Sistema de Control Interno y gestión de riesgos

Administración de riesgos y continuidad

Jorge Arturo Lara
Vicepresidente Riesgo Integral y Cumplimiento

SARE

Sistema de **A**dministración de **R**iesgos de **E**ntidades exceptuadas del SIAR

El Sistema de Administración de Riesgo Operacional se encuentra enmarcado de acuerdo a lo previsto en la circular básica contable 100 de 1995 en el capítulo XXXII de la Superintendencia Financiera de Colombia. Teniendo en cuenta las etapas de identificación, medición, monitoreo y control que se pueden reflejar en las políticas y la metodología que tiene oficializadas Credibanco.

En 2024, se realizó la evaluación transversal de riesgos y controles, encontrando que el perfil de riesgo de la organización se encuentra dentro de los parámetros establecidos, siendo este monitoreado periódicamente. El perfil de riesgos fue presentado ante la Junta Directiva para su seguimiento y pronunciamiento semestralmente, asi como el monitoreo y cumplimiento del mismo de manera trimestral.

Así mismo, los Riesgos Financieros son administrados bajo el conjunto de normas documentadas en la política del sistema de administración de riesgos financieros de los participantes, aprobado por Junta Directiva. El objetivo es proteger a Credibanco asociados y participantes, por las contingencias de pérdida ante la ocurrencia de hechos que afecten el pago de operaciones del sistema, las cuales provienen del proceso de compensación nacional e internacional. También se derivan todas las obligaciones a cargo de las entidades asociadas, de las otras entidades participantes y Credibanco.

Administración de riesgos y continuidad

SGCN
Sistema de Gestión de Continuidad del Negocio

Desde la Dirección de Riesgos y Continuidad de Negocio se desarrolló durante el 2024 el mantenimiento y mejora de todos los componentes del Sistema de Gestión de Continuidad de Negocio, el cual, permite a CredibanCo consolidarse como una compañía resiliente y con capacidad para actuar frente a escenarios adversos que impacten el normal desarrollo de las operaciones y servicios hacia nuestros clientes, esto basado en la implementación de las mejores prácticas del DRII y el estándar ISO 22301:2019.

El proceso de mantenimiento y mejora estuvo enfocado en los siguientes pilares del Sistema de Gestión:

- Análisis de Impacto al Negocio (BIA)
- Análisis de Riesgos
- Estrategias de Continuidad de Negocio
- Plan de Continuidad Organizacional
- Planes de Contingencia Operativos
- Plan de Recuperación de Desastres
- Plan de Gestión de Crisis
- Plan de Comunicaciones CN
- Plan de Atención a Emergencias
- Plan de Pruebas y Ejercicios
- Seguimiento a Proveedores Críticos

Dentro de los hitos más representativos del Sistema de Gestión de Continuidad para el 2024 se relacionan los siguientes.

Modelo de gobierno
Se fortaleció el equipo con la incorporación de un Líder BCP y Líder DRP.

Gestión de crisis y comunicaciones
Se reestructuró el esquema de Gestión de incidentes, atención de crisis y el Protocolo de comunicaciones internas y externas a todos los stackeholders.

BCP/DRP
Con apoyo de consultoría externa, se mejoraron las políticas y procedimientos de recuperación operativa y tecnológica.

SARLAFT

Alcance del SARLAFT

Sistema de administración de riesgos de lavado de activos, financiación del terrorismo y de la proliferación de armas de destrucción masiva

Actividades realizadas dentro el SARLAFT durante el 2024:

Gestión de Cumplimiento

1. Listas Internacionales vinculantes para Colombia: Revisadas en total 1572 actualizaciones sin novedades para la Compañía.
2. Capacitaciones: Se desarrollaron los programas de inducción corporativa y anual llegando al 100% de cumplimiento, así mismo para los terceros no empleados y focalizadas (UIAF).
3. Monitoreo y Análisis: Se adelantaron los análisis correspondientes a los alertamientos generados por los diferentes modelos estadísticos aplicados.
4. Mejoras: Frente al perfil de riesgo, tableros de control y rutas de modeler
5. Reportes y Requerimientos: Se enviaron dentro de los tiempos establecidos y a las instancias correspondientes (UIAF,FISCALIA GENERAL DE LA NACIÓN Y SUPERFINANCIERA).

