Itaú CorpBanca Colombia S.A.
Informe del Sistema de Control Interno año 2019

Objetivo del Trabajo

El objetivo es informar sobre el funcionamiento del Sistema de Control Interno (en adelante SCI) en Itaú CorpBanca Colombia S.A. (el Banco) conforme a los criterios de la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia.

Las conclusiones aquí manifestadas sobre la efectividad del SCI están basadas en los resultados obtenidos en los trabajos de auditoría interna abordados en la planificación del año 2019 y que han sido concluidos al corte del 6 de diciembre de 2019 y presentados al Comité de Auditoría.

Resumen

El SCI del Banco considera los elementos: Ambiente de Control, Evaluación del Riesgo, Actividades de Control, Información y Comunicación, Sistemas Informáticos, Monitoreo y Evaluaciones Independientes, conforme a los criterios establecidos en la norma.

El SCI se encuentra alineado con los estándares internacionales del Committee of Sponsoring Organizations of the Treadeway Commission (COSO), orientado a los objetivos de control sobre estrategia corporativa, efectividad, eficiencia de las operaciones, confiabilidad de los reportes financieros y cumplimiento de las leyes y regulaciones aplicables.

Adicionalmente, el Banco en su SCI integra los principios definidos por la norma como son: El Autocontrol, la Autorregulación y la Autogestión.

A continuación el grado de cumplimiento respecto a los elementos del Sistema de Control Interno:

	Aspectos	Evaluación
I.	Ambiente de Control.	Cumple
II.	Evaluación de Riesgos.	Cumple
III.	Actividades de Control.	Cumple parcialmente
IV.	Información y comunicación.	Cumple
V.	Sistemas informáticos.	Cumple parcialmente
VI.	Monitoreo.	Cumple parcialmente
VII.	Evaluaciones independientes.	Cumple

Cumple | Cumple parcialmente | No cumple

Atentamente,

Marcio G. Palestra
Vicepresidente de Auditoría

Ariel Florido M.
Gerente de Auditoria

1. Elementos del Sistema de Control Interno

Presentamos las conclusiones sobre la situación de Control Interno del Banco durante el año 2019, con base en los resultados de los trabajos de auditoría realizados en este período y en las medidas adoptadas por la entidad para subsanar los hallazgos identificados:

- El Código de Buen Gobierno, el Modelo Corporativo de Ética, el Código de Conducta en el Mercado de Valores, el manual de Prevención de Lavado de Activos y Financiación del Terrorismo, y los demás manuales que conforman el Sistema (Operacionales, Liquidez, Riesgo de Contraparte y Atención al Consumidor Financiero), contienen los principios básicos de actuación que rigen a la entidad.

- El Banco cuenta con políticas de gestión humana y procedimientos de selección, inducción, formación, capacitación, sistemas de compensación y evaluación del desempeño, debidamente documentados.

- Se mantiene una Gobierno Corporativo adecuado, estando definidos los niveles de autoridad y responsabilidad para los entes que soportan el Sistema de Control Interno como lo son: La Junta Directiva, el Comité de Auditoría, la Auditoría Interna y la Revisoría Fiscal.

- En cuanto a la Gestión de Riesgos y en cumplimiento de las instrucciones impartidas por la normativa sobre la materia, el Banco ha implementado todos los Sistemas de Administración de Riesgos considerando los elementos y las etapas de los mismos y conforme a los requerimientos del Regulador, los cuales son objeto de evaluación por parte de la Auditoría Interna.

- Se han establecido políticas, manuales y procedimientos (con controles aplicables) debidamente documentados con acceso a toda la Entidad.

- Las políticas y procedimientos relacionados con la seguridad de la información están documentadas en el Manual General de Políticas y Normas de Seguridad Informática y en los subprocesos del Banco.

- En cuanto a la comunicación, el Banco tiene diseñadas políticas para el manejo de la información al interior y al exterior, esta labor es desarrollada por el área de comunicaciones, bajo el modelo del Grupo Financiero, quien se encarga de crear, desarrollar y ejecutar la estrategia de comunicación.

- Por medio del monitoreo realizado en las diferentes etapas de los procesos se valora la calidad y desempeño del sistema y se ejecutan las acciones necesarias para su mejoramiento.

