erróneo de correos, pérdida de dispositivos con datos, ciberataques, eliminación accidental de información.	Se debe socializar el estándar para las áreas operativas con el fin de identificar la importancia de la aplicabilidad en los procesos de las áreas. Uso o implementación de herramientas de DLP, DdoS, IPS, Backups de información (DBR)	Director de seguridad de la Información (CISO)
Estándar	Gestión de identidades y acceso	25/03/2025	14/03/2025	Vigente	Accesos excesivos o no revocados Falta de autenticación multifactor (MFA) Gestión inadecuada de roles	Implementar autenticación multifactor. Revisar y auditar accesos regularmente. Definir roles y permisos con precisión. Usar o Implementar aplicaciones que permitan identificar la trazabilidad y accesos a información PII y PCI.	Director de Políticas y Concientización sobre Ciberseguridad
Estándar común	Estándar de Clasificación de Seguridad de la Información y los Sistemas	1/12/2023	30/10/2023	Vigente	Clasificación incorrecta. Ausencia de clasificación. Falta de capacitación. Desactualización de niveles.	Establecer una política clara de clasificación de información. Capacitar a todos los usuarios en el uso de dicha política. Integrar los niveles de clasificación en los sistemas tecnológicos. Realizar auditorías periódicas para verificar cumplimiento. Actualizar clasificaciones según cambios regulatorios o de negocio.	Director de Seguridad de la Información (CISO)
Estándar	Seguridad de Activos de Información Críticos (CIA)	22/11/2024	21/11/2024	Vigente	Modificaciones no autorizadas. Accesos indebidos.	Clasificar los activos según su nivel de criticidad. Aplicar controles de acceso basados en el principio de menor privilegio. Implementar autenticación multifactor (MFA). Realizar auditorías periódicas y pruebas de integridad.	Director de Seguridad de la Información (CISO)
Estándar común	Gestión de Incidentes de Tecnología Global	1/02/2024	31/01/2024	Vigente	Clasificación inadecuada. Escasa capacitación. Ausencia de análisis post-incidente.	Implementar modelos de clasificación y priorización. Capacitación continua y simulacros periódicos. Realizar revisiones y aplicar mejoras continuas.	Director, Gestión de Servicios de TI, Tecnología Global y Plataformas Institucionales
Estándar	Registro y Monitoreo de eventos	27/02/2025	31/01/2025	Vigente	Eventos no registrados. Registros poco claros o incompletos. Monitoreo insuficiente. Falta de escalamiento y alertas. Ausencia de revisión periódica.	Implementar una política de auditoría clara, con procedimientos definidos. Usar herramientas de monitoreo centralizado como SIEM. Establecer umbrales de alerta y flujos de escalamiento automático. Proteger los registros contra modificaciones y accesos no autorizados. Realizar revisiones periódicas y conservar los logs por el tiempo necesario para análisis	Director de Seguirdad de la Información (CISO)

Tipo de Documento	Nombre del Documento	Fecha de Emisión	Última Actualización	Estado	Brechas Identificadas	Recomendación	Responsable
						forense.	
Estándar	Autenticación del Personal	29/07/2025	21/07/2025	Vigente	Contraseñas débiles o reutilizadas. Ausencia de autenticación multifactor (MFA). Falta de capacitación del personal. Accesos compartidos. Errores humanos.	Implementar MFA obligatoria en todos los accesos críticos. Usar gestores de contraseñas seguros y políticas de renovación periódica. Capacitar al personal en seguridad y detección de phishing. Asignar credenciales individuales y evitar accesos compartidos. Monitorear accesos y establecer alertas ante comportamientos sospechosos.	Director de Seguridad de la Información (CISO)
Estándar común	Estándar de Seguridad de Aplicaciones	30/10/2023	20/10/2023	Vigente	Uso inadecuado de credenciales. Autenticación insegura. Comunicación insegura. Gestión deficiente de sesiones. Exposición de datos sensibles. Registro y monitoreo ineficaz.	Integrar seguridad desde el diseño (DevSecOps). Realizar pruebas de penetración y análisis estático de código. Implementar autenticación multifactor y cifrado fuerte.	Director de Seguridad de la Información (CISO)
Estándar	Código de Conducta	1/11/2024	29/10/2024	Vigente	Conflictos de interés / Soborno / Corrupción. Incumplimiento de normas y procedimientos. Falta de formación ética. Ausencia de seguimiento disciplinario.	Fortalecer la formación ética continua. Capacitación continua. Evaluación y actualización del código. Fomentar el liderazgo ético. Auditorías éticas y controles internos. Gestión de conflictos de interés Declaraciones periódicas de intereses personales y familiares.	Junta Directiva
Política	Política de Conducta Indebida del Empleado y Gestión de Consecuencias	31/05/2022	feb-22	Caducada	Uso indebido de recursos. Violaciones éticas. Incumplimiento normativo. Riesgos a la seguridad.	Diseñar un sistema de consecuencias: desde amonestaciones verbales hasta desvinculación laboral. Establecer canales de denuncia efectivos. Capacitar en ética y cumplimiento. Auditorías internas periódicas. Monitoreo de reincidencias.	Junta Directiva
Política	Política de Ciberseguridad de The Bank of Nova Scotia	13/08/2024	jun-24	Vigente	Phishing y suplantación. Violación de escritorio limpio. Falta de segmentación de red. Falta de cultura de seguridad. Capacitación insuficiente del personal. Políticas desactualizadas o genéricas. Subestimar el riesgo reputacional.	Revisión periódica de políticas. Segmentación de red y control de accesos. Autenticación multifactor (MFA). Simulacros de phishing y formación. Evaluación de terceros. SIEM y monitoreo 24/7.	Director de Seguridad de la Información (CISO)
Manual	Manual de Gestión de Usuarios y Perfiles	6/06/2025	28/05/2025	Vigente	Asignación excesiva de privilegios. Falta de estandarización en la creación y baja de usuarios. Gestión inadecuada de perfiles. Falta de automatización. Deficiencias en la capacitación.	Definir roles y permisos claros y revisarlos periódicamente. Implementar autenticación multifactor (MFA). Automatizar la gestión de identidades y accesos. Establecer flujos de trabajo estandarizados para creación y baja de usuarios. Capacitar a los usuarios en seguridad digital.	Director de Control de Acceso Lógico

Tipo de Documento	Nombre del Documento	Fecha de Emisión	Última Actualización	Estado	Brechas Identificadas	Recomendación	Responsable
Línea Base	IBM i Security	12/06/2025	6/06/2025	Vigente	Sistemas sin parches críticos. Falta de cifrado en reposo o tránsito.	Implementar autenticación multifactor (MFA). Realizar revisiones periódicas de configuración y accesos. Mantener actualizados todos los sistemas y software (PTF's). Capacitar al personal en ciberseguridad y phishing.	Director de S'guridad de la Información (CISO)
Línea Base	Oracle Data base Security	1/05/2025	10/04/2025	Vigente	Sistemas sin parches críticos. Falta de cifrado de datos en reposo o tránsito. Software malicioso o vulnerabilidades explotadas.	Implementar autenticación multifactor (MFA). Usar cifrado fuerte para datos sensibles. Realizar revisiones periódicas de configuración y accesos. Mantener actualizados todos los sistemas y software. Capacitar al personal en ciberseguridad y phishing.	Director de Seguridad de la Información (CISO)
Línea Base	Red Hat Enterprise Linux an above Security	22/11/2024	20/11/2024	Vigente	Sistemas sin parches críticos. Envío incorrecto de información. Ingeniería Social, Phishing.	Implementar autenticación multifactor (MFA). Usar cifrado fuerte para datos sensibles. Realizar revisiones periódicas de configuración y accesos. Mantener actualizados todos los sistemas y software. Capacitar al personal en ciberseguridad y phishing.	Director de Seguridad de la Información (CISO)
Línea Base	SQL Server Data base Security	5/03/2025	27/02/2025	Vigente	Sistemas sin parches críticos. Falta de cifrado de datos en reposo o tránsito. Software malicioso o vulnerabilidades explotadas.	Implementar autenticación multifactor (MFA). Usar cifrado fuerte para datos sensibles. Realizar revisiones periódicas de configuración y accesos. Mantener actualizados todos los sistemas y software. Capacitar al personal en ciberseguridad y phishing.	Director de Seguridad de la Información (CISO)
Línea Base	Windows Server Security	22/11/2024	21/11/2024	Vigente	Sistemas sin parches críticos. Envío incorrecto de información. Ingeniería Social, Phishing.	Implementar autenticación multifactor (MFA). Usar cifrado fuerte para datos sensibles. Realizar revisiones periódicas de configuración y accesos. Mantener actualizados todos los sistemas y software. Capacitar al personal en ciberseguridad y phishing.	Director de Seguridad de la Información (CISO)

Nota. En la tabla se registran los estandares, lineamientos y políticas de seguridad para el alcance del proyecto. Elaboración propia.

7.6.5.2 Revisión técnica de accesos. Se realiza una revisión técnica de los accesos implementados en las aplicaciones incluidas en el alcance del diagnóstico, con el objetivo de validar la efectividad, coherencia y seguridad de los mecanismos de control de acceso lógico.

7.6.5.2.1 Revisión de mecanismos de autenticación y autorización implementados. Se realiza la revisión de los mecanismos de autenticación y autorización implementados en las aplicaciones Core incluidas en el alcance del proyecto, con el objetivo de validar el cumplimiento de los controles de seguridad establecidos por las normas ISO/IEC 27001:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014.

Durante el análisis, se identifican los siguientes aspectos claves (ver tabla 10) que permite identificar fortalezas y oportunidades de mejora en la protección de la información sensible (PII y PCI) y en la administración de los accesos.

Tabla 10.

Mecanismos de autenticación

Sistema / Aplicación	Tipo de Mecanismo	Descripción del Mecanismo	Responsable	Nivel de Criticidad (Alto/Medio/Bajo)	Evidencia Disponible (Sí/No)	Ubicación de la Evidencia	Observaciones
Core Banco	Contraseña	Aplicación solicita contraseña de autenticación por usuario (Contraseñas alfanuméricas, políticas de complejidad, caducidad)	IT Owner / Control de Acceso Lógico	Alto	Sí	Sitio de SharePoint Control de Acceso	Cuenta con una longitud de mínimo 8 y un máximo de 10 caracteres, lo que se identifica como una contraseña débil. Solicita dígito y carácter especial. Caducidad de 30 días. Intentos inválidos hasta 3 y bloquea la cuenta.
	MFA	Múltiple Factor de Autenticación para accesos privilegiados (PAM) (Contraseña + token OTP)	IT Owner / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Los accesos con MFA son exclusivamente para usuarios administradores o usuarios con altos privilegios de acceso a la aplicación, seguridad e infraestructura. No cuenta con MFA para usuarios de negocio con acceso a la aplicación. EL MFA solo aplica para conexiones remotas a la estación de trabajo para la conexión mediante VPN.
	Roles	Matriz de acceso para áreas de negocio, acceso según rol asignado. (Usuario, administrador, auditor)	Gerente área de negocio / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Existe una matriz de acceso para las áreas de negocio del Banco, pero no se encuentra automatizada, el mantenimiento es manual.
	Perfiles	Perfiles segregados por área de negocio, conjunto de permisos agrupados. (Perfil de operaciones, perfil de seguridad, etc.)	Gerente área de negocio / IT Owner/ Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Se encuentran perfiles definidos para las áreas de negocio, algunos sin una segregación de funciones actualizada.
	Autenticación basada en red	Validación según ubicación o IP (Acceso permitido solo desde red interna)	Infraestructura / Control de Acceso Lógico	Bajo	Sí	Sitio de SharePoint Infraestructura TI / Control de Acceso	Se encuentra administrada desde el Firewall y la aplicación cuenta con un módulo de seguridad que permite autorizar segmentos de red o conexiones ODBC.
	Listas de control de acceso (ACL)	Permisos definidos por recurso. (Usuario puntual puede leer archivo puntual, ejecutar comando puntual).	Control de Acceso Lógico	Alto	Sí	Sitio de SharePoint Infraestructura TI	La aplicación cuenta con un módulo de seguridad que controla desde ACL autorizaciones puntuales a usuarios, no cuenta con validación de autorizaciones con frecuencia.
	Certificados digitales	Uso de certificados X.509 para autenticación. (Certificados cliente en aplicaciones bancarias.)	Infraestructura / Seguridad Técnica / Control de Acceso Lógico	Bajo	Sí	Sitio de SharePoint Infraestructura TI / Seguridad Técnica / Control de Acceso	La aplicación cuenta con certificados digitales para la conexión segura mediante TLS/SSL (usado en HTTPS) y se utilizan para verificar la identidad de servidores, clientes, y otros recursos en la red. Al igual que utiliza puerto seguro para el Client Access por el que acceden los usuarios de negocio.
Core Tarjetas	Contraseña	Aplicación solicita contraseña de autenticación por usuario (Contraseñas alfanuméricas, políticas de complejidad, caducidad)	IT Owner / Control de Acceso Lógico	Alto	Sí	Sitio de SharePoint Control de Acceso	Cuenta con una longitud de mínimo 8 y un máximo de 10 caracteres, lo que se identifica como una contraseña débil. Solicita dígito y carácter especial. Caducidad de 30 días. Intentos inválidos hasta 3 y bloquea la cuenta.

Sistema / Aplicación	Tipo de Mecanismo	Descripción del Mecanismo	Responsable	Nivel de Criticidad (Alto/Medio/Bajo)	Evidencia Disponible (Sí/No)	Ubicación de la Evidencia	Observaciones
	MFA	Múltiple Factor de Autenticación para accesos privilegiados (PAM) (Contraseña + token OTP)	IT Owner / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Los accesos con MFA son exclusivamente para usuarios administradores o usuarios con altos privilegios de acceso a la infraestructura. No cuenta con MFA para usuarios de negocio con acceso a la aplicación. EL MFA solo aplica para conexiones remotas a la estación de trabajo para la conexión mediante VPN.
	Roles	Matriz de acceso para áreas de negocio, acceso según rol asignado. (Usuario, administrador, auditor)	Gerente área de negocio / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Existe una matriz de acceso para las áreas de negocio del Banco, pero no se encuentra automatizada, el mantenimiento es manual.
	Perfiles	Perfiles segregados por área de negocio, conjunto de permisos agrupados. (Perfil de operaciones, perfil de seguridad, etc.)	Gerente área de negocio / IT Owner/ Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Se encuentran perfiles definidos para las áreas de negocio, algunos sin una segregación de funciones actualizada.
	Autenticación basada en red	Validación según ubicación o IP (Acceso permitido solo desde red interna)	Infraestructura	Bajo	Sí	Sitio de SharePoint Infraestructura TI / Control de Acceso	Se encuentra administrada desde el Firewall que permite autorizar segmentos de red.
	Listas de control de acceso (ACL)	Permisos definidos por recurso. (Usuario puntual puede ver número de Tarjeta en claro)	Control de Acceso Lógico	Alto	Sí	Sitio de SharePoint Infraestructura TI	La aplicación cuenta con un módulo de seguridad que gestiona autorizaciones específicas mediante Listas de Control de Acceso (ACL), permitiendo a ciertos usuarios visualizar números de tarjeta en claro.
	Certificados digitales	Uso de certificados X.509 para autenticación. (Certificados cliente en aplicaciones bancarias.)	Infraestructura / Seguridad Técnica / Control de Acceso Lógico	Bajo	Sí	Sitio de SharePoint Infraestructura TI / Seguridad Técnica / Control de Acceso	La aplicación cuenta con certificados digitales para la conexión segura mediante TLS/SSL (usado en HTTPS) y se utilizan para verificar la identidad de servidores, clientes, y otros recursos en la red.
	Contraseña	Aplicación solicita contraseña de autenticación por usuario (Contraseñas alfanuméricas, políticas de complejidad, caducidad)	IT Owner / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	La aplicación se encuentra integrada al Directorio Activo (LDAP) del Banco, configurada con niveles de seguridad de mínimo 14 caracteres. Solicita dígito y carácter especial. Caducidad de 180 días. Intentos inválidos hasta 3 y bloquea la cuenta del Directorio Activo.
CRM	MFA	Múltiple Factor de Autenticación para accesos privilegiados (PAM) (Contraseña + token OTP)	IT Owner / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Los accesos con MFA son exclusivamente para usuarios administradores o usuarios con altos privilegios de acceso a la infraestructura. No cuenta con MFA para usuarios de negocio con acceso a la aplicación. EL MFA solo aplica para conexiones remotas a la estación de trabajo para la conexión mediante VPN.
	Roles	Matriz de acceso para áreas de negocio, acceso según rol asignado. (Usuario, administrador, auditor)	Gerente área de negocio / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Existe una matriz de acceso para las áreas de negocio del Banco, pero no se encuentra automatizada, el mantenimiento es manual.
	Perfiles	Perfiles segregados por área de negocio, conjunto de permisos agrupados. (Perfil de operaciones, perfil de seguridad, etc.)	Gerente área de negocio / IT Owner/ Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Se encuentran perfiles definidos para las áreas de negocio, algunos sin una segregación de funciones actualizada.