Gestión de Riesgo

1. Perfil de Riesgo: El riesgo residual se mantuvo calificado en BAJO
2. Controles: Se aplicaron los controles pertinentes para la mitigación de las causas generadoras del riesgo LAFTPADM.
3. Mecanismos e Instrumentos: Se atendieron al 100% cada uno de los componentes que los conforman

Trimestralmente y en cumplimiento de lo establecido en la normatividad frente al SARLAFT, la Oficial de Cumplimiento de Credibanco, presentó sus informes de gestión a la Junta Directiva.
Los órganos de control internos y externos adelantaron sus evaluaciones al SARLAFT, sin evidenciar incumplimientos que afectarán a la compañía.
Todo lo anterior en cumplimiento de lo establecido en la Circular Básica Jurídica Parte I, Título IV,Capítulo IV expedida por la Superintendencia Financiera de Colombia, aplicable a Credibanco S.A como entidad vigilada por esta.

POLÍTICA DE TOLERANCIA CERO: Durante el año se atendieron los lineamientos allí establecidos y se dieron los tratamientos a las denuncias recibidas.

Seguridad de la Información y Ciberseguridad

Durante el 2024 CredibanCo focalizó esfuerzos encaminados en el mejoramiento continuo en su sistema de gestión de Seguridad de la información y Ciberseguridad desde los frentes relacionados a continuación, siguiendo los lineamientos de la regulación local y las prácticas de normatividad de industria tales como PCI DSS v4.0.1, PCI PIN Security v3.1, ISO 27001, ISO 27032, ISO27035 e ISO27103:

- Políticas y directrices de seguridad de la información y ciberseguridad.
- Gestión activa de riesgos en activos de información.
- Seguridad en el acceso físico y lógico.
- Adquisición, desarrollo e implementación de controles de seguridad.
- Gestión de seguridad de la información en la operación.
- Gestión de incidentes de seguridad de la información.
- Monitoreo de ciberseguridad.
- Seguridad perimetral y red.
- Seguridad en plataformas On premise y Cloud.
- Seguridad en el uso de tecnologías emergentes.
- Protección en estación de trabajo y móviles.
- Protección usuario final.

De igual manera, desde el frente de monitoreo de Ciberseguridad y monitoreo de Marca, en 2024 se lograron identificar, analizar y contener alrededor de 200 millones de ciberataques los cuales estaban dirigidos a la infraestructura, servicios y/o aplicaciones de nuestro negocio. Lo anterior permitió mitigar la materialización de riesgos cibernéticos e impactos sobre los datos de nuestra organización, así como los datos de nuestros clientes.

Desde el frente de sostenibilidad, donde se evalúan indicadores asociados a los pilares de i) Ciberseguridad y Cibercrimen, ii) Protección y privacidad de la información y iii) Confianza, CredibanCo logró un cumplimiento del **91%** al cierre de 2024, permitiendo demostrar que el ecosistema de ciberseguridad y ciberdefensa cuenta con procesos robustos, sistematizados y con un alto grado de institucionalización de las Políticas de Seguridad de la Información y Ciberseguridad.

Control interno

Martha Rueda
Auditora interna

Actividades realizadas **Comité de Auditoría**

No se detectaron deficiencias materiales que afectaron los estados financieros y el control interno

Temas de Auditoría

- Informe Revisor Fiscal
- Seguimiento gestión de acciones (Junta, Comité, Mandates)
- Resultados del indicador
- Revisión y aprobación estrategia y plan auditoría interna.
- Revisión estados financieros y temas tributarios.
- Seguimiento recomendaciones visita Extra Situ SPBV.
- Revisión y aprobación de las políticas de control Interno (CE008/2023).
- Revisión de informes de compras y procesos judiciales

Temas Riesgos

- Revisión Perfil de riesgos
- Aprobación y seguimiento Apetito de Riesgo
- Análisis Cuenta de riesgo operacional
- Revisión y aprobación de manual de Riesgo operativo
- Informe de fraude
- Revisión riesgo de contraparte
- Seguimiento Resultados certificaciones PCI DSS, PCI PIN, ISAE 3402.