Con base en lo señalado en este informe, se concluye que el Banco, tiene una estructura adecuada de control interno, dando una seguridad razonable en la consecución de los objetivos relativos a las operaciones, a la información y al cumplimiento. No obstante, se observan oportunidades de mejora relacionadas con los siguientes elementos en cuanto al ambiente de control, sistemas informáticos y el monitoreo:

Actividades de Control: En la evaluación de los procesos del producto leasing se identificó que en general existen debilidades en la administración de bienes, actualización de avalúos y aplicación de prepagos. En el proceso de ética y conducta se evidenciaron deficiencias en la recepción y tratamiento de las denuncias recibidas por la página web, al igual que debilidades en el proceso de recepción, gestión, seguimiento y monitoreo de las denuncias. En el Proceso de Cuentas de Depósito se eviedenció incumplimiento al control a cargo de las oficinas sobre transferencia de fondos entre cuentas del mismo cliente.

Sistemas informáticos: En la Prueba de intrusión APP´s se identificaron 9 vulnerabilidades, las cuales fueron clasificadas una como alta, 2 medias y 6 bajas, dichas vulnerabilidades tienen como principales causas, inadecuado desarrollo de la aplicación por procesos no seguros, la falta de mecanismos de defensa en los formularios (campos para registrar datos) para obtención de información de clientes, como también deficiencias en la APP que la hacen susceptible a alteración de parámetros, situaciones que exponen al Banco principalmente al riesgo de captura de información de clientes para realizar un ataque; en la prueba de intrusión al Portal ejecutada fue tipo Blackbox (no se tenía información de la infraestructura), identificando dos puntos con vulnerabilidades clasificadas como alta (1) y como baja (1); dichas vulnerabilidades tienen como principales causas la falta de mecanismos de defensa configurados correctamente para

ofuscar información de la infraestructura tecnológica. En el proyecto de Seguridad (Prisma) se evidenciaron fallas en el control del inventario sobre la infraestructura de TI y escaneo de vulnerabilidades, al igual que debilidad en el aseguramiento de los estándares de seguridad y reportes al comité.

Monitoreo: En el Proceso de reportes a Centrales de Riesgos falta de controles en el proceso de generación y aseguramiento de los mismos, lo que ocasiona incumplimiento normativo. Se identificaron errores en el registro contable de Bienes Recibidos en Dación de Pago, Restituidos y Adjudicaciones Judiciales por inadecuada identificación. Respecto al cumplimiento de la ley FATCA y CRS evidenciamos cuentas no reportados a la DIAN sujetas a la Ley, al igual que falta de segregación de funciones en el proceso, e insuficiencia de controles de integridad de la información. En los procesos del Producto Libranza se evidenciaron debilidades en el proceso de vinculación y monitoreo de convenios. Debilidades en la ejecución de controles y falta de oportunidad en el proceso de conciliación Bancaria. Al igual que deficiencias en la identificación, aprobación, administración, publicación y actualización de contratos estandarizados.

2. Trabajos de Auditoría Interna

El plan anual de auditoría 2019 consideró 45 trabajos, con cobertura a los riesgos de cumplimiento, regulatorio, financiero, contable y de gestión, operativo, crédito y tecnológico; éste fue aprobado por el Comité de Auditoría el 13 de diciembre de 2018 (acta 154) y ratificado por la Junta Directiva el 24 de enero de 2019 (Acta 3696).

La planificación se ha venido desarrollando de acuerdo con los alcances previstos; sin embargo, se realizaron las siguientes modificaciones, cambios que fueron aprobados por el Comité de Auditoría el 29 de julio de 2019 (acta 161).

- Postergación de los trabajos relacionados con selección y contratación de proveedores y proceso de crédito Banca Minorista, a realizarse en el año 2020.
- Modificación al alcance del trabajo del Sistema Administración Riesgos Lavado de Activos y Financiación del Terrorismo (SARLAFT).
- Adición de los siguientes trabajos:
  - Proceso de elaboración del presupuesto y contrato de metas de la Tesorería - Itaú CorpBanca Colombia.
  - FATCA - Itaú CorpBanca Colombia S.A. y Filiales (Colombia y Panamá).
  - Procesos Operativos Red de Sucursales.
  - Resolución BACEN 4062 - Itaú CorpBanca Colombia.