Sistema / Aplicación	Tipo de Mecanismo	Descripción del Mecanismo	Responsable	Nivel de Criticidad (Alto/Medio/Bajo)	Evidencia Disponible (Sí/No)	Ubicación de la Evidencia	Observaciones
Originador	Autenticación basada en red	Validación según ubicación o IP (Acceso permitido solo desde red interna)	Infraestructura	Bajo	Sí	Sitio de SharePoint Infraestructura TI / Control de Acceso	Se encuentra administrada desde el Firewall que permite autorizar segmentos de red.
	Certificados digitales	Uso de certificados X.509 para autenticación. (Certificados cliente en aplicaciones bancarias.)	Infraestructura / Seguridad Técnica / Control de Acceso Lógico	Bajo	Sí	Sitio de SharePoint Infraestructura TI / Seguridad Técnica / Control de Acceso	La aplicación cuenta con certificados digitales para la conexión segura mediante TLS/SSL (usado en HTTPS) y se utilizan para verificar la identidad de servidores, clientes, y otros recursos en la red.
	Contraseña	Aplicación solicita contraseña de autenticación por usuario (Contraseñas alfanuméricas, políticas de complejidad, caducidad)	IT Owner / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	La aplicación se encuentra integrada al Directorio Activo (LDAP) del Banco, configurada con niveles de seguridad de mínimo 14 caracteres. Solicita dígito y carácter especial. Caducidad de 180 días. Intentos inválidos hasta 3 y bloquea la cuenta del Directorio Activo.
	MFA	Múltiple Factor de Autenticación para accesos privilegiados (PAM) (Contraseña + token OTP)	IT Owner / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Los accesos con MFA son exclusivamente para usuarios administradores o usuarios con altos privilegios de acceso a la infraestructura. No cuenta con MFA para usuarios de negocio con acceso a la aplicación. EL MFA solo aplica para conexiones remotas a la estación de trabajo para la conexión mediante VPN.
	Roles	Matriz de acceso para áreas de negocio, acceso según rol asignado. (Usuario, administrador, auditor)	Gerente área de negocio / Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Existe una matriz de acceso para las áreas de negocio del Banco, pero no se encuentra automatizada, el mantenimiento es manual.
	Perfiles	Perfiles segregados por área de negocio, conjunto de permisos agrupados. (Perfil de operaciones, perfil de seguridad, etc.)	Gerente área de negocio / IT Owner/ Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Se encuentran perfiles definidos para las áreas de negocio, algunos sin una segregación de funciones actualizada.
	Autenticación basada en red	Validación según ubicación o IP (Acceso permitido solo desde red interna)	Infraestructura	Bajo	Sí	Sitio de SharePoint Infraestructura TI / Control de Acceso	Se encuentra administrada desde el Firewall que permite autorizar segmentos de red.
	Certificados digitales	Uso de certificados X.509 para autenticación. (Certificados cliente en aplicaciones bancarias.)	Infraestructura / Seguridad Técnica / Control de Acceso Lógico	Bajo	Sí	Sitio de SharePoint Infraestructura TI / Seguridad Técnica / Control de Acceso	La aplicación cuenta con certificados digitales para la conexión segura mediante TLS/SSL (usado en HTTPS) y se utilizan para verificar la identidad de servidores, clientes, y otros recursos en la red.
	Grupos de seguridad	Usuarios agrupados con permisos comunes. (Grupo “Gestores de productos” con acceso a informes)	Gerente área de negocio / IT Owner/ Control de Acceso Lógico	Medio	Sí	Sitio de SharePoint Control de Acceso	Existen grupos de seguridad que se encuentran creados en el Directorio Activo (LDAP) que permiten autorizar a los usuarios a los perfiles de acceso configurados en la aplicación.

Nota. En la tabla se registran los mecanismos de autenticación evaluados para cada aplicación, junto con los hallazgos. Elaboración propia.

7.6.5.2.2 Análisis de segregación de funciones de accesos indebidos. Se realiza una revisión de los procesos de segregación de funciones implementados en cada aplicación crítica, con el objetivo de prevenir accesos indebidos y garantizar la integridad de los procesos operativos y de seguridad.

Este análisis permite identificar funciones que no deben coexistir en un mismo perfil o usuario, especialmente en contextos sensibles como:

- La visualización de datos personales o financieros (PII/PCI).
- El acceso a archivos clasificados como críticos.
- La gestión de accesos y privilegios.

La segregación adecuada de funciones, acompañada de revisiones periódicas, contribuye a:

- Reducir el riesgo de abuso de privilegios.
- Fortalecer el cumplimiento de los principios de mínimo privilegio y necesidad de conocer.
- Alinear los controles con los requisitos de ISO/IEC 27001:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia.

7.6.5.2.3 Procedimientos operativos. Se realiza la entrevista y la solicitud formal de documentación sobre las funciones por cargo de los funcionarios del área de Control de Acceso Lógico del Banco. Como respuesta, se reciben los formatos correspondientes, los cuales detallan las funciones de los usuarios encargados de administrar la seguridad de las aplicaciones Core. Esta información sirve como base para la revisión de la administración de los accesos requeridos por las áreas operativas. Durante el análisis, se identifica que la documentación incluye información sobre las aplicaciones administradas, la segregación de funciones, la certificación de

accesos, la gestión de accesos y el manejo de incidencias y excepciones, validando que las actividades operativas estén alineadas con los estándares establecidos por las normas ISO/IEC 27001:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014.

7.6.5.3 Matrices de acceso. Se realiza la entrevista y la solicitud formal de documentación de las Matrices de Acceso al equipo de Control de Acceso del Banco, correspondientes a las áreas operativas incluidas en el alcance del proyecto. Como respuesta, se reciben las matrices de acceso de la Gerencia de Operaciones, las cuales sirven como base para la revisión de los accesos requeridos por cargo sobre las aplicaciones Core.

Durante esta revisión, se identifica que la documentación contempla elementos clave como el control de versiones, las áreas funcionales, los cargos, las aplicaciones y los perfiles autorizados por cargo, lo que permite validar la alineación de los accesos con los principios de seguridad y segregación de funciones.

A continuación, en la tabla 11, se presenta un modelo de la matriz de acceso correspondiente a la Gerencia de Operaciones.

Tabla 11.

Matriz de Acceso Gc Operaciones (Modelo)

Cod	VP	Gerencia	Dirección	Cargos Activos	Categoría	Core Banco	Core Tarjetas	CRM	Originador
1	Operaciones	Gc Operaciones	Dir Banca Empresas	Director Banca Empresas	N/A	N/A	N/A	N/A	N/A
2	Operaciones	Gc Operaciones	Dir Banca Personas	Director Banca Personas	N/A	N/A	N/A	N/A	N/A
3	Operaciones	Gc Operaciones	Dir Banca Empresas	Analista I Banca Empresas	Legaliza	P80241-GC BCA Empresas Analista Legalizador	CO-CONSULTA	N/A	N/A
4	Operaciones	Gc Operaciones	Dir Banca Empresas	Analista I Banca Empresas	Desembolsos	P80242-GC BCA Empresas Analist Desembolso	RA-REALCE	N/A	N/A
5	Operaciones	Gc Operaciones	Dir Banca Personas	Analista I Banca Personas	Tarjetas	P80341-GC BCA Personas Analist Tarjetas	MT-MANTTO REALCE	Responsabilidad 1	Mtto_prod_Tarjeta
6	Operaciones	Gc Operaciones	Dir Banca Personas	Auxiliar II Banca Personas	Ciclo de Vida	P80352-GC BCA Personas Analist Ciclo De Vida	CO-CONSULTA	Responsabilidad 2	Consulta_prod_Tarjeta

Nota. La tabla muestra el acceso autorizado a las aplicaciones por cargo. Elaboración propia

7.6.5.4 Análisis de Trazabilidad y Registros de Auditoría. Se evalúa la capacidad de los sistemas Core para registrar, conservar y analizar eventos relacionados con el acceso a información sensible (PII y PCI), con el objetivo de detectar accesos indebidos, no autorizados o comportamientos anómalos.

Para ello, se realiza una entrevista con el equipo de Gestión de Vulnerabilidades de Seguridad del Banco, en la cual se solicita evidencia de los registros (logs) que son recibidos por el sistema de gestión de eventos e información de seguridad (SIEM) implementado en la entidad. La solicitud abarca los registros generados por las aplicaciones Core, servidores, bases de datos y sistemas de autenticación como Active Directory (AD), LDAP y IAM. Esta información es clave para evaluar la trazabilidad de los eventos relacionados con el acceso a información sensible (PII y PCI) y validar el cumplimiento de los controles establecidos por los estándares de seguridad aplicables. En los registros analizados se identifican eventos relevantes como accesos fuera del horario laboral, accesos desde ubicaciones inusuales, intentos reiterados o automatizados de acceso, y algunos accesos no autorizados a archivos o tablas de datos sensibles (PII y PCI).

Adicionalmente, se consulta el tiempo de conservación de dichos registros, confirmando que, de acuerdo con el estándar de registro y monitoreo de eventos, los logs se conservan por un periodo de 15 meses en línea y 36 meses en cinta, lo que permite garantizar la trazabilidad y disponibilidad de la información para fines de auditoría y análisis forense.

Como resultado, se presenta a continuación, en la tabla 12, una muestra representativa de los logs generados por las aplicaciones que manejan información PII y PCI, compartida por el equipo de Monitoreo de Seguridad, la cual permite validar la trazabilidad de los eventos y el cumplimiento de los controles establecidos por las normas ISO/IEC 27001:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014.

Tabla 12.

Muestra de logs generados

Aplicación	Usuario	Fecha/Hora del Acceso	Tipo de Acceso	Resultado del Acceso	Anomalía Detectada	Riesgo Asociado	Acción Recomendada	Responsable
Core Banco	CORGONZAGA	09/07/25/08:22:05	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Banco	CORRODRIJE	09/07/25/11:39:56	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Banco	CORAREVALO	09/07/25/14:02:21	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Banco	CORPAGDOJO	09/07/25/16:09:21	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Banco	CORSOSAMIL	09/07/25/09:09:21	User A escalated privileg	Access denied to / secure	User A escalated privileges to admin witho	Escalated privileges	Bloquear temporalmente la cuenta, revisar IP origen	Operación
Core Banco	CORMORASAN	09/07/25/11:10:02	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Banco	CORSIABAYO	09/07/25/12:28:02	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Banco	CORJIMENEF	09/07/25/15:56:29	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Banco	CORSUAREME	09/07/25/11:24:43	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Banco	CORTORRECE	09/07/25/17:01:43	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
CMR	GONZAGA	09/07/25/08:31:32	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
CMR	RODRIJE	09/07/25/11:48:03	Usr Z accessed file/date	Access successful for user	Accesed Usr Z file/date successful	Change file	Validar trazabilidad, revisar justificación, aplicar monitoreo reforzado	Operación
CMR	AREVALO	09/07/25/14:14:29	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
CMR	PAGDOJO	09/07/25/16:17:18	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
CMR	SOSAMIL	09/07/25/09:16:12	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
CMR	MORASAN	09/07/25/11:19:21	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
CMR	SIABAYO	09/07/25/14:34:26	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
CMR	JIMENEF	09/07/25/16:48:41	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
CMR	SUAREME	09/07/25/15:14:21	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
CMR	TORRECE	09/07/25/03:52:32	Access denied to resume	Access denied to /secure	User A accessed system at 03:52 AM from	Access denied	Generar alerta, validar legitimidad del usuario, revisar geolocalización	Operación
Originador	GONZAGA	09/07/25/08:43:24	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Originador	RODRIJE	09/07/25/11:54:11	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Originador	AREVALO	09/07/25/14:26:32	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación

Aplicación	Usuario	Fecha/Hora del Acceso	Tipo de Acceso	Resultado del Acceso	Anomalía Detectada	Riesgo Asociado	Acción Recomendada	Responsable
Originador	PAGDOJO	09/07/25/16:24:19	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Originador	SOSAMIL	09/07/25/09:24:34	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Originador	MORASAN	09/07/25/11:24:39	Usr Z accessed file/date	Accessed sucessfull for user	Accesed Usr Z file/date successful	Change file	Validar trazabilidad, revisar justificación, aplicar monitoreo reforzado	Operación
Originador	SIABAYO	09/07/25/14:34:26	Usr B accessed transac	Transac accessed for user	Transac successful	Change file	Validar trazabilidad, revisar justificación, aplicar monitoreo reforzado	Operación
Originador	JIMENEF	09/07/25/14:32:18	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Originador	SUAREME	09/07/25/16:41:12	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Originador	TORRECE	09/07/25/15:19:21	Usr T accessed file/date	Accessed sucessfull for user	Accesed Usr T file/date successful	Change file	Validar trazabilidad, revisar justificación, aplicar monitoreo reforzado	Operación
Core Tarjetas	GONZAGA	09/07/25/08:54:28	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Tarjetas	RODRIJE	09/07/25/12:03:16	Usr T accessed transac	Transac accessed for user	Transac successful	Change file	Validar trazabilidad, revisar justificación, aplicar monitoreo reforzado	Operación
Core Tarjetas	AREVALO	09/07/25/14:32:43	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Tarjetas	PAGDOJO	09/07/25/16:31:26	Usr P accessed file/date	Accessed sucessfull for user	Accesed Usr P file/date successful	Change file	Validar trazabilidad, revisar justificación, aplicar monitoreo reforzado	Operación
Core Tarjetas	SOSAMIL	09/07/25/09:31:59	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Tarjetas	MORASAN	09/07/25/11:28:52	Usr T accessed transac	Transac accessed for user	Transac successful	Change file	Validar trazabilidad, revisar justificación, aplicar monitoreo reforzado	Operación
Core Tarjetas	SIABAYO	09/07/25/16:42:41	Usr SN accessed file/date	Accessed sucessfull for user	Accesed Usr SN file/date successful	Change file	Validar trazabilidad, revisar justificación, aplicar monitoreo reforzado	Operación
Core Tarjetas	JIMENEF	09/07/25/16:34:29	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación
Core Tarjetas	SUAREME	09/07/25/11:24:21	Usr S accessed file/date	Accessed denied for user	Accesed Usr S file/date successful	Change file	Validar trazabilidad, revisar justificación, aplicar monitoreo reforzado	Operación
Core Tarjetas	TORRECE	09/07/25/16:32:12	User logged in success	Login successful for user	Correct login successful	Login user	Validar acceso y actividad	Operación

Nota. La tabla muestra los logs consolidados y registrados de las aplicaciones del alcance. Elaboración propia

7.6.6 Evaluación de Controles de Acceso Lógico en Aplicaciones Core.

Se analiza la eficacia, adecuación y alineación de los controles de acceso lógico implementados en las aplicaciones Core del Banco que procesan o almacenan información sensible, como datos personales identificables (PII) y datos de tarjetas de pago (PCI).

El objetivo de esta evaluación es verificar que los mecanismos de control implementados, incluyendo autenticación, autorización, segregación de funciones, y gestión de privilegios, estén correctamente definidos, operativos y alineados con los estándares establecidos por las normas ISO/IEC 27001:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014.

Esta revisión permite identificar posibles brechas de seguridad, accesos indebidos o configuraciones que puedan representar riesgos para la confidencialidad, integridad y disponibilidad de la información.

7.6.6.1 Evaluación normativa. Como parte del diagnóstico, se realiza una evaluación normativa con el objetivo de verificar el grado de alineación de los controles implementados en las aplicaciones evaluadas frente a los requisitos establecidos por los marcos regulatorios y estándares internacionales ISO/IEC 27001:2022, PCI DSS v4.0.1 y Circular Externa 029 de 2014 – Superintendencia Financiera de Colombia.

7.6.6.1.1 Lista de chequeo del cumplimiento normativo. Como parte de la valoración de riesgos y la evaluación normativa, se elaboran las listas de chequeo que permite verificar el cumplimiento de los controles de acceso lógico frente a los requisitos establecidos por los marcos regulatorios aplicables, incluyendo ISO/IEC 27001:2022 en la tabla 13, PCI DSS v4.0.1 en la tabla 14 y Circular Externa 029 de 2014 en la tabla 15.

Los rangos para la medición cuantitativa se estimaron de la siguiente forma:

- **No existe:** El control no está implementado ni cumple con los requisitos establecidos, **Porcentaje de 0%.**
- **Solo aplica a veces:** El control se utiliza de forma ocasional o informal, sin implementación formal, rango del **porcentaje del 1% a 39%.**
- **Si, pero no documentado:** El control está parcialmente implementado, pero carece de documentación formal, rango del **porcentaje del 40% al 69%.**
- **Definido y documentado:** El control está implementado y documentado, pero presenta deficiencias que generan riesgos, rango del **porcentaje del 70% a 89%.**
- **Medible:** El control está maduro, con métricas definidas que permiten evaluar su cumplimiento, rango del **porcentaje del 90% al 95%.**
- **Optimizado:** El control es eficaz, no genera riesgos identificados y es sostenible en el tiempo, rango del **porcentaje del 95% al 100%.**

Tabla 13.