Control interno

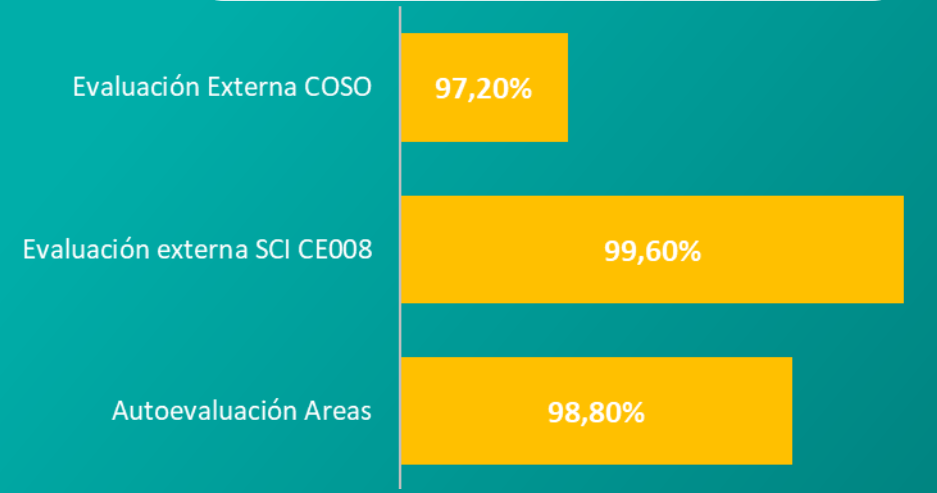
Recomendaciones entes de control

Son gestionadas por cada área responsable y seguimiento por Auditoría Interna, entre las más relevantes gestionadas durante el 2024 se encuentran:

- Mejoras identificadas en la evaluación de continuidad del negocio.
- Gestión de los riesgos asociados al uso de tecnologías emergentes y la forma en que mitigan las ciberamenazas avanzadas asociadas al uso de nuevas tecnologías.
- Resultado inspección Extra Situ SFC al SPBV.

Informe de evaluación
Sistema de Control Interno

Cumplimiento 96,4% - Nivel Optimizado

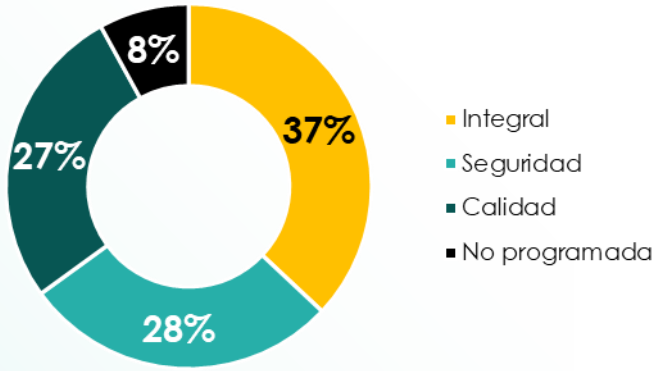


Elementos:

- Revisión y aprobación de las políticas del SCI (CE08/2023 SFC).
- Cierre de brechas pendientes (hallazgos Auditorías internas, externas o eventos de riesgo).
- Evaluación de Control Interno por la Revisoría Fiscal.
- Revisión de la administración de riesgos SARE y SARLAFT por parte de la Auditoría Interna y la Revisoría Fiscal.

Control interno

Auditoría interna



Alcance Auditorías
71 revisiones
100% ejecución

- Revisión de cumplimiento de procesos y políticas
- Cumplimiento de las disposiciones normativas aplicables
- Evaluación de sistemas de información
- Gestión de riesgos y efectividad de controles
- Seguimiento cierre de hallazgos

No se presentaron limitaciones ni se vio comprometida la independencia de la Auditoría Interna.

Recursos Auditoría: Auditor Interno y 6 auditores (Sistemas, Operativo y Financiero)

Protección de Datos Personales

Yenny Sotelo
Secretaria General

En Credibanco contamos con una Política de Protección y Tratamiento de Datos Personales en cuyo contenido se encuentra la transferencia nacional e internacional de datos personales, uso de los datos, finalidades, así como una serie de obligaciones que la compañía y sus colaboradores deben cumplir al momento de actuar en calidad de responsables o encargados de los datos.

Gestionamos la exposición de los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad sobre los datos corporativos y de nuestros grupos de interés, por medio de metodologías enfocadas en la revisión y fortalecimiento continuo de controles sobre la infraestructura administrativa y tecnológica de la organización.

Lo anterior, nos ha permitido alcanzar una mayor madurez del sistema de gestión de seguridad de la información y ciberseguridad, habilitando mecanismos para identificar y atender oportunamente ataques dirigidos a nuestra infraestructura tecnológica y marca, logrando una capacidad de contención efectiva.

Como evidencia de aplicación y eficiencia de nuestros controles y políticas para el debido tratamiento de datos personales, damos a conocer que, en el año 2024 no fuimos requeridos por la autoridad competente para el pago de multas o sanciones por la violación de datos personales, lo cual, nos convierte en una compañía que busca garantizar la confianza y seguridad de los titulares que comparten sus datos con nosotros.