Conforme con la ejecución del plan de auditoría del año 2019 y de acuerdo al avance a la fecha de emisión del presente informe, se han obtenido los siguientes resultados por niveles de riesgo (ver detalle Anexo I):

Tipo de Auditoria	Calificación				Total
	Elevado	Moderado	Satisfactorio	Sin Calificación	
Crédito	1	5	1	-	7
Financiero	-	3	1	1	5
Gestión	-	6	-	-	6
Operacional	1	4	1	2	8
Tecnológico	2	2	-	1	5
Total	4	20	3	4	31

Los trabajos que están pendientes de concluir son:

- Proceso de Crédito Banca Mayorista.
- Proceso del Producto Hipotecario y Leasing Habitacional.
- Gestión de Monitoreo y Cobranza de Crédito Banca Minorista.
- Sistema de Administración de Riesgo de Mercado (SARM) - Modelo Interno y Regulatorio.

- Sistema de Atención al Consumidor (SAC) II Semestre.
- Procesos Contables.
- Procesos Operativos Red de Sucursales
- Base Line.
- Auditoría Salas Digitales.

Adicionalmente, la Auditoría Interna realizó seguimiento a los siguientes proyectos relevantes del Banco:

- Seguimiento al proyecto Cajeros Automáticos – Itaú CorpBanca Colombia S.A.
- Falla Incidente Telecomunicaciones - Superintendencia Financiera de Colombia.

Indicar que las observaciones de control interno, identificadas por la Auditoría Interna en el desarrollo del plan anual han sido comunicadas de manera oportuna a las partes responsables de tomar los correctivos y se han establecido fechas para su regularización, las cuales han sido atendidas en tiempo y forma por el Banco. Adicionalmente, éstas han sido puestas en conocimiento de la Alta Dirección del Banco, el Comité de Auditoría y la Junta Directiva, cuando fue necesario para el caso de ésta última.

Al corte de este informe, en el año 2019 se han levantado 113 puntos de auditoría con el siguiente estado:

Tipo de auditoría	Calificación						
	Elevado		Moderado		Moderado Sox		Bajo*
	Formulados	Implantados	Formulados	Implantados	Formulados	Implantados	Formulados
Crédito	6	1	13	4	1	1	4
Financiero	-	-	13	-	1	-	2
Gestión	4	2	17	-	-	-	3
Operacional	6	3	23	1	4	-	4
Tecnológico	3	1	5	-	-	-	4

* La implementación de los planes de acción calificados con Riesgo Bajo se revisan en la siguiente auditoria.

Es importante señalar que los puntos que no han sido implantados, se encuentran en plazo conforme a la política.

Por otro lado, y conforme a la política interna, el Banco solicitó ante las instancias correspondientes autorización para tratar nueve puntos como estructurantes, en detalle:

Auditoría	Descripción	Nivel de Riesgo	Estado
Seguridad de la información y Continuidad de Negocio (Salas Digitales)	Aplicaciones no administradas por el área de Control de Acceso.	Moderado	En Plazo
Baseline de Seguridad	Equipos con acceso a modificaciones de arranque sin contraseña.	Moderado	En Plazo
Proceso de Bienes Recibidos en Dación de Pago, Restituidos y Adjudicaciones Judiciales	Errores en el registro contable de Bienes Recibidos en Dación de Pago, Restituidos y Adjudicaciones Judiciales por inadecuada identificación.	Elevado	En Plazo
Seguridad de la Información y Continuidad del Negocio	Ausencia de la definición de un procedimiento sobre la gestión de usuarios genéricos/funcionales, fallas en la ejecución de los controles relacionados con la gestión y certificación de usuarios y falta de una adecuada concientización de la certificación de usuarios por los dueños de los procesos.	Elevado	En Plazo
	Sistemas Operativos instalados en los servidores, laptops y desktops y Base de Datos con tecnologías obsoletas en la infraestructura.	Elevado	En Plazo