ISO/IEC 27001:2022

			0	1	2	3	4	5					
Numero	**Control**	**Requisito**	**No existe**	**Solo se aplica aveces**	**Si, pero no documentado**	**Definido y documentado**	**medible**	**Optimizado**	**% Cumplimiento Actual**	**% Cumplimiento Esperado**	**Respuesta del cliente**	**Próximos pasos**	**Responsable**
5.1	Políticas de seguridad de la información	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?				X			81 %	> 95%	Existen políticas de seguridad publicadas desde octubre de 2023 con las que actualmente el Banco se rige y cumple.	Actualizar las políticas de seguridad a partir de la propuesta del presente proyecto.	CISO del Banco
5.2	Funciones y responsabilidades en materia de seguridad de la información	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?		X					40 %	> 95%	Se tiene definido algunos responsables de parte del negocio donde se tienen definidas las responsabilidades de aceptación como dueños de la información, pero no se encuentra en cumplimiento para todas las áreas de operaciones.	Se deben definir las responsabilidades para todas las áreas de negocio y en especial para el área de operaciones quienes acceden y manipulan la información de las aplicaciones Core del Banco para la operación diaria en la generación de reportes y tratamiento de la información.	Vicepresidentes de las áreas de negocio
5.3	Segregación de funciones	¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?		X					35%	> 90%	Se tiene identificado algunos responsables o dueños de la información, pero no se ha podido formalizar la aceptación de parte de los dueños que autoricen los accesos o el uso adecuado de la información.	Se requiere identificar y tener el soporte documentado de aceptación de los dueños de la información quienes sean los responsables de autorizar el acceso a los usuarios que requieren la información, en especial aquella información clasificada como crítica o sensible para la compañía.	Vicepresidentes de las áreas de negocio
5.4	Responsabilidades de la dirección	Direccion debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida				X			85%	> 95%	El Banco cuenta con un código de conducta donde exige el cumplimiento de las políticas de seguridad.	Se requiere campañas de sensibilización a los funcionarios de manera periódica, a partir de cursos de capacitación, que sean evaluados y certificados con los frentes que aborda la seguridad de la información, reconocer la importancia del compromiso y responsabilidad que tiene cada funcionario con el cumplimiento de estas políticas.	Junta Directiva / CISO del Banco
5.5	Contacto con las autoridades	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?			X				69%	> 95%	El Banco cuenta con un área de Gestión de Incidentes de ciberseguridad, con un plan de respuesta, pero no tiene definidas métricas que determine cantidad de eventos que pueda presentar en un periodo requerido.	Se requiere establecer un plan de tratamiento de incidentes gestionados en una bitácora de seguimiento que sea medible para poder tener estadísticamente la cantidad de eventos presentados en un periodo ante las autoridades competentes.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad
5.6	Contacto con grupos de interés especial	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas				X			89%	> 95%	Se tiene definido un comité de incidentes de ciberseguridad en conjunto con los organismos de control como la POLICIA	Se requiere madurar y documentar el proceso de gestión de incidentes de fuga de información, apoyado de los	CISO del Banco / Equipo de gestión de

			0	1	2	3	4	5					
Numero	**Control**	**Requisito**	**No existe**	**Solo se aplica aveces**	**Si, pero no documentado**	**Definido y documentado**	**medible**	**Optimizado**	**% Cumplimiento Actual**	**% Cumplimiento Esperado**	**Respuesta del cliente**	**Próximos pasos**	**Responsable**
		con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?									NACIONAL y ASOBANCARIA para realizar seguimiento de eventos presentados y definición de medidas a tomar para mitigar nuevos eventos o reincidencias de estos.	organismos de control y vigilancia.	incidentes de ciberseguridad
5.7	Inteligencia de amenazas	¿Se tiene definido un mecanismo para recopilar y analizar estas amenazas y determinar las acciones adecuadas que se pueden tomar para proteger la seguridad de su información?		X					39%	> 90%	El Banco cuenta con mecanismos de recopilación de eventos de seguridad, y seguimiento de alertas de estos.	Se debe automatizar el proceso de alertas y notificaciones de justificación de posibles incidentes de seguridad o falsos positivos para minimizar la manualidad del proceso.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad
5.8	Seguridad de la información en la gestión de proyectos	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?			X				65%	> 95%	El Banco cuenta con un área de Gobierno y Consultoría de seguridad quienes realizan el acompañamiento a los proyectos siendo apoyo y guía de las necesidades requeridas para el cumplimiento de los controles e identificación de riesgos en la implementación de los proyectos.	Se debe mantener el acompañamiento en los proyectos e iniciativas, actualizar la documentación para el tratamiento de información PII y PCI donde aplique y tener una sinergia con las demás áreas de seguridad para alinear los controles de seguridad sobre esta información.	CISO del Banco / Equipo de Gobierno y Consultoría
5.9	Inventario de la información y otros activos asociados	¿Se ha realizado un inventario de activos que dan soporte al negocio y de Información y se ha identificado al responsable de cada activo en cuanto a su seguridad?			X				61%	> 95%	Se tiene una línea base de activos de información general que se tiene en el Banco, pero no se tiene actualizado.	Se debe actualizar y mantener actualizado el inventario de activos de información, así como generar el inventario de archivos críticos que contienen información PII y PCI para poder consultar y adicionar archivos que sean identificados en los nuevos proyectos.	CISO del Banco / Equipo de Gobierno y Consultoría
5.10	Uso aceptable de la información y otros activos asociados	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad definido procedimientos para el manipulado de la información de acuerdo con su clasificación?			X				65%	> 90%	Se tienen identificados algunos responsables desde las áreas de negocio, pero no se tiene en su totalidad identificadas las áreas de operaciones quienes consumen información a demanda de acuerdo con sus funciones.	Se debe identificar la totalidad de los responsables de la información por parte de las áres de negocio, en especial el área de operaciones quienes representan la mayoría de los accesos a información crítica o sensible para la generación de reportes y operaciones transversales en el Back office.	Equipo de Gobierno y Consultoría/ Líderes de las áreas de negocio.
5.11	Devolución de activos	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?				X			85%	> 95%	Se cuenta con un procedimiento establecido operada por un laboratorio con técnicos capacitados para la entrega y recepción de estaciones de trabajo, quienes realizan las respectivas configuraciones para la entrega o el borrado seguro en la recepción de los activos que devuelven los funcionarios de	Se debe mantener y reforzar el inventario de activos manteniendo el control de las estaciones de trabajo que son entregadas a los funcionarios o son devueltos al finalizar la vinculación se directa con la compañía o por terceros, garantizando el borrado seguro para la reasignación de equipos a un nuevo	Gerencia de Operaciones TI

			0	1	2	3	4	5					
Numero	**Control**	**Requisito**	**No existe**	**Solo se aplica aveces**	**Si, pero no documentado**	**Definido y documentado**	**medible**	**Optimizado**	**% Cumplimiento Actual**	**% Cumplimiento Esperado**	**Respuesta del cliente**	**Próximos pasos**	**Responsable**
											planta o contratistas.	funcionario.	
5.12	Clasificación de la información	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?				X			85%	> 95%	Existe un Estándar de Clasificación de seguridad de la información y los sistemas publicadas desde diciembre de 2023 con las que actualmente el Banco se rige y cumple.	Actualizar el estándar de Clasificación de seguridad a partir de la propuesta del presente proyecto.	CISO del Banco / Equipo de Gobierno y Consultoría
5.14	Transferencia de información	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?			X				66%	> 95%	El Banco cuenta con políticas y procedimientos para el intercambio de información segura, pero se desconoce por parte de las áreas de negocio.	Se debe reforzar a los funcionarios del Banco la existencia de estas políticas y procedimientos mediante capacitaciones y comunicados frecuentes que informen la importancia del uso y la seguridad que se debe aplicar al momento del intercambio de información.	CISO del Banco / Equipo de Gobierno y Consultoría / Áreas de Negocio
5.15	Control de acceso	¿Existe una política para definir los controles de acceso fisico y logico a la información y sus activos asociados, según las necesidades de cada actividad o puesto de trabajo?				X			85%	> 95%	Existe un estándar de Gestión de Identidades y Acceso de seguridad de la información actualizado a marzo de 2025 con el que actualmente el Banco se rige y cumple.	Se debe actualizar el estándar cada vez que se realice un cambio a los lineamientos y políticas de seguridad, en este caso se hace necesario en el momento que sea aplicada la presente propuesta y dar a conocer a todo el Banco.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Control de Acceso / Áreas de Negocio
5.16	Gestión de la identidad	¿Existen procesos formales de registros de usuarios?				X			85%	> 95%	Existe el manual de procesamiento de gestión de identidades en donde se describe los flujos y procesos en las aplicaciones.	Se debe actualizar el Manual cada vez que se realice un cambio de los procesos de Gestión de identidades, en este caso se hace necesario en el momento que sea aplicada la presente propuesta y dar a conocer a todo el Banco.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Control de Acceso / Áreas de Negocio
5.17	Información de autenticación	¿Se ha establecido una política específica para: - manejo de información clasificada como secreta - creación de contraseñas seguras y salvaguarda de estas				X			87%	> 95%	Existe un Estandar de Clasificación de seguridad de la información y los sistemas publicadas desde diciembre de 2023 con las que actualmente el Banco se rige	Actualizar el Estandar de Clasificación de seguridad a partir de la propuesta del presente proyecto.	CISO del Banco / Equipo de Gobierno y Consultoría
5.18	Derechos de acceso	¿Existen procesos formales para asignación de perfiles de acceso? - se establecen periodos concretos para renovación de permisos de acceso? - revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?				X			89%	> 95%	Existe el manual de procesamiento de gestión de identidades en donde se describe los flujos y procesos en las aplicaciones (Creación, Modificación, Eliminación)	Se debe actualizar el Manual cada vez que se realice un cambio de los procesos de Gestión de identidades, en este caso se hace necesario en el momento que sea aplicada la presente propuesta y dar a conocer a todo el Banco.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Control de Acceso / Áreas de Negocio
5.24	Planificación y preparación de la gestión de	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la				X			86%	> 95%	El Banco cuenta con un área de Gestión de Incidentes de ciberseguridad, con un proceso definido de acuerdo con el	Se requiere establecer un plan de tratamiento de incidentes generados por una fuga de información, escalamiento	CISO del Banco / Equipo de gestión de

			0	1	2	3	4	5					
Numero	**Control**	**Requisito**	**No existe**	**Solo se aplica aveces**	**Si, pero no documentado**	**Definido y documentado**	**medible**	**Optimizado**	**% Cumplimiento Actual**	**% Cumplimiento Esperado**	**Respuesta del cliente**	**Próximos pasos**	**Responsable**
	incidentes de seguridad de la información	Información?									escalamiento requerido de acuerdo al nivel de criticidad del incidente presentado.	y responsables claramente identificados.	incidentes de ciberseguridad / Áreas de Negocio
5.25	Evaluación y decisión sobre eventos de seguridad de la información	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?				X			89%	> 95%	El Banco cuenta con un área de Gestión de Incidentes de ciberseguridad, con un proceso definido de acuerdo al escalamiento requerido de acuerdo con el nivel de criticidad del incidente presentado.	Se requiere establecer un plan de tratamiento de incidentes generados por una fuga de información, escalamiento y responsables claramente identificados.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Áreas de Negocio
5.26	Respuesta a incidentes de seguridad de la información	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?				X			87%	> 95%	El equipo de ciberseguridad cuenta con herramientas y procesos definidos para el escalmiento y respuesta a incidentes de seguridad, de igual forma cuentan con el apoyo del área de Seguridad Corporativa para el apoyo forense en caso de requerirlo.	Se debe incluir en el proceso de respuesta a incidentes el incidente de fuga de información.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Seguridad Corporativa / Áreas de Negocio
5.27	Aprendizaje de los incidentes de seguridad de la información	¿La información que proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas?			X				69%	> 95%	Se tiene definido en el Banco un comité de atención a incidentes que incluye el proceso de lecciones aprendidas y solución a problemas identificados con el fin de poder actuar en el momento que sea requerido.	Se debe incluir en el proceso de atención a problemas identificados o lecciones aprendidas los incidentes que sean de tipo fuga de información.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Seguridad Corporativa / Áreas de Negocio
5.28	Recogida de pruebas	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?			X				66%	> 95%	El equipo de ciberseguridad cuenta con herramientas y procesos definidos para la identificación y recogida de pruebas de los incidentes de seguridad presentados con el apoyo del área de Seguridad Corporativa para el acompañamiento forense y utilizar la cadena de custodia de evidencias y recogida de pruebas en caso de ser requerido para el cumplimiento de No repudio.	Se debe incluir en el proceso de toma de evidencia y recogida de pruebas los incidentes que sean de tipo fuga de información.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Seguridad Corporativa
5.29	Seguridad de la información durante la interrupción	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información? ¿Se ha implementado las medidas			X				69%	> 95%	El Banco cuenta con un BRP (Bussines Recovery Plan) ante incidentes de seguridad, con toma de Backups de las aplicaciones programados periódicamente (Semanal, Mensual, Anual) incremental	Se debe actualizar el BRP donde se incluya planes de acción en caso de presentarse un incidente por fuga de información	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad /

			0	1	2	3	4	5					
Numero	**Control**	**Requisito**	**No existe**	**Solo se aplica aveces**	**Si, pero no documentado**	**Definido y documentado**	**medible**	**Optimizado**	**% Cumplimiento Actual**	**% Cumplimiento Esperado**	**Respuesta del cliente**	**Próximos pasos**	**Responsable**
		de recuperación previstas en el plan de Continuidad del Negocio? ¿Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio?									con el fin de ser utilizada o accedida en el momento que sea requerida, de igual forma se ha probado de forma satisfactoria en las pruebas controladas.		Equipo de BRM
5.31	Identificación de los requisitos legales, reglamentarios y contractuales	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento? -Ley general de Telecomunicaciones -Leyes para comercio Electrónico -Transacciones Bancarias -Información Protegida -Otras propias del negocio o actividad ¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?				X			84%	> 95%	El Banco se rige por los lineamientos y requisitos legales de los entes reguladores locales y regionales, mediante las circulares que son publicadas por la Superintendencia Financiera de Colombia, las normas PCI DSS e ISO, con el fin de proteger la información de los clientes.	Se debe definir nuevos controles de acceso sobre los archivos que almacenan información PII y PCI con el fin de protegerlos ante un riesgo de una posible fuga de información.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Seguridad Técnica / Áreas de Negocio
5.33	Protección de registros	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?		X					37%	> 90%	Existe un estándar de Clasificación de seguridad de la información y los sistemas publicadas desde diciembre de 2023 con las que actualmente el Banco se rige y cumple.	Actualizar el estándar de Clasificación de seguridad a partir de la propuesta del presente proyecto.	CISO del Banco / Equipo de Gobierno y Consultoría
5.34	Privacidad y protección de la información personal	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?				X			86%	> 95%	El Banco cuenta con algunos controles para la protección de Datos en cumplimiento con las normativas y circulares de la Superintendencia Financiera de Colombia, las normas PCI DSS e ISO, con el fin de proteger la información de los clientes.	Se debe definir nuevos controles de acceso sobre los archivos que almacenan información PII y PCI con el fin de protegerlos ante un riesgo de una posible fuga de información.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Seguridad Técnica / Áreas de Negocio
5.35	Revisión independiente de la seguridad de la información	¿Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles?			X				68%	> 95%	Si, se aplican controles a los usuarios de áreas operativas y controles a los administradores de seguridad de parte de Control de Acceso.	Se debe mantener esta diferenciación de autorizaciones especiales por tener perfil administrador de seguridad con los de las áreas operativas, esto a partir de cláusulas de confidencialidad y manejo y confianza, ya que los administradores de seguridad cuentan con cuentas privilegiadas y debe estar documentado en los procesos y manuales en cumplimiento con las políticas de seguridad.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Control de Acceso / Áreas de Negocio

			0	1	2	3	4	5					
Numero	**Control**	**Requisito**	**No existe**	**Solo se aplica aveces**	**Si, pero no documentado**	**Definido y documentado**	**medible**	**Optimizado**	**% Cumplimiento Actual**	**% Cumplimiento Esperado**	**Respuesta del cliente**	**Próximos pasos**	**Responsable**
5.36	Cumplimiento de políticas y normas de seguridad de la información	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información? ¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?				X			88%	> 95%	El área de Gobierno y Consultoría en conjunto con los demás equipos de Seguridad realizan certificaciones periodicas sobre políticas y controles de la seguridad de la información para las áreas del Banco.	Se debe mantener las certificaciones de acceso periódico y actualizaer el cronograma de certificación que es acompañado por el equipo de Auditoría interna y externa para la evaluación de los controles estén vigentes y en cumplimiento.	CISO del Banco / Equipos de seguridad del Banco / Auditoría
5.37	Procedimientos operativos documentados	¿Se documentan los procedimientos y se establecen responsabilidades?			X				67%	> 95%	El Banco tiene procedimientos documentados con los cuales se guía para el cumplimiento de la operación correcta.	Se debe mantener actualizado los procedimientos cada vez que se presente un cambio a estos, manuales y darlos a conocer a los equipos involucrados y requeridos para ser socializados y aplicados.	CISO del Banco / Equipos de seguridad del Banco / Auditoría
8.2	Derechos de acceso con privilegios	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?				X			**82%**	**> 95%**	Se tiene un proceso definido para la asignación de permisos a nivel de roles y perfiles, pero no se tiene definido para el acceso a los archivos críticos que actualmente utiliza el área de negocio mediante consultas directas desde herramientas externas a la aplicación.	Se debe definir el proceso de autorización de acceso a los archivos críticos por parte de las áreas de negocio, partiendo de la identificación de archivos críticos, de los usuarios que acceden los mismos e identificación de los responsables de la información, así como los controles que se requieren para la prevención de fuga de información.	CISO del Banco / Equipos de seguridad del Banco / Áreas de negocio
8.3	Restricción de acceso a la información	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?				X			**86%**	**> 95%**	Se establecen permisos a nivel de roles y perfiles, pero no se tiene definido para el acceso a los archivos críticos que actualmente utiliza el área de negocio mediante consultas directas desde herramientas externas a la aplicación.	Se debe establecer niveles de autorización de acceso a los archivos críticos por parte de las áreas de negocio, partiendo de la identificación de archivos críticos, de los usuarios que acceden los mismos e identificación de los responsables de la información, así como los controles que se requieren para la prevención de fuga de información con monitoreo y trazabilidad del uso de la información.	CISO del Banco / Equipos de seguridad del Banco / Áreas de negocio

Nota. La tabla muestra el GAP sobre cada uno de los controles asociados a la norma y evaluados para el alcance del proyecto.