Ley aplicable	Descripción
Decreto 2555 de 2010 y las demás normas que lo modifiquen o complementen	Normas en materia del sector financiero, asegurador y del mercado de valores y se dictan otras disposiciones.
Ley 1340 de 2009	Protección de la competencia.
La ley 1581 del 2012 y ley 1266 de 2008	Protección de datos personales
Resolución 3501 de 2011 de la Comisión de Regulación de Comunicaciones	Se determinan las condiciones de acceso a las redes de telecomunicaciones.
Circular Básica Jurídica 029 de 2014 SFC	Aspectos aplicables a entidades vigiladas por la Superintendencia Financiera de Colombia.
Circular Externa 052 de 2007 SFC	Manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.
Ley 1735 de 21 de octubre de 2014 y Decretos Reglamentarios	Sociedades Especializadas en depósitos y pagos electrónicos
Decreto 1076 de 2015 y las demás normas que lo modifiquen o complementen	Decreto Único Reglamentario del Sector Ambiente y Desarrollo Sostenible.
Estatuto Tributario y Ley de Crecimiento Económico	Disposiciones de los impuestos administrados por la Dirección General de Impuestos Naciones.
Decreto 2443 de 2018	Inversión en sociedades FINTECH con objeto exclusivo.
Resolución 17 de 2020 DIAN	Procedimiento para los prestadores de servicios electrónicos o digitales desde el exterior que se acojan voluntariamente al sistema alternativo de pago del impuesto a través de la retención en la fuente a título de impuesto sobre las ventas (IVA).
Resolución 019 de 2016 y demás resoluciones/decretos que lo complementen	Regulación del funcionamiento de la factura electrónica.
Circulares Externas 005 de 2019, 006 de 2019, 029 de 2019, 025 de 2020, 027 de 2020, 005 de 2021, 020 de 2021 SFC	Uso de servicios de computación en la nube; Seguridad y calidad para realización de operaciones mediante códigos QR; Requerimientos mínimos de seguridad y calidad para la realización de operaciones y acceso e información al consumidor financiero y uso de factores biométricos; Riesgo Operacional; Administración del riesgo de lavado de activos y de financiación del terrorismo; Registro de Adquirentes No Vigilados- RANV; Actividades que desarrollan las entidades vigiladas en los Sistemas de Pago de Bajo Valor.
Decreto 1297 de 2022, Art 89 Plan Nacional de Desarrollo 2022-2026, Circular Externa 004 de 2024 SFC	Open Data (Datos Abiertos) / Open Finance
Circular Externa 008 de 2023 SFC	Sistema de Control Interno
Art. 104 del Plan Nacional de Desarrollo 2022-2026; Resolución Externa 6 del 2023 Circular Externa DSP 465 2023, Circular Externa DSP 471 MOL 2024, Circular Externa 470 DICE 2024 (Banco de la República)	Sistemas de Pago de Bajo Valor Inmediato.
La ley 1480 de 2011 y Decretos Reglamentarios	Estatuto de Protección al Consumidor.

Propiedad intelectual y derechos de autor

De conformidad con lo dispuesto en el artículo 47 de la Ley 222 de 1995, modificada por la Ley 603 del 27 de julio de 2000, la administración de Credibanco informa que, los bienes protegidos por derechos de autor y de propiedad intelectual son utilizados de manera legal, en cumplimiento de las normas respectivas y con las debidas autorizaciones otorgadas.

Los vínculos de Credibanco con los diferentes grupos de interés se encuentran alineados con el marco normativo e incorporan cláusulas contractuales, requisitos o condiciones que los desarrollan, reforzando dicha normativa e incluyendo mecanismos para resolver eventuales controversias al respecto.

Operaciones celebradas con vinculados económicos

Estas operaciones están siendo reveladas en la nota No.41 de los Estados Financieros.

Nota sobre la Libre circulación de Facturas

Dando cumplimiento a lo indicado en el artículo 87, parágrafo 2 de la Ley 1676 de 2013, y en concordancia con el parágrafo primero del artículo 778 del código de comercio, se deja constancia que no se ha entorpecido, ni se han puesto obstáculos a la libre circulación de las facturas emitidas por los vendedores o proveedores. Tampoco ha existido cuestionamientos para el año 2024 por parte de algún proveedor sobre alguna limitación de la norma para Credibanco S.A.