Auditoría	Descripción	Nivel de Riesgo	Estado
Proceso de Gestión de los Canales Electrónicos (Internet Banking) - Itaú CorpBanca Colombia	Portal sin factores de autenticación dinámicos para el ingreso y para la ejecución de transacciones.	Moderado	En Plazo
	Servidores del front que soportan el portal persona natural se encuentran alojados en la red interna. No se evidenciaron firewall de aplicación (WAF) instalados para la protección de servidores web que prevenga la inyección de código malicioso u objetos maliciosos, que afecten la seguridad de la operación. Información de clientes en la red interna no cuenta con controles de cifrado tanto en canal como su contenido.	Elevado	En Plazo
Cybersecurity	Exposición de información confidencial por la ejecución de ataques de fuerza bruta. Suplantación del portal transaccional por duplicación total del contenido de la página web. Perdida de información por simultaneidad de sesiones a causa de la no activación de la sesión de Cookies. Exposición de los componentes de hardware del portal generando un análisis de vulnerabilidades de los componentes / denegación del servicio.	Moderado	En Plazo
	Vulnerabilidades en Internet Banking que afectan la seguridad y la disponibilidad del portal transaccional, se identificaron riesgos de posible denegación de servicios y la posibilidad de una inyección de sentencias SQL al motor de BD del portal transaccional.	Elevado	En Plazo

3. Entes de Control Externo

Durante el 2019 se recibieron 2 visitas del Autorregulador del Mercado de Valores de Colombia, como resultado de la inspección se obtuvieron los siguientes informes:

- Informe visita de Supervisión AMV dirigido a Itaú CorpBanca Colombia con 3 incidencias, las cuales ya fueron implantadas.
- En relación con la Superfinanciera de Colombia, en el año 2019 se recibieron diversas inspecciones relacionadas con los siguientes aspectos:
    - Visita con foco en: Cuentas abandonadas e inactivas, Ley de Costos, Tarifas y tasas de servicios financieros, Gravamen de movimientos financieros – GMF.
    - Visita con el ánimo de revisar Actividad Significativa (AS) de Banca Mayorista, y Pyme y realizar un seguimiento a la gestión de liquidez y al fortalecimiento de la función de supervisión de Gestión de Riesgos.

- La Revisoría Fiscal para el Banco, no ha levantado recomendaciones frente al SCI durante el año 2019.

Anexo I

Área	Nombre del trabajo	Calificación
Crédito	Proceso del Producto de Leasing de Banca Mayorista	Elevado
Operativo	FATCA	Elevado
Tecnológico	Ciberseguridad Prueba de intrusión APP´s	Elevado
Tecnológico	Aseguramiento proyecto de Seguridad (Prisma)	Elevado
Crédito	Proceso del Producto Libranza	Moderado
Crédito	Control y Gestión de Garantías y Pagarés	Moderado
Crédito	Gestión de Monitoreo y Cobranza de Crédito Banca Mayorista	Moderado
Crédito	Proceso de Reporte a Centrales de Riesgos	Moderado
Crédito	Proceso de Bienes Recibidos en Dación de Pago	Moderado
Financiero	Sistema de Administración de Riesgo de Liquidez (SARL) Modelo Interno y Regulatorio	Moderado
Financiero	Gestión de Capital y Margen de Solvencia	Moderado
Financiero	Procesos de la Tesorería (Front Office, Back Office y Riesgo de Crédito)	Moderado
Gestión	Sistema de Atención al Consumidor (SAC) I Semestre	Moderado
Gestión	Impuestos	Moderado
Gestión	Ética y Conducta	Moderado
Gestión	Proceso de elaboración, presentación y seguimiento de los resultados de gestión	Moderado
Gestión	Modelo IFRS 9	Moderado
Gestión	Proceso de Conciliaciones Bancarias	Moderado
Operativo	Procesos de Medios de Pago (Tarjetas)	Moderado
Operativo	Proceso de Compensación Electrónica	Moderado
Operativo	Procesos de Cuentas de Depósito	Moderado
Operativo	Proceso de Gestión del Efectivo	Moderado
Tecnológico	SWIFT	Moderado
Tecnológico	Controles Generales De IT e Infraestructura IVR	Moderado
Financiero	Auditoría Volcker Rule	Satisfactorio
Financiero	Clasificación y provisiones de Cartera Minorista	Satisfactorio
Operativo	Sistema de Administración de Riesgo de Operativo (SARO) y Modelo de Control Interno	Satisfactorio
Financiero	Proceso de elaboración del presupuesto y contrato de metas de la Tesorería	Sin Calificación
Operativo	Asesoría Sistema de Administración de Riesgos de Lavado de Activos y Financiación del terrorismo (SARLAFT)	Sin Calificación
Operativo	Sistema de Control Interno SCI	Sin Calificación
Tecnológico	Resolución BACEN 4062	Sin Calificación