Elaboración propia

Tabla 14.

PCI DSS v4.0.1

Número de Cláusula	Descripción del Control	No existe	Solo se aplica aveces	Si, pero no documentado	Definido y documentado	medible	Optimizado	% Cumplimiento Actual	% Cumplimiento Esperado	Respuesta del cliente	Próximos pasos	Responsable
2.2	Los componentes del sistema se configuran y administran de forma segura.			X				68%	>95%	Si, se aplican controles a los usuarios de áreas operativas y controles a los administradores de seguridad de parte de Control de Acceso.	Se debe mantener esta diferenciación de autorizaciones especiales por tener perfil administrador de seguridad con los de las áreas operativas, esto a partir de cláusulas de confidencialidad y manejo y confianza, ya que los administradores de seguridad cuentan con cuentas privilegiadas y debe estar documentado en los procesos y manuales en cumplimiento con las políticas de seguridad.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Control de Acceso / Áreas de Negocio
3.1	Se definen y comprenden los procesos y los mecanismos para proteger los datos del titular de la tarjeta almacenados.			X				69%	>95%	El Banco cuenta con un área de Gobierno y Consultoría de seguridad quienes realizan el acompañamiento a los proyectos siendo apoyo y guia de las necesidades requeridas para el cumplimiento de los controles e identificación de riesgos en la implementación de los proyectos.	Se debe mantener el acompañamiento en los proyectos e iniciativas, actualizar la documentación para el tratamiento de información PII y PCI donde aplique y tener una sinergia con las demás áreas de seguridad para alinear los controles de seguridad sobre esta información.	CISO del Banco / Equipo de Gobierno y Consultoría
3.3	Los datos de autenticación sensibles (SAD) no se almacenan después de su autorización.				X			89%	>95%	Existe un estándar de Clasificación de seguridad de la información y los sistemas publicadas desde diciembre de 2023 con las que actualmente el Banco se rige y cumple.	Actualizar el estándar de Clasificación de seguridad a partir de la propuesta del presente proyecto.	CISO del Banco / Equipo de Gobierno y Consultoría
3.7	Cuando se utiliza la criptografía para proteger los datos del titular de la tarjeta almacenados se definen e implementan procesos y procedimientos de gestión de claves que cubren todos los aspectos del ciclo de vida de estas.				X			89%	>95%	Existe un estándar de Clasificación de seguridad de la información y los sistemas publicadas desde diciembre de 2023 con las que actualmente el Banco se rige y cumple.	Actualizar el estándar de Clasificación de seguridad a partir de la propuesta del presente proyecto.	CISO del Banco / Equipo de Gobierno y Consultoría

Nota. La tabla muestra el GAP sobre cada uno de los controles asociados a la norma y evaluados para el alcance del proyecto.

Tabla 15.

Circular Externa 029 de 2014

Número de Cláusula	Descripción del Control	No existe	Solo se aplica a veces	Si, pero no documentado	Definido y documentado	medible	Optimizado	% Cumplimiento Actual	% Cumplimiento Esperado	Respuesta del cliente	Próximos pasos	Responsable
3.1.1	Ser aprobada por la junta directiva				X			89%	>95 %	Existen políticas de seguridad publicadas desde octubre de 2023 con las que actualmente el Banco se rige y cumple.	Actualizar las políticas de seguridad a partir de la propuesta del presente proyecto.	CISO del Banco
3.1.2	Documentar las responsabilidades, procesos, procedimientos, etapas y la gestión que se realiza frente a la ciberseguridad		X					38%	>95 %	Se tiene definido algunos responsables de parte del negocio donde se tienen definidas las responsabilidades de aceptación como dueños de la información, pero no se encuentra en cumplimiento para todas las áreas de operaciones.	Se deben definir las responsabilidades para todas las áreas de negocio y en especial para el área de operaciones quienes acceden y manipulan la información de las aplicaciones Core del Banco para la operación diaria en la generación de reportes y tratamiento de la información.	Vicepresidentes de las áreas de negocio
3.1.3	Establecer las funciones de la unidad de seguridad de la información y la ciberseguridad		X					39%	>95 %	Se tiene identificado algunos responsables o dueños de la información, pero no se ha podido formalizar la aceptación de parte de los dueños que autoricen los accesos o el uso adecuado de la información.	Se requiere identificar y tener el soporte documentado de aceptación de los dueños de la información quienes sean los responsables de autorizar el acceso a los usuarios que requieren la información, en especial aquella información clasificada como crítica o sensible para la compañía.	Vicepresidentes de las áreas de negocio
3.2.1	Se debe conformar considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados por la entidad.			X				69%	>95 %	El Banco cuenta con mecanismos de recopilación de eventos de seguridad, y seguimiento de alertas de estos. El Banco cuenta con un área de Gestión de Incidentes de ciberseguridad, con un plan de respuesta, pero no tiene definida métricas que determine cantidad de	Se debe automatizar el proceso de alertas y notificaciones de justificación de posibles incidentes de seguridad o falsos positivos para minimizar la manualidad del proceso. Se requiere establecer un plan de tratamiento de incidentes	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad

						eventos que pueda presentar en un periodo requerido.	gestionados en una bitácora de seguimiento que sea medible para poder tener estadísticamente la cantidad de eventos presentados en un periodo ante las autoridades competentes.	
3.2.2	Debe realizar una gestión efectiva de la seguridad de la información y la ciberseguridad en la entidad.	X			39%	>95 %	El Banco cuenta con un área de Gobierno y Consultoría de seguridad quienes realizan el acompañamiento a los proyectos siendo apoyo y guia de las necesidades requeridas para el cumplimiento de los controles e identificación de riesgos en la implementación de los proyectos.	Se debe mantener el acompañamiento en los proyectos e iniciativas, actualizar la documentación para el tratamiento de información PII y PCI donde aplique y tener una sinergia con las demás áreas de seguridad para alinear los controles de seguridad sobre esta información.	CISO del Banco / Equipo de Gobierno y Consultoría
3.2.3	Debe reportar a la junta directiva y a la alta dirección, los resultados de su gestión, especialmente en la evaluación que haga de la confidencialidad, integridad y disponibilidad de la información, identificación de ciberamenazas, resultados de la evaluación de efectividad de los programas de ciberseguridad, propuestas de mejora en materia de ciberseguridad y resumen de los incidentes de ciberseguridad que afectaron la entidad. La periodicidad de los reportes debe ser, al menos, semestralmente.		X		89%	>95 %	El Banco cuenta con un código de conducta donde exige el cumplimiento de las políticas de seguridad.	Se requiere campañas de sensibilización a los funcionarios de manera periódica, a partir de cursos de capacitación, que sean evaluados y certificados con los frentes que aborda la seguridad de la información, reconocer la importancia del compromiso y responsabilidad que tiene cada funcionario con el cumplimiento de estas políticas.	Junta Directiva / CISO del Banco
3.2.5	Debe sugerir las capacitaciones que deben recibir regularmente los funcionarios de la entidad en temas relacionados con ciberseguridad y mantenerlos actualizados sobre las nuevas ciberamenazas.		X		66%	>95 %	Se tiene definido en el Banco un comité de atención a incidentes que incluye el proceso de lecciones aprendidas y solución a problemas identificados con el fin de poder actuar en el momento que sea requerido.	Se debe incluir en el proceso de atención a problemas identificados o lecciones aprendidas los incidentes que sean de tipo fuga de información.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Seguridad Corporativa / Áreas de Negocio
3.2.6	Ser la principal responsable en el monitoreo y verificación del cumplimiento de las políticas y procedimientos que se establezcan en materia de ciberseguridad, sin perjuicio a aquellas tareas que realiza la auditoría interna.		X		89%	>95 %	El área de Gobierno y Consultoría en conjunto con los demás equipos de Seguridad realizan certificaciones periódicas sobre políticas y controles de la seguridad de la información para las áreas del Banco.	Se debe mantener las certificaciones de acceso periódico y actualizar el cronograma de certificación que es acompañado por el equipo de Auditoría interna y externa para la evaluación de los controles estén vigentes y en cumplimiento.	CISO del Banco / Equipos de seguridad del Banco / Auditoría
3.2.8	Realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un SOC, que puede ser manejado desde el exterior. El análisis debe identificar las características del proveedor y herramientas y servicios que se contratarán.		X		69%	>95 %	El Banco cuenta con un área de Gestión de Incidentes de ciberseguridad, con un plan de respuesta, pero no tiene definida métricas que determine cantidad de eventos que pueda presentar en un periodo requerido.	Se requiere establecer un plan de tratamiento de incidentes gestionados en una bitácora de seguimiento que sea medible para poder tener estadísticamente la cantidad de eventos presentados en un periodo ante las autoridades competentes.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad

3.2.11	Debe realizar las demás actividades establecidas en este Capítulo que por su naturaleza les sean asignadas. Sin perjuicio de las funciones que debe realizar la unidad de la que trata este subnumeral 3.2., las funciones de gestión de riesgos relacionadas con respuesta a incidentes pueden ser desagregadas en diferentes áreas de la entidad.		X		68%	>95 %	El equipo de ciberseguridad cuenta con herramientas y procesos definidos para la identificación y recogida de pruebas de los incidentes de seguridad presentados con el apoyo del área de Seguridad Corporativa para el acompañamiento forense y utilizar la cadena de custodia de evidencias y recogida de pruebas en caso de ser requerido para el cumplimiento de No repudio.	Se debe incluir en el proceso de toma de evidencia y recogida de pruebas los incidentes que sean de tipo fuga de información.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Seguridad Corporativa
3.3	Contar con un sistema de gestión para la ciberseguridad, para lo cual se pueden tomar como referencia el estándar ISO 27032, NIST con sus publicaciones SP800 y SP1800, ISF (Information Security Forum), CIS Critical Security Controls (CSC) o Cobit 5 for Information Security, y sus respectivas actualizaciones.		X		69%	>95 %	El Banco cuenta con un área de Gobierno y Consultoría de seguridad quienes realizan el acompañamiento a los proyectos siendo apoyo y guia de las necesidades requeridas para el cumplimiento de los controles e identificación de riesgos en la implementación de los proyectos.	Se debe mantener el acompañamiento en los proyectos e iniciativas, actualizar la documentación para el tratamiento de información PII y PCI donde aplique y tener una sinergia con las demás áreas de seguridad para alinear los controles de seguridad sobre esta información.	CISO del Banco / Equipo de Gobierno y Consultoría
3.4	Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito.		X		66%	>95 %	El Banco cuenta con politicas y procedimientos para el intercambio de información segura, pero se desconoce por parte de las áreas de negocio.	Se debe reforzar a los funcionarios del Banco la existencia de estas políticas y procedimientos mediante capacitaciones y comunicados frecuentes que informen la importancia del uso y la seguridad que se debe aplicar al momento del intercambio de información.	CISO del Banco / Equipo de Gobierno y Consultoría / Áreas de Negocio
3.5	Emplear mecanismos para la adecuada autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información.		X		69%	>95 %	Si, se aplican controles a los usuarios de áreas operativas y controles a los administradores de seguridad de parte de Control de Acceso.	Se debe mantener esta diferenciación de autorizaciones especiales por tener perfil administrador de seguridad con los de las áreas operativas, esto a partir de cláusulas de confidencialidad y manejo y confianza, ya que los administradores de seguridad cuentan con cuentas privilegiadas y debe estar documentado en los procesos y manuales en cumplimiento con las políticas de seguridad.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Control de Acceso / Áreas de Negocio
3.7.1	Información que reportará a la SFC, sobre incidentes de ciberseguridad que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información de la entidad, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlo.	X			38%	>95 %	El Banco cuenta con mecanismos de recopilación de eventos de seguridad, y seguimiento de alertas de los mismos.	Se debe automatizar el proceso de alertas y notificaciones de justificación de posibles incidentes de seguridad o falsos positivos para minimizar la manualidad del proceso.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad
3.7.2	Información que reportará a las			X	87%	>95	Se tiene definido un comité de	Se requiere madurar y documentar	CISO del Banco / Equipo de

	autoridades que hacen parte del modelo nacional de gestión de incidentes cibernéticos, sobre incidentes cibernéticos.				%	incidentes de ciberseguridad en conjunto con los organismos de control como la POLICIA NACIONAL y ASOBANCARIA para realizar seguimiento de eventos presentados y definición de medidas a tomar para mitigar nuevos eventos o reincidencias	el proceso de gestión de incidentes de fuga de información, apoyado de los organismos de control y vigilancia.	gestión de incidentes de ciberseguridad
3.12	Gestionar la seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.	X		69%	>95 %	El Banco cuenta con un área de Gobierno y Consultoría de seguridad quienes realizan el acompañamiento a los proyectos siendo apoyo y guía de las necesidades requeridas para el cumplimiento de los controles e identificación de riesgos en la implementación de los proyectos.	Se debe mantener el acompañamiento en los proyectos e iniciativas, actualizar la documentación para el tratamiento de información PII y PCI donde aplique y tener una sinergia con las demás áreas de seguridad para alinear los controles de seguridad sobre esta información.	CISO del Banco / Equipo de Gobierno y Consultoría
4.1.1	Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades bajo la premisa que las personas solo pueden disponer de los recursos que demande su trabajo, durante el tiempo que ello sea necesario.		x	89%	>95 %	Existe el manual de procesamiento de gestión de identidades en donde se describe los flujos y procesos en las aplicaciones (Creación, Modificación, Eliminación, Certificación).	Se debe actualizar el Manual cada vez que se realice un cambio de los procesos de Gestión de identidades, en este caso se hace necesario en el momento que sea aplicada la presente propuesta y dar a conocer a todo el Banco.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Control de Acceso / Áreas de Negocio
4.1.3	Gestionar y documentar la seguridad de la plataforma tecnológica.	X		62%	>95 %	El Banco cuenta con un área de Gobierno y Consultoría de seguridad quienes realizan el acompañamiento a los proyectos siendo apoyo y guia de las necesidades requeridas para el cumplimiento de los controles e identificación de riesgos en la implementación de los proyectos.	Se debe mantener el acompañamiento en los proyectos e iniciativas, actualizar la documentación para el tratamiento de información PII y PCI donde aplique y tener una sinergia con las demás áreas de seguridad para alinear los controles de seguridad sobre esta información.	CISO del Banco / Equipo de Gobierno y Consultoría
4.1.6	Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.	X		65%	>95 %	El Banco cuenta con un BRP (Bussines Recovery Plan) ante incidentes de seguridad, con toma de Backups de las aplicaciones programados periodicamente (Semanal, Mensual, Anual) incremental con el fin de ser utilizada o accedida en el momento que sea requerida, de igual forma se ha probado de forma satisfactoria en las pruebas controladas.	Se debe actualizar el BRP donde se incluya planes de acción en caso de presentarse un icnidente por fuga de información	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Equipo de BRM
4.1.8	Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, tal como un SIEM.		X	83%	>95 %	El equipo de ciberseguridad cuenta con herramientas y procesos definidos para el escalmiento y respuesta a incidentes de seguridad, de igual forma cuentan con el apoyo del área de Seguridad Corporativa para el apoyo forense en caso de requerirlo.	Se debe incluir en el proceso de respuesta a incidentes el incidente de fuga de información.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Seguridad Corporativa / Áreas de Negocio
4.1.9	De acuerdo con la estructura, canales de atención, volumen transaccional y número de		X	85%	>95 %	El Banco cuenta con un área de Gestión de Incidentes de ciberseguridad, con un proceso	Se requiere establecer un plan de tratamiento de incidentes generados por una fuga de información,	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Áreas de

	clientes, monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad.					definido de acuerdo con el escalamiento requerido de acuerdo con el nivel de criticidad del incidente presentado.	escalamiento y responsables claramente identificados.	Negocio
4.1.10	Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad en el sector financiero y a nivel nacional.		X	88%	>95 %	El Banco se rige por los lineamientos y requisitos legales de los entes reguladores locales y regionales, mediante las circulares que son publicadas por la Superintendencia Financiera de Colombia, las normas PCI DSS e ISO, con el fin de proteger la información de los clientes.	Se debe definir nuevos controles de acceso sobre los archivos que almacenan información PII y PCI con el fin de protegerlos ante un riesgo de una posible fuga de información.	CISO del Banco / Equipo de Gobierno y Consultoría / Equipo de Seguridad Técnica / Áreas de Negocio
4.2.1	Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten.		X	84%	>95 %	El Banco cuenta con un área de Gestión de Incidentes de ciberseguridad, con un proceso definido de acuerdo con el escalamiento requerido de acuerdo con el nivel de criticidad del incidente presentado.	Se requiere establecer un plan de tratamiento de incidentes generados por una fuga de información, escalamiento y responsables claramente identificados.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Áreas de Negocio
4.3.3	Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, directamente o a través de CSIRT sectoriales, los ataques cibernéticos que requieran de su gestión.		X	86%	>95 %	Se tiene definido un comité de incidentes de ciberseguridad en conjunto con los organismos de control como la Policia Nacional y Asobancaria para realizar seguimiento de eventos presentados y definición de medidas a tomar para mitigar nuevos eventos o reincidencias esto	Se requiere madurar y documentar el proceso de gestión de incidentes de fuga de información, apoyado de los organismos de control y vigilancia.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad
4.4.2	Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades de su sector.	X		63%	>95 %	Se tiene definido en el Banco un comité de atención a incidentes que incluye el proceso de lecciones aprendidas y solución a problemas identificados con el fin de poder actuar en el momento que sea requerido.	Se debe incluir en el proceso de atención a problemas identificados o lecciones aprendidas los incidentes que sean de tipo fuga de información.	CISO del Banco / Equipo de gestión de incidentes de ciberseguridad / Seguridad Corporativa / Áreas de Negocio

Nota. La tabla muestra el GAP sobre cada uno de los controles asociados a la norma y evaluados para el alcance del proyecto.

7.6.6.2 Identificación de Brechas frente a Estándares Internacionales. Como parte del diagnóstico de controles de acceso lógico, se realiza un análisis comparativo entre los controles implementados en las aplicaciones evaluadas y los requisitos establecidos por los estándares internacionales de seguridad de la información, específicamente:

ISO/IEC 27001:2022 – En lo relacionado con el control de accesos, gestión de identidades, revisión de privilegios y segregación de funciones.

PCI DSS v4.0.1 – En lo referente a la protección de datos de tarjetas, control de accesos lógicos, autenticación robusta y monitoreo de accesos.

Circular Externa 029 de 2014 – En cuanto a la gestión de usuarios, perfiles, trazabilidad y revisión periódica de accesos en entidades vigiladas por la Superintendencia Financiera de Colombia.

Durante este análisis, se identifican **brechas y desviaciones** que evidencian oportunidades de mejora en la implementación actual, tales como:

- Ausencia de revisiones periódicas documentadas de accesos.
- Perfiles con privilegios excesivos o funciones incompatibles.
- Documentación desactualizada o no alineada con los estándares vigentes.
- Falta de trazabilidad en la asignación y modificación de accesos.

Estas brechas se documentan en la siguiente **matriz de brechas**, la cual incluye el control esperado según el estándar, la situación actual observada, la brecha identificada y las recomendaciones correspondientes para su cierre (Ver tabla 16)

Tabla 16.

Matriz de brechas

Estándar	Control/Requisito	Brecha Identificada	Riesgo Asociado	Recomendación	Prioridad
ISO/IEC 27001:2022	A.5.15 - Gestión de acceso a la información	No existe revisión periódica de accesos a sistemas con información PII o PCI	Accesos no autorizados persistentes	Se debe actualizar el Estándar cada vez que se realice un cambio a los lineamientos y políticas de seguridad, en este caso se hace necesario en el momento que sea aplicada la presente propuesta y dar a conocer a todo el Banco.	Alta
ISO/IEC 27001:2022	A.5.16 - Gestión de identidades	Cuentas con roles desactualizados y con opciones que ya no utiliza el funcionario.	Escalada de privilegios Persistencia de cuentas obsoletas	Se debe actualizar el Manual cada vez que se realice un cambio de los procesos de Gestión de identidades, en este caso se hace necesario en el momento que sea aplicada la presente propuesta y dar a conocer a todo el Banco.	Alta
ISO/IEC 27001:2022	A.5.17 - Gestión de credenciales de autenticación	Cuentas Huérfanas, Contraseñas débiles y sin política de expiración	Compromiso de credenciales	Implementar procesos de bajas y monitoreo a usuarios huérfanos. Aplicar políticas de contraseñas robustas y rotación periódica. Actualizar el Estándar de Clasificación de seguridad a partir de la propuesta del presente proyecto.	Alta
ISO/IEC 27001:2022	A.5.18 - Gestión de usuarios y perfiles	Privilegios excesivos	Ausencia de revisión de accesos.	Establecer revisiones trimestrales de accesos.	Alta
ISO/IEC 27001:2022	A.8.2 - Clasificación de la información	Asignación de privilegios sin justificación.	Abuso de privilegios Acceso innecesario Falta de trazabilidad	Se debe definir el proceso de autorización de acceso a los archivos críticos por parte de las áreas de negocio, partiendo de la identificación de archivos críticos, de los usuarios que acceden los mismos e identificación de los responsables de la información, así como los controles que se requieren para la prevención de fuga de información.	Alta
ISO/IEC 27001:2022	A.8.3 - Manejo de Información	Usuarios sin permisos adecuados podrían visualizar o modificar datos sensibles. Información PII o PCI puede quedar accesible a terceros o al público si no se restringe correctamente. Falta de segmentación de accesos.	Acceso no autorizado a información confidencial Exposición de información PII o PCI Falta de segmentación de accesos Configuraciones inseguras	Se debe establecer niveles de autorización de acceso a los archivos críticos por parte de las áreas de negocio, partiendo de la identificación de archivos críticos, de los usuarios que acceden los mismos e identificación de los responsables de la información, así como los controles que se requieren para la prevención de fuga de información con monitoreo y trazabilidad del uso de la información.	Alta
PCI DSS v4.0.1	Requisito 7.2.3 - Revisión de accesos	No se revisan los accesos de usuarios con privilegios elevados Cuentas con roles desactualizados y con opciones que ya no utiliza el funcionario.	Abuso de privilegios por parte de administradores	La aprobación documentada (por ejemplo, por escrito o electrónicamente) garantiza que las personas con acceso y privilegios son conocidas y están autorizadas por la dirección, y que su acceso es necesario para su función laboral.	Alta
PCI DSS v4.0.1	Requisito 8.3.1 - MFA para accesos administrativos	No se ha implementado MFA en accesos a bases de datos con datos PCI	Acceso no autorizado a datos de tarjetas	Un enfoque común que individuos maliciosos emplean para comprometer un sistema es explotar factores de autenticación débiles o inexistentes (como, por ejemplo, contraseñas/preguntas de seguridad). Exigir factores de autenticación fuertes ayuda a protegerse contra este tipo de ataque.	Alta
PCI DSS v4.0.1	Requisito 10.2.1 - Registro de eventos	Los logs de acceso no se almacenan centralizadamente	Dificultad para detectar accesos indebidos	Cuando una entidad considera qué información guardar en sus registros, es importante recordar que la información	Media

Estándar	Control/Requisito	Brecha Identificada	Riesgo Asociado	Recomendación	Prioridad
				almacenada en los registros de auditoría es sensible y debe protegerse según los requisitos de este estándar. Se debe tener el cuidado de almacenar solo información esencial para minimizar riesgos.	
CE 029 2014	Requisito 3.1 - Política SGSI	Socialización sobre actualización de Políticas y estándares del SGSI	Desconocimiento de las políticas y estándares de seguridad de la información por parte de las áreas operativas.	Implementar una estrategia de socialización de los estándares y políticas de seguridad de la información en toda la organización. Realizar mínimo anualmente un curso de seguridad de la información donde sean relevantes el tema de manejo seguro de archivos PII y PCI.	Alta
CE 029 2014	Requisito 3.5 - Autenticación y autorización de usuarios	Falta de autenticación multifactor en aplicaciones críticas.	Compromiso de cuentas privilegiadas Accesos no autorizados	Implementar MFA en todos los accesos a sistemas que manejan datos PII y PCI.	Alta
CE 029 2014	Requisito 4.1.1 - Mínimos privilegios de acceso	Matrices de acceso por rol; falta de revisión periódica.	Dificultad para detectar accesos indebidos	Establecer responsables de autorizar el acceso a la información. Establecer revisiones trimestrales de accesos por parte de los dueños de la información.	Alta
CE 029 2014	Requisito 4.1.8 - Monitoreo de eventos en las aplicaciones	Algunos Logs habilitados en bases de datos y servidores; no se centralizan en SIEM.	Sistemas automatizados que no detectan patrones sospechosos. Retrasos que pueden comprometer investigaciones o sanciones.	Verificar que los activos de información donde se encuentran los archivos que contienen información PCI y PII estén debidamente monitoreados con la herramienta SIEM que posee el banco configurando todos loa accesos anómalos que posea estos servidores.	Alta
CE 029 2014	Requisito 3.2.6. - Revisión de procedimientos periódicamente	No existe procedimiento formal de revisión periódica.	Dificultad para detectar accesos indebidos	Implementar política de revisión semestral de accesos con trazabilidad.	Alta
CE 029 2014	Requisito 4.3.5. - Conservación de registros de auditoría	Falta de revisión de backups automáticos de logs en almacenamiento seguro que se debe tener por 12 meses.	Falla en almacenamiento de registros de auditoría sobre servidores que poseen información PCI y PII.	Mantener y revisar políticas de backups vigentes y auditar cumplimiento anual.	Baja

Nota. La tabla muestra cada una de las brechas de seguridad identificadas por cada uno de los controles evaluados. Elaboración propia.

7.6.7 Análisis de riesgo

Teniendo en cuenta la presencia de diversas amenazas que afectan los archivos que contienen información sensible, como datos PII y PCI, en el entorno operativo de una entidad financiera, es posible establecer un análisis de riesgos basado en dos escenarios claves: la probabilidad de ocurrencia y el impacto potencial sobre los archivos involucrados.

Este enfoque permite evaluar de manera estructurada cada brecha identificada, determinando la probabilidad con la que una amenaza podría materializarse y, simultáneamente, el nivel de afectación que generaría sobre los archivos con información PII y PCI.

A partir de esta evaluación, se podrá priorizar la implementación de controles correctivos y preventivos, alineados con los estándares internacionales de seguridad de la información.

“La evaluación de riesgos debe ayudar a la organización a tomar decisiones sobre la gestión de los riesgos que afectan a la consecución de sus objetivos. Por lo tanto, debe dirigirse a aquellos riesgos y controles que, si se gestionan con éxito, mejorarán la probabilidad de que la organización logre sus objetivos.” (ISO 27005, 2022,p.12)

Para ello debe tener en cuenta los siguientes aspectos en el manejo del riesgo:

7.6.7.1 Criterios de aceptación del riesgo. En el tratamiento del riesgo, los criterios de aceptación del riesgo pueden utilizarse para determinar si el tratamiento del riesgo propuesto es suficiente para alcanzar un nivel de riesgo aceptable o el apetito de riesgo, o si es necesario un tratamiento adicional del riesgo.

El Banco tiene definidos los niveles de aceptación del riesgo o apetito de riesgo. Durante el desarrollo se debe tener en cuenta lo siguiente:

a) La coherencia entre los criterios de aceptación del riesgo para la seguridad de la información y los criterios generales de aceptación del riesgo de la organización.

b) Se identifica el nivel de gestión con autoridad delegada para tomar decisiones de aceptación de riesgos.

c) Los criterios de aceptación de riesgos pueden incluir múltiples umbrales, y la autoridad para la aceptación puede asignarse a diferentes niveles de gestión.

d) Los criterios de aceptación del riesgo pueden basarse únicamente en la probabilidad y las consecuencias, o pueden ampliarse para considerar también el equilibrio coste/beneficio entre las pérdidas previstas y el coste de los controles

e) Pueden aplicarse diferentes criterios de aceptación de riesgos a diferentes clases de riesgo (por ejemplo, los riesgos que pueden dar lugar a un incumplimiento de la normativa o las leyes no siempre se retienen, mientras que la aceptación de riesgos puede permitirse si la aceptación es resultado de un requisito contractual); Los criterios de aceptación del riesgo deben ser aprobados por el nivel de gestión autorizado.

De acuerdo con el numeral “6.4.3. Criterios para realizar valoraciones de riesgos para la seguridad de la información” de la norma ISO 27005:2022 hay que tener en cuenta:

Los criterios de valoración de riesgos especifican cómo se determina la importancia de un riesgo en términos de sus consecuencias, probabilidad y nivel de riesgo.

Los criterios de valoración de riesgos para la seguridad de la información deben tener en cuenta la idoneidad de las actividades de gestión de riesgos.

Las consideraciones para lograr esto incluyen:

a) el nivel de clasificación de la información

b) la cantidad y, en su caso, la concentración de la información

c) el valor estratégico de los procesos empresariales que hacen uso de la información

d) la criticidad de la información y de los activos relacionados con ella.

e) la importancia operativa y empresarial de la disponibilidad, la confidencialidad y la integridad.

f) las expectativas y percepciones de las partes interesadas (por ejemplo, la alta dirección)

g) las consecuencias negativas, como la pérdida de la buena voluntad y la reputación.

h) la coherencia con los criterios de riesgo de la organización. (ISO 27005, 2022)

Los criterios de evaluación de riesgos, o una base formal para definirlos, deben ser estandarizados en toda la organización para todos los tipos de evaluación de riesgos, ya que esto puede facilitar la comunicación, la comparación y la agregación de los riesgos asociados a múltiples ámbitos empresariales en el caso de una entidad financiera se debería implementar un proceso de estandarización con el área de riesgo operativo con la finalidad de tener matrices de riegos estandarizadas y apuntando hacia los objetivos estratégicos de la organización.

Los criterios de evaluación de riesgos para la seguridad de la información suelen incluir:

• Consecuencias, • Probabilidad y • Nivel de riesgo.

7.6.7.2 Criterios de consecuencias. Los criterios de consecuencia deben desarrollarse y especificarse en términos de la magnitud del daño o pérdida, o del perjuicio para el Banco, resultante de la pérdida de confidencialidad, integridad y disponibilidad de la información. Al definir los criterios de consecuencia, se debe considerar especialmente lo siguiente:

a) La pérdida de vidas o el daño a individuos o grupos.

b) Pérdida de la libertad, la dignidad o el derecho a la intimidad.

c) Pérdida de personal y de capital intelectual (habilidades y conocimientos).

d) El deterioro de las operaciones internas o de terceros (por ejemplo, el daño a una función o proceso empresarial).

e) Efectos sobre los planes y los plazos.

f) Pérdida de valor empresarial y financiero.

g) Pérdida de ventaja comercial o de cuota de mercado.

h) Daños a la confianza o reputación del público.

i) Incumplimientos de requisitos legales, reglamentarios o estatutarios.

j) Incumplimientos de contratos o niveles de servicio.

k) Impacto negativo en las partes interesadas.

l) Impacto negativo en el medio ambiente, contaminación.

Normalmente, los criterios de consecuencias son diferentes para las distintas organizaciones, dependiendo del contexto interno y externo de la organización. (Circular Básica C.E 029, 2014)

La siguiente escala de consecuencias ha sido definida en concordancia con el estándar ISO/IEC 27005:2022, y permite clasificar el impacto potencial de los eventos de riesgo sobre los activos de información evaluados, tal como se aprecia en la tabla 17.

Tabla 17.

Escala de consecuencias

Consecuencias	Descripción
5 - Catastrófico	**Consecuencias sectoriales o normativas más allá de la organización** Ecosistema(s) sectorial(es) sustancialmente afectado(s), con consecuencias que pueden ser duraderas. Y/o: dificultad para el Estado, e incluso incapacidad, de asegurar una función reguladora o una de sus misiones de vital importancia. Y/o: consecuencias críticas sobre la seguridad de las personas y los bienes (crisis sanitaria, contaminación ambiental importante, destrucción de infraestructuras esenciales, etc.).
4 - Critico	**Consecuencias desastrosas para la organización** Incapacidad de la organización para garantizar toda o parte de su actividad, con posibles consecuencias graves para la seguridad de las personas y los bienes. Lo más probable es que la organización no supere la situación (su Supervivencia está amenazada), los sectores de actividad o los sectores estatales en los que opera se verán probablemente afectados de forma leve, sin consecuencias duraderas.
3 - Serio	**Consecuencias sustanciales para la organización** Alta degradación en el desempeño de la actividad, con posibles consecuencias significativas en la seguridad de las personas y los bienes. La organización superará la situación con serias dificultades (funcionamiento en modo altamente degradado), sin impacto sectorial o estatal.
2 - Significante	**Consecuencias significativas pero limitadas para la organización** Degradación del rendimiento de la actividad sin consecuencias para la seguridad de las personas y los bienes. La organización superará la situación a pesar de algunas dificultades (funcionamiento en modo degradado).
1 - Menor	**Consecuencias insignificantes para la organización** No hay consecuencias sobre las operaciones o el desempeño de la actividad ni sobre la seguridad de las personas y los bienes. La organización superará la situación sin demasiada dificultad (se consumirán los márgenes).

Nota. En la tabla muestra los niveles de criticidad de riesgos para tener de referencia en la evaluación de riesgos. Tomado de ISO 27005 (2022).

7.6.7.3 Criterios de probabilidad. La determinación de los criterios de probabilidad depende de aspectos tales como:

a) Los acontecimientos accidentales o naturales.

b) El grado de exposición de la información relevante o del activo relacionado con la información a la amenaza.

c) El grado de explotación de la vulnerabilidad de la organización.

d) El fallo de la tecnología.

e) Actos u omisiones humanas (ISO 27005, 2022)

La probabilidad puede representarse de dos maneras: en términos probabilísticos, como la posibilidad de que un evento ocurra dentro de un periodo determinado; o en términos de frecuencia, como el número medio estimado de ocurrencias en dicho periodo. Aunque la probabilidad frecuencial es comúnmente utilizada en la comunicación de riesgos por su facilidad interpretativa, únicamente la probabilidad probabilística es válida para procesos de agregación de probabilidades, conforme a los lineamientos del estándar ISO/IEC 27005:2022.

Tabla 18.

Escala de probabilidades

Probabilidad	Descripción
5 – Casi Seguro	La fuente de riesgo alcanzará con toda seguridad su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy alta.
4 – Muy probable	La fuente de riesgo probablemente alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es alta.
3 – Probable	La fuente de riesgo es capaz de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es significativa.
2 – Bastante improbable	La fuente de riesgo tiene relativamente pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es baja.

1 – Improbable	La fuente de riesgo tiene muy pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy baja.

Nota. En la tabla muestra los niveles de probabilidad de riesgos para tener de referencia en la evaluación de riesgos. Tomado de ISO 27005 (2022).

7.6.7.4 Criterios para determinar el nivel de riesgo. El propósito de las escalas para el nivel de riesgo es ayudar a los propietarios del riesgo a decidir sobre la retención o el tratamiento de los riesgos y priorizarlos para su tratamiento. El nivel evaluado de un riesgo concreto debe ayudar a la organización a determinar la urgencia de tratar ese riesgo.

Dependiendo de la situación, se recomienda considerar el nivel de riesgo inherente (sin tener en cuenta ningún control), o el nivel de riesgo actual (teniendo en cuenta la eficacia de cualquier control ya implementado). La organización debe elaborar una clasificación de los riesgos, teniendo en cuenta lo siguiente

a) los criterios de consecuencia y de probabilidad.

b) las consecuencias que pueden tener los eventos de seguridad de la información a nivel estratégico, táctico y operativo (esto puede definirse como el peor caso, en otros términos, siempre que se utilice la misma base de forma coherente).

c) los requisitos legales y reglamentarios, y las obligaciones contractuales.

d) los riesgos que aparecen más allá de los límites del ámbito de la organización, incluidos los efectos imprevistos sobre terceros.

Los criterios de nivel de riesgo son necesarios para evaluar los riesgos analizados.

Los criterios de nivel de riesgo pueden ser cualitativos (por ejemplo, muy alto, alto, medio, bajo) o cuantitativos (por ejemplo, expresados en términos de valor esperado de pérdida monetaria, pérdida de vidas o cuota de mercado en un periodo de tiempo determinado).

La identificación del riesgo es fundamental, porque un riesgo para la seguridad de la información que no se identifique en esta fase no se incluirá en el análisis posterior.

La identificación de riesgos debe considerar los riesgos independientemente de si su fuente está bajo el control de la organización, incluso si no se evidencian fuentes de riesgo específicas. Especialmente cuando se evalúan escenarios de riesgo complejos, debe realizarse una evaluación de riesgos iterativa.

La primera ronda debe concentrarse en las observaciones de alto nivel y las rondas sucesivas deben abordar niveles adicionales de detalle hasta que puedan identificarse las causas fundamentales de los riesgos.

La gestión de los riesgos de la seguridad de la información no debe estar limitada por puntos de vista arbitrarios o restrictivos sobre cómo deben estructurarse, agruparse, agregarse, dividirse o describirse los riesgos. Los riesgos pueden parecer superpuestos o ser subconjuntos o instancias específicas de otros riesgos. Sin embargo, los controles de los riesgos individuales deben considerarse e identificarse por separado de los riesgos más amplios o de los riesgos agregados a efectos del tratamiento de los riesgos.

La agregación de riesgos no debe llevarse a cabo a menos que sean relevantes entre sí en el nivel en el que se está considerando el contexto de la organización. Puede ser necesario considerar por separado los riesgos que se fusionan a efectos del presupuesto de la gestión global de los riesgos, cuando se planifican las opciones de tratamiento, ya que pueden ser necesarios diferentes controles para gestionarlos. (ver tabla 19). (ISO 27005, 2022)

Tabla 19.

Enfoque cualitativo de los criterios de riesgo

Probabilidad	**Consecuencia**				
	Catastrófico	**Critico**	**Serio**	**Significante**	**Menor**
Casi Seguro	Muy alto	Muy alto	Alto	Alto	Alto

Muy probable	Muy alto	Alto	Alto	Medio	Bajo
Probable	Alto	Alto	Medio	Bajo	Bajo
Bastante improbable	Medio	Medio	Bajo	Bajo	Muy bajo
Improbable	Bajo	Bajo	Bajo	Muy bajo	Muy bajo

Nota. En la tabla muestra los niveles cualitativos de riesgos para tener de referencia en la evaluación de riesgos. Tomado de ISO 27005 (2022).

7.6.7.5 Evaluación de la probabilidad. La evaluación de la probabilidad se hace necesaria cuando:

• No se ha hecho antes.

• Se determinan cambios en el alcance o el contexto que pueden afectar a la probabilidad.

• Se descubren vulnerabilidades en los controles implementados.

• Las pruebas/auditorías de eficacia de los controles arrojan resultados inesperados.

• Se descubren cambios en el entorno de la amenaza (por ejemplo, nuevos actores / fuentes de amenaza).

Una vez identificados los escenarios de riesgo, es necesario analizar la probabilidad de que se produzca cada escenario y consecuencia, utilizando técnicas de análisis cualitativo o cuantitativo. La evaluación de la probabilidad no siempre es fácil y debe expresarse de diferentes maneras. Debe tenerse en cuenta la frecuencia con la que se producen las fuentes de riesgo o la facilidad con la que se pueden explotar algunas de ellas (por ejemplo, las vulnerabilidades), teniendo en cuenta:

- La experiencia y las estadísticas aplicables a la probabilidad de las fuentes de riesgo.
- Para las fuentes de riesgo deliberadas: el grado de motivación [por ejemplo, la viabilidad (coste/beneficio) del ataque] y las capacidades (por ejemplo, el nivel de destreza de los posibles atacantes), que cambian con el tiempo, los recursos de que disponen los posibles atacantes, y las influencias sobre los posibles atacantes, como la delincuencia grave, las

organizaciones terroristas o la inteligencia extranjera, así como la percepción del atractivo y la vulnerabilidad de la información para un posible atacante.

- Para las fuentes de riesgo accidentales: factores geográficos (por ejemplo, la proximidad a instalaciones o actividades peligrosas), la posibilidad de que se produzcan catástrofes naturales como condiciones meteorológicas extremas, actividad volcánica, terremotos, inundaciones, tsunamis y factores que puedan influir en los errores humanos y el mal funcionamiento de los equipos.
- Los puntos débiles conocidos y cualquier control compensatorio, tanto individualmente como en conjunto.
- Los controles existentes y su eficacia para reducir las debilidades conocidas.

La estimación de la probabilidad es intrínsecamente incierta, no sólo porque tiene en cuenta cosas que aún no han sucedido y, por tanto, no se conocen del todo, sino también porque la probabilidad es una medida estadística y no es directamente representativa de los acontecimientos individuales.

Las tres fuentes básicas de incertidumbre en la evaluación son:

- La incertidumbre personal, que se origina en el juicio del evaluador y que se deriva de la variabilidad de la heurística mental de la toma de decisiones
- La incertidumbre metodológica, que se deriva del uso de herramientas que inevitablemente modelan los sucesos de forma simplista.
- La incertidumbre sistémica sobre el propio acontecimiento previsto, que se deriva de un conocimiento insuficiente (en particular, si las pruebas son limitadas o una fuente de riesgo cambia con el tiempo) (ISO 27005, 2022)

El nivel de riesgo puede determinarse de muchas maneras posibles. Normalmente se

determina como una combinación de la probabilidad evaluada y las consecuencias evaluadas para todos los escenarios de riesgo relevantes. Los cálculos alternativos pueden incluir un valor del activo además de la probabilidad y las consecuencias. Además, el cálculo no es necesariamente lineal, por ejemplo, puede ser la probabilidad al cuadrado combinada con la consecuencia.

7.6.7.6 Valoración de los riesgos para la seguridad de la información. Como parte del proceso de evaluación normativa, se realiza una valoración de los riesgos asociados a la seguridad de la información, con el objetivo de identificar posibles vulnerabilidades, amenazas y desviaciones que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos críticos.

7.6.7.6.1 Comparación de los resultados del análisis de riesgos con los criterios de riesgo. Una vez identificados los riesgos y asignados los valores de probabilidad y gravedad de las consecuencias, las organizaciones deben aplicar sus criterios de aceptación de los riesgos para determinar si pueden aceptarse o no. Si no se pueden aceptar, se debe dar prioridad a su tratamiento.

Para valorar los riesgos, el Banco podría comparar los riesgos evaluados con los criterios de riesgo definidos durante el establecimiento del contexto.

Las decisiones de valoración de los riesgos deben basarse en la comparación del riesgo evaluado con los criterios de aceptación definidos, teniendo en cuenta idealmente el grado de confianza en la evaluación.

En algunos casos, como la ocurrencia frecuente de sucesos de consecuencias relativamente bajas, puede ser útil considerar su efecto acumulativo a lo largo de una escala temporal de interés, en lugar del riesgo de cada suceso considerado individualmente, ya que esto

puede proporcionar una representación más realista de los riesgos globales.

Los niveles de riesgo pueden validarse sobre la base de un consenso entre los propietarios de los riesgos y los especialistas empresariales y técnicos. Es importante que los propietarios de los riesgos tengan una buena comprensión de los riesgos de los que son responsables que coincida con los resultados de la valoración objetiva. En consecuencia, cualquier disparidad entre los niveles de riesgo valorados y los percibidos por los propietarios de los riesgos debe investigarse para determinar cuál se aproxima más a la realidad.

7.6.7.6.2 Priorización de los riesgos analizados para su tratamiento. La valoración de riesgos utiliza la comprensión del riesgo obtenida por el análisis de riesgos para hacer propuestas para decidir sobre el siguiente paso a dar. Éstas deben referirse a:

- Si es necesario un tratamiento del riesgo.
- Las prioridades para el tratamiento del riesgo teniendo en cuenta los niveles de riesgo valorados.

Los criterios de riesgo utilizados para priorizar los riesgos deben tener en cuenta los objetivos de la organización, los requisitos contractuales, legales y reglamentarios y las opiniones de las partes interesadas pertinentes. La priorización adoptada en la actividad de valoración de riesgos se basa principalmente en los criterios de aceptación. (ISO 27005, 2022)

Como resultado del diagnóstico realizado, se identificaron múltiples riesgos asociados a los activos evaluados. A continuación, se presenta su categorización y análisis conforme a los criterios de impacto y probabilidad establecidos que se presentan en la tabla 20.

Tabla 20.

Mapa de Riesgos

ID Riesgo	Riesgo Asociado	Activo afectado	Causa	Impacto	Probabilidad	Nivel de Riesgo
R1	Accesos no autorizados persistentes	Archivos PII o PCI	No existe revisión periódica de accesos a sistemas con información PII o PCI	4- Critico	4- Muy Probable	Alta
R2	Escalada de privilegios Persistencia de cuentas obsoletas	Aplicaciones CORE	Cuentas con roles desactualizados y con opciones que ya no utiliza el funcionario.	4- Critico	3- Probable	Alta
R3	Compromiso de credenciales	Servidores de aplicación, Servidores de Bases de Datos y Bases de Datos	Contraseñas débiles y sin política de expiración	4- Critico	4- Muy Probable	Alta
R4	Abuso de privilegios Acceso innecesario Falta de trazabilidad	Servidores de aplicación, Servidores de Bases de Datos y Bases de Datos	Asignacion de privilegios sin justificación.	4- Critico	3- Probable	Alta
R5	Acceso no autorizado a información confidencial Expoción de información PII o PCI Falta de segmentación de accesos Configuraciones inseguras	Aplicaciones CORE	Usuarios sin permisos adecuados podrian visualizar o modificar datos sensibles. Información PII o PCI puede quedar accesible a terceros o al público si o se restringe correctamente. Falta de segmentación de accesos.	4- Critico	4- Muy Probable	Alta
R6	Abuso de privilegios por parte de administradores	Aplicaciones CORE	No se revisan los accesos de usuarios con privilegios elevados Cuentas con roles desactualizados y con opciones que ya no utiliza el funcionario.	4- Critico	4- Muy Probable	Alta
R7	Acceso no autorizado a datos de tarjetas	Servidores de aplicación, Servidores de Bases de Datos y Bases de Datos, Aplicación CORE	No se ha implementado MFA en accesos a bases de datos con datos PCI	4- Critico	4- Muy Probable	Alta
R8	Dificultad para detectar accesos indebidos	Servidores de aplicación, Servidores de Bases de Datos y Bases de Datos, Aplicación CORE	Los logs de acceso no se almacenan centralizadamente	3- Serio	4- Muy Probable	Media
R9	Desconocimiento de las politicas y estándares de seguridad de la información por pate del las areas operativas.	Estándares y politicas de Seguridad de la información	Socialización sobre actualización de Politicas y estándares del SGSI	3- Serio	3- Probable	Media
R10	Compromiso de cuentas privilegiadas Accesos no autorizados	Servidores de aplicación, Servidores de Bases de Datos, Bases de Datos y aplicaciones CORE.	Falta de autenticación multifactor en aplicaciones críticas.	4- Critico	4- Muy Probable	Alta
R11	Dificultad para detectar accesos indebidos	Aplicaciones CORE	Matrices de acceso por rol; falta de revisión periódica.	3- Serio	4- Muy Probable	Media
R12	Sistemas automatizados que no detectan patrones sospechosos. Retrasos que pueden comprometer investigaciones o sanciones.	Servidores de aplicación, Servidores de Bases de Datos, Bases de Datos y aplicaciones CORE.	Algunos Logs habilitados en bases de datos y servidores; no se centralizan en SIEM.	3- Serio	3- Probable	Media

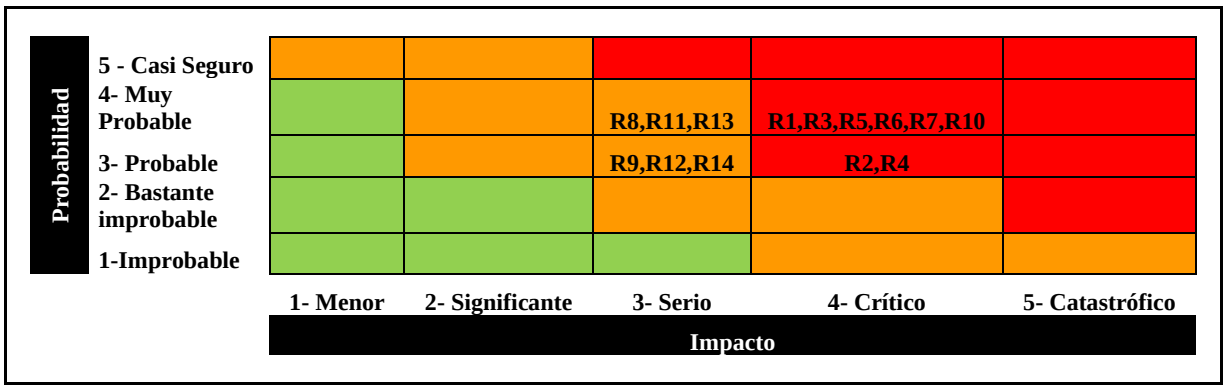
ID Riesgo	Riesgo Asociado	Activo afectado	Causa	Impacto	Probabilidad	Nivel de Riesgo
R13	Dificultad para detectar accesos indebidos	Servidores de aplicación, Servidores de Bases de Datos, Bases de Datos y aplicaciones CORE.	No existe procedimiento formal de revisión periódica.	3- Serio	4- Muy Probable	Media
R14	Falla en almacenamiento de registros de auditoría sobre servidores que poseen informacion PCI y PII.	Servidores de Backup.	Falta de revisióna los backups automáticos de logs en almacenamiento seguro que se debe tener por 12 meses.	3- Serio	3- Probable	Media

Nota. En la tabla se registran los riesgos identificados con la evaluación realizada, activos afectado, causa, impacto, probabilidad y nivel de riesgo. Elaboración propia.

Mapa de calor de riesgos. Con base en la matriz de riesgos previamente presentada, se construye el siguiente mapa de calor de riesgos en la tabla 21:

Tabla 21.

Mapa de calor



Nota. La tabla permite visualizar la distribución de los riesgos según su nivel de impacto y probabilidad. Elaboración propia.

7.6.8 Plan de tratamiento de riesgos

El tratamiento de los riesgos para la seguridad de la información se basa en los resultados del proceso de evaluación de riesgos en forma de un conjunto priorizado de riesgos a tratar,

basado en criterios de riesgo.

El resultado de este proceso es un conjunto de controles de seguridad de la información necesarios que deben desplegarse o mejorarse entre sí, de acuerdo con el plan de tratamiento de riesgos. Desplegado de esta manera, la eficacia del plan de tratamiento de riesgos es modificar el riesgo de seguridad de la información al que se enfrenta la organización para que cumpla con los criterios de aceptación de la organización.

Varias opciones para el tratamiento del riesgo incluyen:

- Evitar el riesgo, decidiendo no iniciar o continuar con la actividad que da lugar al riesgo.
- Modificar el riesgo, cambiando la probabilidad de que se produzca un suceso o una consecuencia o cambiando la gravedad de la consecuencia.
- Retener del riesgo, mediante una elección informada.
- Compartir o transferir el riesgo, repartiendo las responsabilidades con otras partes, ya sea interna o externamente (por ejemplo, compartiendo las consecuencias a través de un seguro).

En el caso de compartir el riesgo, se requiere al menos un control para modificar la probabilidad o la consecuencia, pero la organización delega la responsabilidad de aplicar el control a otra parte. (ISO 27005, 2022)

Con base en los riesgos identificados, se elabora el siguiente plan de tratamiento de riesgos, ver tabla 22:

Tabla 22.

Plan de tratamiento de riesgos

ID Riesgo	Riesgo	Acción recomendada	Responsable	Plazo	Estado
R1	Accesos no autorizados persistentes	* Implementar autenticación multifactor (MFA) obligatoria para accesos privilegiados a sistemas considerados como críticos. * Gestión robusta de cuentas privilegiadas (PAM) realizando rotación automática de credenciales y monitoreo de sesiones.	Administrador de seguridad TI	30 días	Pendiente

ID Riesgo	Riesgo	Acción recomendada	Responsable	Plazo	Estado
		* Capacitación especifica en accesos privilegiados para usuarios técnicos y administradores. * Simulacros de respuesta ante accesos persistentes evaluando tiempos de detección y contención.			
R2	Escalada de privilegios Persistencia de cuentas obsoletas	* Aplicar el principio de mínimo privilegio asegurando que cada usuario tenga solo los accesos necesarios para su función. * Separación de funciones evitando que una sola persona tenga control completo sobre procesos críticos (Ej. acceso a información PII o PCI y permisos de envío de información a dominios externos). * Revisión periódica de roles y accesos validando que no existan acumulaciones indebidas de privilegios por cambios de rol o antigüedad. Realizar certificaciones periódicas de tres meses para no tener accesos no necesarios. * Alertas sobre cambios en grupos de seguridad en los sistemas involucrados en el proceso (Ej. D.A y aplicaciones donde se almacene información PCI y PII). * Politicas claras de asignación y revocación de privilegios que incluya validaciones por parte de responsables de área.	Administrador de seguridad TI Responsable de sistemas	45 días	Pendiente
R3	Compromiso de credenciales	* Implementar política robusta de contraseñas donde tanto el funcionario de operaciones como los administradores de control de acceso lógico tengan claros los criterios de longitud mínima, complejidad, caducidad y prohibición de reutilización de contraseñas de usuario. * Desactivación de cuentas inactivas o huérfanas evitando que sean utilizadas como vectores de ataque. * Implementar UEBA (User and Entity Behavior Analytics) identificando patrones de comportamiento que sugieran uso indebido de credenciales. * Habilitar registros de acceso y monitoreo de eventos, realizar verificación a las reglas de monitoreo en la herramienta SIEM. * Evitar almacenamiento local de credenciales deshabilitando funciones de autoguardado en navegadores y aplicaciones.	Equipo de seguridad TI	30 días	Pendiente
R4	Abuso de privilegios Acceso innecesario Falta de trazabilidad	* Detectar desviaciones en el comportamiento de usuarios privilegiados a través de UEBA (User and Entity Behavior Analytics). * Documentar funciones, responsabilidades y necesidades de acceso por área. * Evitar asignaciones genéricas o acumulativas. * Prevenir conflictos de interés y acumulación de privilegios críticos. * Verificar y reforzar las reglas de monitoreo en las herramientas SIEM del Banco.	Equipo de seguridad TI	15 días	Pendiente
R5	Acceso no autorizado a información confidencial Exposición de información PII o PCI Falta de segmentación de accesos Configuraciones inseguras	* Implementar accesos otorgados solo según rol y necesidad operativa. * Evitar acumulación de privilegios que permitan acceso y modificación simultánea. * Verificar el Aislamiento de entornos que manejan información confidencial (ej. bases de datos, servidores de archivos). * Realizar un etiquetado mas robusto de datos según su sensibilidad (Confidencial registrada, confidencial, interna y publica). * Restringir copia o traslado de información fuera de entornos seguros. * Revisión de configuraciones de permisos especialmente en carpetas compartidas, bases de datos y sistemas legados. * Separar sistemas que procesan PCI/PII de redes corporativas generales. * Desactivación de almacenamiento innecesario evitando retención de PAN completo o datos PII no requeridos. * Revisión de logs y trazabilidad validando que todo acceso a PII/PCI esté registrado y sea auditable. * Entrenamiento específico sobre manejo de PII/PCI diferenciando entre tipos de datos, riesgos y buenas prácticas. * Desactivación de servicios innecesarios evitando exposición de puertos y servicios no requeridos. * Simulacros de explotación de configuraciones débiles evaluando respuesta ante escenarios de escalamiento de privilegios y fuga de datos.	Administrador de seguridad TI Responsable de sistemas	90 días	Pendiente

ID Riesgo	Riesgo	Acción recomendada	Responsable	Plazo	Estado
		* Política de configuración segura incluyendo criterios de hardening, validación, y revisión periódica.			
R6	Abuso de privilegios por parte de administradores	* Implementación de PAM (Privileged Access Management) con los siguientes criterios: - Bóvedas seguras para credenciales - Accesos just-in-time - Grabación y monitoreo de sesiones privilegiadas - Rotación automática de contraseñas * Evitar que un solo administrador tenga control total sobre procesos críticos. * Política clara de uso de privilegios administrativos definiendo límites, responsabilidades y sanciones. * Rotación de funciones y supervisión periódica evitando dependencia excesiva de un solo administrador.	Administrador de seguridad TI/Áreas de operaciones	30 días	Pendiente
R7	Acceso no autorizado a datos de tarjetas	* MFA obligatoria para usuarios con acceso a datos de tarjetas. * Principio de mínimo privilegio y separación de funciones. * Alertas por accesos no autorizados, extracción masiva o uso fuera de horario. * Validar trazabilidad y legitimidad de cada acceso * Capacitación específica sobre manejo de datos de tarjetas en todos los niveles: técnico, operativo y ejecutivo.	Administrador de seguridad TI/Áreas de operaciones	90 días	Pendiente
R8	Dificultad para detectar accesos indebidos	* Redefinir reglas de correlación específicas para accesos indebido. * Detectar intentos de extracción o envío de información sensible a través de DLP (Data Loss Prevention). * Simulacros de accesos indebidos y ejercicios de Red Team evaluando la capacidad de detección. * Definir matriz RACI para gestión de accesos y monitoreo identificando roles responsables de revisar, escalar y responder. * Clasificación de activos críticos y usuarios sensibles priorizando monitoreo en sistemas con datos PII, PCI, financieros o regulatorios. * Capacitación en identificación de accesos indebidos para custodios de información, analistas SOC y líderes de área.	Administrador de seguridad TI	90 días	Pendiente
R9	Desconocimiento de las políticas y estándares de seguridad de la información por parte de las áreas operativas.	* Publicar y mantener actualizadas las políticas de seguridad manteniéndolas accesibles en la intranet corporativa o un repositorio central. * Asignar responsables de seguridad por área operativa (líderes de cumplimiento) donde actúen como enlace entre Seguridad y Operaciones. * Programas de formación obligatoria por rol adaptados a funciones operativas, con ejemplos prácticos. * Programas de formación obligatoria por rol adaptados a funciones operativas, con ejemplos prácticos. * Campañas internas de seguridad de la información enviando mensajes clave, casos reales, participación de líderes. * Integración de seguridad en procesos operativos clave como la seguridad como parte del “cómo se hace el trabajo”.	Equipo de seguridad TI/Áreas de operaciones	60 días	Pendiente
R10	Compromiso de cuentas privilegiadas Accesos no autorizados	* Revisión de configuraciones y herencias inseguras evitando acumulación de privilegios por antigüedad o movilidad interna. * Implementar autenticación multifactor (MFA) obligatoria para accesos privilegiados a sistemas considerados como críticos. * Gestión robusta de cuentas privilegiadas (PAM) realizando rotación automática de credenciales y monitoreo de sesiones. * Capacitación especifica en accesos privilegiados para usuarios técnicos y administradores. * Simulacros de respuesta ante accesos persistentes evaluando tiempos de detección y contención.	Equipo de seguridad TI	30 días	Pendiente
R11	Dificultad para detectar accesos indebidos	* Redefinir reglas de correlación específicas para accesos indebido. * Detectar intentos de extracción o envío de información sensible a través de DLP (Data Loss Prevention). * Simulacros de accesos indebidos y ejercicios de Red Team evaluando la capacidad de detección. * Definir matriz RACI para gestión de accesos y monitoreo identificando roles responsables de revisar, escalar y responder. * Clasificación de activos críticos y usuarios sensibles priorizando monitoreo en sistemas con datos PII, PCI, financieros o regulatorios. * Capacitación en identificación de accesos indebidos para custodios de información, analistas SOC y líderes de área.	Administrador de seguridad TI	90 días	Pendiente

ID Riesgo	Riesgo	Acción recomendada	Responsable	Plazo	Estado
R12	Sistemas automatizados que no detectan patrones sospechosos. Retrasos que pueden comprometer investigaciones o sanciones.	* Redefinir reglas de correlación específicas para accesos indebido. * Revisar el proceso de gestión de incidentes de seguridad.	Equipo de seguridad TI/Áreas de operaciones	30 días	Pendiente
R13	Dificultad para detectar accesos indebidos	* Redefinir reglas de correlación específicas para accesos indebido. * Detectar intentos de extracción o envío de información sensible a través de DLP (Data Loss Prevention). * Simulacros de accesos indebidos y ejercicios de Red Team evaluando la capacidad de detección. * Definir matriz RACI para gestión de accesos y monitoreo identificando roles responsables de revisar, escalar y responder. * Clasificación de activos críticos y usuarios sensibles priorizando monitoreo en sistemas con datos PII, PCI, financieros o regulatorios. * Capacitación en identificación de accesos indebidos para custodios de información, analistas SOC y líderes de área.	Administrador de seguridad TI	90 días	Pendiente
R14	Falla en almacenamiento de registros de auditoría sobre servidores que poseen información PCI y PII.	* Uso de servidores dedicados o soluciones SIEM con alta disponibilidad. * Backups cifrados y verificados periódicamente validando integridad y restauración de logs críticos. * Monitoreo de capacidad y alertas de saturación para evitar pérdida de registros por falta de espacio. * Firmado digital de registros para garantizar que no han sido alterados. * Control de acceso granular a logs para solo personal autorizado puede visualizar, modificar o eliminar. * Alertas por fallos en generación o almacenamiento de logs para detectar interrupciones, errores de escritura o corrupción.	Administrador de seguridad TI	90 días	Pendiente

Nota. En la tabla se describen los planes de acción, responsables, tiempo estimado de remediación y estado, para cada uno de los riesgos identificados. Elaboración propia.

7.6.9 Propuesta de recomendaciones para fortalecer los controles de acceso

Como resultado del diagnóstico realizado sobre los controles de acceso lógico en las aplicaciones evaluadas, se propone un conjunto de recomendaciones, orientadas a fortalecer la seguridad de los accesos y reducir el riesgo de fuga de información, especialmente aquella clasificada como sensible (PII y PCI).

Las recomendaciones se alinean con los principios de mínimo privilegio, necesidad de conocer, segregación de funciones, y los requisitos establecidos por ISO/IEC 27001:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014. Las recomendaciones se agrupan en las siguientes categorías (Ver tablas 23,24 y25)

7.6.9.1 Gestión de Accesos y Privilegios

- Implementar revisiones periódicas de accesos por parte de los responsables de cada sistema.
- Establecer ciclos formales de revisión de usuarios, roles y privilegios en cada aplicación, con trazabilidad y aprobación por parte de los responsables del negocio.
- Establecer controles para evitar la asignación de privilegios excesivos o innecesarios.
- Automatizar la revocación de accesos inactivos o no utilizados.
- Asignación de Responsabilidades.

Tabla 23.

Recomendación Gestión de Accesos y Privilegios

Recomendación	Justificación	Responsable Sugerido
Establecer un modelo RACI para la gestión de accesos	Clarifica quién solicita, aprueba, implementa y revisa accesos	Seguridad de la Información / Dueños de Proceso
Designar responsables por cada aplicación Core	Facilita la trazabilidad y control de accesos específicos	TI / Dueños de Aplicación
Formalizar la aprobación de accesos por parte de líderes de proceso	Asegura que los accesos estén alineados con funciones reales	Líderes de Área / Recursos Humanos

Nota. La tabla muestra recomendaciones y responsables en el plan de remediación. Elaboración propia

7.6.9.2 Fortalecer la segregación de funciones (SoD).

- Actualizar las matrices de acceso para evitar que un mismo usuario tenga funciones incompatibles (ej. creación y aprobación de transacciones).
- Definir y mantener matrices SoD actualizadas para cada aplicación crítica.
- Reasignar funciones incompatibles detectadas en perfiles existentes.
- Incorporar controles compensatorios en casos donde la segregación no sea viable.

7.6.9.3 Aplicar controles de acceso basados en roles (RBAC). Definir roles estandarizados por función y área, evitando asignaciones personalizadas que puedan generar privilegios excesivos.

7.6.9.4 Implementar Múltiple Factor de Autenticación (MFA). Reforzar el acceso a sistemas críticos mediante MFA, especialmente para usuarios con privilegios elevados o acceso remoto.

7.6.9.5 Monitorear accesos a información sensible

- Establecer alertas ante actividades inusuales o no autorizadas.
- Integrar los registros de auditoría en los procesos de revisión interna.
- Activar alertas y registros de auditoría para accesos a archivos clasificados como críticos, incluyendo intentos fallidos y accesos fuera del horario laboral.}
- Mecanismos de Trazabilidad

Tabla 24.

Recomendación de Monitoreo accesos a archivos con información sensible

Recomendación	Justificación	Responsable Sugerido
Centralizar los logs de acceso en una solución SIEM	Facilita el monitoreo y la detección de accesos indebidos	Infraestructura / Seguridad de la Información
Establecer alertas automáticas para accesos anómalos	Mejora la capacidad de respuesta ante incidentes	Seguridad de la Información
Realizar revisiones periódicas de registros de acceso	Asegura la trazabilidad y cumplimiento normativo	Auditoría Interna / Seguridad de la Información

Nota. La tabla muestra recomendaciones y responsables en el plan de remediación. Elaboración propia

7.6.9.6 Establecer controles de prevención de fuga de información (DLP). Implementar soluciones de DLP para detectar y bloquear la transferencia no autorizada de

información sensible por correo, dispositivos USB o plataformas en la nube.

7.6.9.7 Documentación y Procedimientos

- Actualizar los manuales de gestión de usuarios y perfiles conforme a los estándares vigentes.
- Formalizar los procedimientos de asignación, modificación y revocación de accesos.
- Mantener trazabilidad documental de todas las acciones relacionadas con accesos.
- Clasificación de la Información

Tabla 25.

Recomendación Sensibilización documentos de estándares y políticas de seguridad

Recomendación	Justificación	Responsable Sugerido
Implementar un esquema de clasificación de información (Confidencial, Interna, Pública)	Permite aplicar controles diferenciados según sensibilidad	Seguridad de la Información
Asociar niveles de acceso a cada clase de información	Minimiza el riesgo de exposición indebida	Dueños de Información / TI
Capacitar a los usuarios sobre el manejo de información clasificada	Reduce errores humanos y fugas accidentales	Seguridad de la Información / Recursos Humanos

Nota. La tabla muestra recomendaciones y responsables en el plan de remediación. Elaboración propia

7.6.9.8 Capacitación continua en seguridad de la información

- Sensibilizar a los usuarios sobre buenas prácticas de acceso, manejo de información confidencial y riesgos asociados al uso indebido de credenciales.
- Promover la cultura de mínimo privilegio y necesidad de conocer.
- Incluir la gestión de accesos como parte de los programas de inducción y formación continua.

Estas recomendaciones buscan reducir el riesgo de accesos indebidos, fortalecer la gobernanza de identidades y garantizar la integridad de los procesos operativos, contribuyendo al cumplimiento normativo y a la mejora continua del sistema de gestión de seguridad de la información.

7.6.10 Plan de Implementación de Controles Compensatorios

Mitigar los riesgos identificados en el diagnóstico de controles de acceso lógico mediante la implementación de controles compensatorios que garanticen la protección de la información sensible (PII y PCI), en cumplimiento con ISO/IEC 27001:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014. (Ver tabla 26, 27 y 28)

Tabla 26.

Controles Compensatorios Propuestos

Riesgo Identificado	Control Compensatorio	Justificación	Normativa
Accesos excesivos por falta de segregación	Revisión mensual de accesos por auditoría interna	Control manual mientras se implementa IAM	ISO 27001 A.5.18, PCI DSS 7.2
Provisión manual sin trazabilidad	Registro en sistema de tickets con aprobación documentada	Mitiga la falta de automatización	PCI DSS 7.1, Circular 029
Ausencia de monitoreo en tiempo real	Revisión diaria de logs críticos por el equipo de seguridad	Suple la reconfiguración de reglas en SIEM	ISO 27001 A.5.17
Roles no definidos claramente	Matriz de roles y responsabilidades publicada y revisada trimestralmente	Control organizacional	ISO 27001 A.6.1
Capacitación insuficiente	Talleres mensuales de concientización en gestión de accesos	Mejora la cultura de seguridad	ISO 27001 A.6.3

Nota. La tabla muestra los controles compensatorios propuestos para la remediación de los riesgos identificados en cumplimiento a cada uno de los controles normativos. Elaboración propia.

Tabla 27.

Cronograma de Implementación

Fase	Actividad	Responsable	Fecha
Fase 1	Diseño de controles compensatorios	Seguridad de la Información	01/09/2025
Fase 2	Validación con Stakeholders	Seguridad de la información / Auditoría	10/09/2025
Fase 3	Implementación operativa	Dueños aplicación TI / Seguridad de la información	15/09/2025
Fase 4	Seguimiento y ajustes	Seguridad de la información / Auditoría	Desde 01/10/2025

Nota. La tabla muestra el cronograma propuesto para la implementación de los controles compensatorios de acuerdo a cada una de las fases. Elaboración propia.

Tabla 28.

Presupuesto Estimado

Rubro	Descripción	Costo Estimado (COP)
Capacitación	Talleres mensuales (material y facilitador)	$6.000.000
Consultoría externa	Validación de controles compensatorios	$12.000.000
Herramientas	Licencias temporales para gestión de accesos	$18.000.000
Auditoría interna	Horas hombre para revisión de accesos	$8.000.000
Contingencia	10% sobre el total	$4.400.000
Total Aproximado		$48.400.000

Nota. La tabla muestra el presupuesto estimado para la implementación de los controles compensatorios de acuerdo a cada una de los rubros requeridos. Elaboración propia.

7.6.11 Presentación de informe final

Este informe presenta los resultados de la evaluación de los controles de acceso lógico implementados en las aplicaciones Core de las áreas de operaciones de una entidad financiera. La evaluación se realizó conforme a los estándares ISO/IEC 27001:2022, ISO/IEC 27005:2022, PCI DSS v4.0.1 y la Circular Externa 029 de la Superintendencia Financiera de Colombia. Se utilizó una escala de madurez para calificar el nivel de implementación de cada control (ver figura 29)

Escala de Madurez

- Inicial: No existe el control o está en etapa incipiente.
- Repetible: El control se aplica de forma informal o reactiva.
- Definido: El control está documentado y estandarizado.
- Gestionado: El control se monitorea y revisa periódicamente.
- Optimizado: El control está automatizado y en mejora continua.

Tabla 29.

Resultados de la evaluación

Categoría	Control Evaluado	Estándar/Norma	Nivel de Madurez	Observaciones
Política de acceso	Existencia y actualización de la política de control de acceso	ISO/IEC 27001 A.9.1.1	Definido	Existen políticas globales que en las áreas de negocio desconocen por falta de socialización.
Gestión de identidades	Asignación, modificación y revocación de accesos	ISO/IEC 27001 A.9.2 / PCI DSS Req. 7	Repetible	El área de control de acceso gestiona de forma manual y reactiva la asignación y revocación de accesos sobre archivos con información sensible (PII y PCI), presentando una administración compleja para el control de la gestión de permisos.
Autenticación	Implementación de MFA en accesos críticos	PCI DSS Req. 8 / Circular 029	Repetible	Aunque existen controles MFA en la administración de plataformas, no se tiene implementado para las áreas de negocio que acceden a información sensible, en especial a las áreas operativas que acceden diariamente a esta información.

Segregación de funciones	Separación de roles críticos	ISO/IEC 27001 A.9.2.6 / Circular 029	Repetible	Existen perfiles segregados en las aplicaciones, pero por la dinámica del negocio de traslados de procesos o reestructuraciones internas y en conjunto con el proceso manual de la administración de usuarios y perfiles, se encuentran perfiles desactualizados con funciones que no son requeridas en las nuevas funciones, esto requiere definición de responsables, capacitación periódica a líderes y ajustes automatizados para la correcta segregación de funciones.
Monitoreo de accesos	Registro y revisión de logs de acceso	ISO/IEC 27001 A.12.4 / PCI DSS Req. 10	Repetible	Existen logs de algunas aplicaciones, pero se recomienda revisar las reglas de monitoreo, dado que no todas se encuentran en cumplimiento, esto debe ser revisado por parte de los administradores de las aplicaciones y en conjunto con el equipo de Monitoreo de seguridad, que garanticen el cumplimiento de acuerdo con el estándar de Monitoreo de eventos de seguridad.
Evaluación de riesgos	Identificación de riesgos asociados al acceso lógico	ISO/IEC 27005 / Circular 029	Definido	Los riesgos se encuentran documentados, pero se recomienda realizar un seguimiento con mayor frecuencia a los planes de tratamiento de los correspondientes riesgos de seguridad identificados.
Protección de PII/PCI	Controles específicos para archivos sensibles	PCI DSS Req. 3 / Circular 029	Repetible	Existen controles de acceso básicos sobre los archivos que contienen información sensible PII y PCI, pero se deben reforzar con controles compensatorios que prevengan una fuga de información, mediante identificación de responsables que autoricen el acceso, restricciones de salida de correo externo, automatizaciones que permitan cambiar la forma en la que acceden los usuarios a la información en claro, herramientas de DLP, limitar el acceso a usuarios expertos y concientización al personal que accede, manipula y comparte este tipo de información.
Auditoría y cumplimiento	Evidencia de cumplimiento normativo	Todos	Definido	Se recomienda formalizar un mecanismo de revisión normativa recurrente, con responsables definidos, trazabilidad documental y criterios de actualización para políticas, procedimientos y controles técnicos.

Nota. La tabla muestra el resultado de la evaluación de los controles de acuerdo a cada una de las normativas y estándares de seguridad según el alcance. Elaboración propia.

El diagnóstico de controles de acceso lógico a archivos con información PII y PCI en las aplicaciones Core de las áreas operativas de una entidad financiera ha permitido identificar brechas relevantes en la gestión de accesos, así como oportunidades de mejora alineadas con los estándares internacionales y normativos aplicables.

Durante el desarrollo del proyecto, se logró:

- Evaluar el estado actual de los controles de acceso lógico.

- Identificar riesgos asociados al acceso indebido a información sensible.
- Proponer controles compensatorios efectivos y viables.
- Diseñar un plan de implementación con cronograma, responsables y presupuesto estimado.
- Generar conciencia sobre la importancia de proteger los datos críticos del banco.

La ejecución de las recomendaciones planteadas contribuirá significativamente a fortalecer la postura de seguridad de la entidad, reducir el riesgo de exposición de datos sensibles y garantizar el cumplimiento normativo. Además, se promueve una cultura organizacional orientada a la protección de la información, la trazabilidad de los accesos y la responsabilidad en el manejo de datos.

Con el cierre de este proyecto, se habilita una hoja de ruta clara para la mejora continua en la gestión de accesos, que podrá ser integrada en futuras auditorías, revisiones regulatorias y procesos de transformación digital del banco.

Conclusiones

El diagnóstico realizado sobre los controles de acceso lógico a archivos que contienen información sensible (PII y PCI) en las aplicaciones Core de las áreas de Operaciones de una entidad financiera permitió identificar fortalezas, oportunidades de mejora y riesgos asociados a la gestión de accesos en entornos críticos.

Entre los principales hallazgos se destacan:

La existencia de controles de acceso básicos que permiten una protección inicial de la información sensible, aunque requieren ser reforzados mediante controles compensatorios más robustos.

La documentación de políticas, procedimientos y matrices de acceso está disponible, pero en algunos casos presenta desactualización o falta de alineación con estándares internacionales como ISO/IEC 27001:2022, PCI DSS v4.0.1 y la Circular Externa 029 de 2014.

Se evidencian brechas en la segregación de funciones, asignación de privilegios y trazabilidad de accesos, lo que puede representar un riesgo operativo y de cumplimiento.

El proceso de cumplimiento normativo es reactivo, lo que implica la necesidad de establecer mecanismos de revisión periódica para asegurar un cumplimiento continuo.

Se identifica la necesidad de implementar herramientas de prevención de fuga de información (DLP), automatizaciones para el acceso a datos en claro, y campañas de concientización al personal que manipula información sensible.

Como resultado del diagnóstico, se propone un conjunto de recomendaciones técnicas y organizacionales orientadas a fortalecer los controles de acceso, reducir el riesgo de fuga de información y asegurar el cumplimiento normativo en el marco de los estándares aplicables.

Este proyecto concluye con la entrega de una matriz de brechas, un plan de implementación de controles compensatorios y un presupuesto estimado, que servirán como base para la toma de decisiones por parte de la Alta Dirección y los equipos responsables de seguridad de la información.

Glosario

Circular Externa 029 de 2014. Normativa de la Superintendencia Financiera de Colombia que establece requisitos de seguridad de la información para entidades vigiladas.

Controles Compensatorios. Medidas alternativas que se implementan cuando los controles principales no están disponibles o son insuficientes.

Controles de Acceso Lógico. Mecanismos que regulan el acceso a sistemas y archivos digitales, incluyendo autenticación, autorización y trazabilidad.

DLP. Data Loss Prevention (Prevención de Pérdida de Datos, por sus siglas en inglés) es un conjunto de tecnologías, políticas y procesos diseñados para evitar que información sensible salga de la organización de forma no autorizada, ya sea por accidente o de manera maliciosa.

Dueño de la Información. Persona responsable de autorizar el acceso, definir el uso y proteger la información bajo su custodia.

IAM. Identity and Access Management (Gestión de Acceso e Identidades, por sus siglas en inglés) es el conjunto de tecnologías y procesos que permiten gestionar identidades digitales y controlar el acceso a recursos de forma segura.

ISO/IEC 27001:2022. Norma internacional que establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

MFA. Multi-Factor Authentication (Autenticación de Múltiple Factor, por sus siglas en inglés) es un mecanismo de seguridad que requiere que el usuario proporcione dos o más factores de verificación para acceder a un sistema, aplicación o recurso.

PAM. Privileged Access Management (Gestión de Accesos Privilegiados, por siglas en inglés)

es un conjunto de políticas, procesos y tecnologías diseñadas para controlar, monitorear y asegurar el uso de cuentas con privilegios elevados dentro de una organización.

PCI. Payment Card Industry (Industria de las Tarjetas de Pago, por sus siglas en inglés) es toda información de tarjetas de pago, como número de tarjeta, CVV, fecha de expiración, que debe ser protegida según el estándar PCI DSS.

PCI DSS v4.0.1. Payment Card Industry Data Security Standard (Estandar de Seguridad de Datos de la Industria de las Tarjetas de Pago, por sus siglas en inglés) orientada para organizaciones que procesan datos de tarjetas de pago, con requisitos técnicos y operativos.

PII. Personally Identifiable Information (Información de Identificación Personal, por sus siglas en inglés) permite identificar a una persona, como nombre, número de identificación, dirección, correo electrónico, entre otros.

PTF. Program Temporary Fix (Solución Temporal de Programa, por sus siglas en inglés) es un parche o actualización que IBM proporciona para corregir errores, mejorar funcionalidades o cerrar vulnerabilidades de seguridad en el sistema operativo o en sus componentes.

RBAC. Role-Based Access Control (Control de Acceso Basado en Roles) es un modelo de gestión de acceso que asigna permisos a los usuarios en función de los roles que desempeñan dentro de una organización, en lugar de asignar permisos directamente a cada usuario individual.

SIEM. Security Information and Event Management (Gestión de Información y Eventos de Seguridad, por sus siglas en inglés) es una herramienta que permite recolectar, analizar y correlacionar eventos de seguridad en tiempo real para detectar amenazas.

SoD. Segregation of Duties (Segregación de Funciones, por sus siglas en inglés) es el principio de seguridad que busca evitar que una misma persona tenga control total sobre un proceso crítico, reduciendo el riesgo de fraude o error.

Stakeholder. (Grupo de involucrados o partes interesadas, por sus siglas en inglés) es cualquier persona, grupo u organización que tiene un interés directo o indirecto en un proyecto, empresa o iniciativa, y que puede afectar o verse afectado por sus resultados.

Trazabilidad. Capacidad de registrar y seguir las acciones realizadas por los usuarios en los sistemas, especialmente sobre información sensible.

UEBA. User and Entity Behavior Analytics (Análisis del Comportamiento de Usuarios y Entidades, por sus siglas en inglés). Es una tecnología de ciberseguridad que utiliza técnicas de machine learning, análisis estadístico y modelado del comportamiento para detectar actividades anómalas o sospechosas dentro de una red o sistema.

Referencias

Circular Básica C.E 029. (2014). https://www.superfinanciera.gov.co/publicaciones/10083443/normativanormativa-generalcircular-basica-juridica-ce-10083443/: Superintendecia Financiera.

ISO 27005. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad.* https://www.iso.org/standard/80585.html .

NIST. (2010). *NIST SP 800-122 - Guía para proteger la confidencialidad de la información de identificación personal (PII).* https://csrc.nist.gov/publications/detail/sp/800-122/final.

PCI. (2023). *Security Standards Council. Payment Card Industry Data Security Standard – Requirements and Security Assessment Procedures, Version 4.0.1.* https://www.pcisecuritystandards.org.

Peters, S. (2025). *ISO 27002:2022 – Control 5.34 – Privacidad y Protección de la PII.* https://es.isms.online/iso-27002/control-5-34-privacy-and-protection-of-pii/.

Revista Seguridad 360. (2024). *Sistemas de Control de Acceso para el Sector Financiero: Seguridad y Eficiencia en la Gestión de Datos.* https://revistaseguridad360.com/noticias/control-de-accesos/sistemas-de-control-de-acceso-para-el-sector-financiero-seguridad-y-eficiencia-en-la-gestion-de-datos/.

Rojas, O. (2023). *Estado del arte de la IA en control de acceso, panorama actual, avances más recientes y tendencias.* https://www.tecnoseguro.com/analisis/pro/acceso-ia-tecnologia-tendencias-2.

Rouse, M. (2021). *Logical access control. TechTarget.* Texas.

SGS Academy. (2023). *ISO/IEC 27005:2022 - Seguridad de la información,ciberseguridad y protección de la privacidad.* https://campusvirtual.cenoeder.com/wp-content/uploads/2025/05/Norma-ISO-27005_2022-SGS.pdf.

SO/IEC 27001. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.*