INFORME DE GESTIÓN DE RIESGOS

Equifax Centroamérica, S.A de C.V.

2025

I. INTRODUCCIÓN

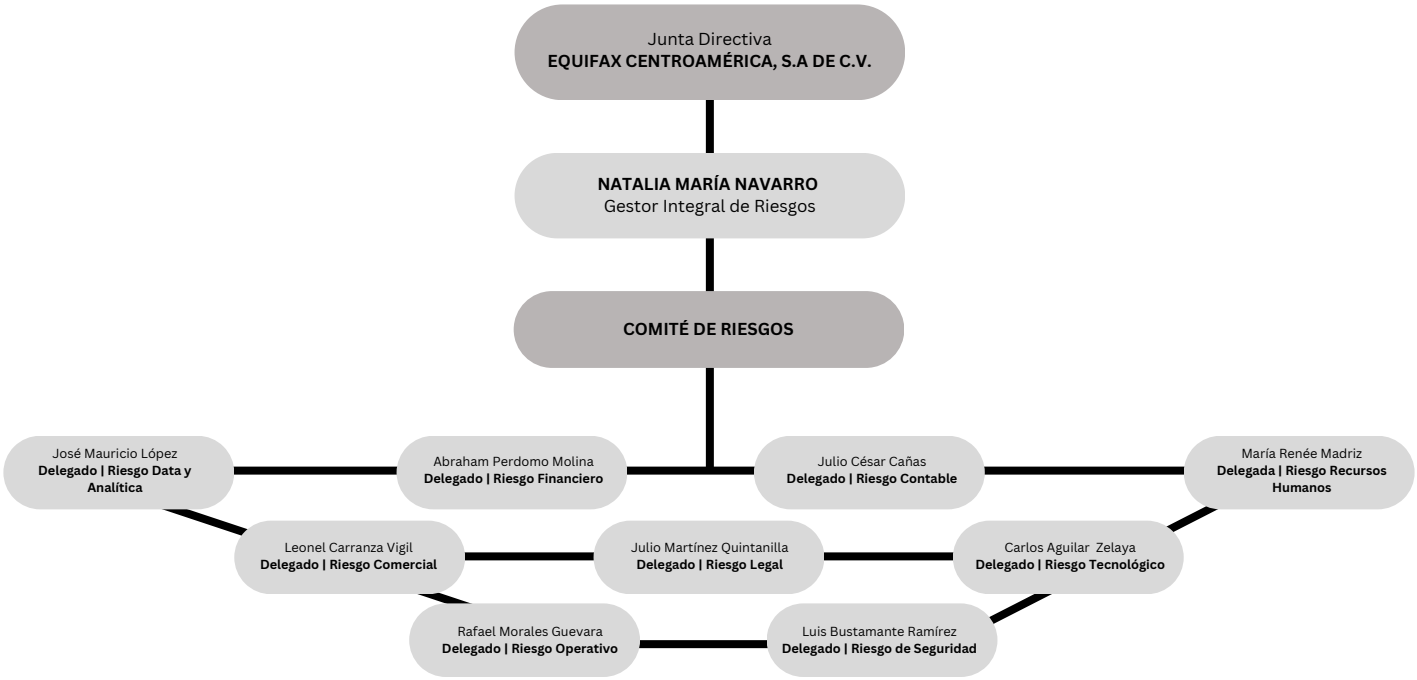
El presente informe de análisis de riesgos tiene como propósito principal examinar las áreas críticas identificadas en la operación de la institución, con el objetivo de evaluar los desafíos y las oportunidades relacionadas con la gestión de riesgos. A través de este análisis, se busca proporcionar una visión integral y estructurada que facilite la toma de decisiones estratégicas orientadas hacia la mitigación de riesgos y el fortalecimiento de las capacidades operativas y regulatorias.

II. ALCANCE

El alcance del análisis abarca las principales áreas funcionales de la institución, como Operaciones, Legal, Continuidad del Negocio, Recursos Humanos, Servicio de Atención al Consumidor y Productos. Cada una de estas áreas ha sido evaluada en función de sus procesos internos, su alineación con las normativas locales y su capacidad para gestionar riesgos potenciales que podrían comprometer la resiliencia y sostenibilidad operativa. En este contexto, se han identificado puntos clave de mejora en planificación, auditoría y comunicación interdepartamental, los cuales son tratados de manera detallada en este informe.

El alcance del análisis abarca las principales áreas funcionales de la institución, como Operaciones, Legal, Continuidad del Negocio, Recursos Humanos, Servicio de Atención al Consumidor y Productos. Cada una de estas áreas ha sido evaluada en función de sus procesos internos, su alineación con las normativas locales y su capacidad para gestionar riesgos potenciales que podrían comprometer la resiliencia y sostenibilidad operativa. En este contexto, se han identificado puntos clave de mejora en planificación, auditoría y comunicación interdepartamental, los cuales son tratados de manera detallada en este informe.

III. ESTRUCTURA ORGANIZATIVA DE GESTIÓN DE RIESGOS



IV. GENERALIDADES

En primer lugar, el área de Operaciones su función principal radica en la consolidación de datos proveniente de agentes económicos, que debe ser procesada y cargada en plazos regulados. Estos plazos, marcados como obligatorios, abarcan la recepción de información durante los primeros diez días calendario y su carga el día quince de cada mes. Aunque este proceso está definido. Se subraya la necesidad de fortalecer los mecanismos de validación de datos y de establecer procedimientos claros para el manejo de retrasos en las cargas reguladas.

El área de Legal, por su parte, se encuentra gestionando un proceso abierto relacionado con un incidente leve de seguridad ocurrido en 2024. Estos factores evidencian la necesidad urgente de consolidar un informe robusto de gestión de riesgos regulatorios que aborde tanto la situación actual como las medidas de mitigación a futuro.

En cuanto a la Continuidad del Negocio, se destaca la existencia de un cuadro de control que organiza políticas y eventos, así como la definición de cuarenta procesos orientados a garantizar la resiliencia empresarial. Sin embargo, en 2024 no se contó con un respaldo total en la nube para contingencias, lo que limita la capacidad de respuesta ante eventos críticos. Se requiere avanzar hacia la implementación de estrategias de respaldo de datos más robustas, incluyendo infraestructura en nube y la adopción de certificaciones en normas de continuidad que garanticen una mayor seguridad operativa.

El análisis del área de Recursos Humanos revela una participación limitada en el diagnóstico y pone de manifiesto diversas carencias en procesos clave. Aunque existe un reglamento interno y políticas de comportamiento, los riesgos asociados a la selección, capacitación, retención y salida de personal reflejan falta de evidencia concreta y de controles documentados adecuados. Aspectos como la firma de documentos clave, la transferencia de conocimiento al salir un empleado crítico y los entrenamientos enfocados en seguridad y código de ética necesitan ser evaluados y fortalecidos para minimizar el impacto de estos riesgos en la operación.

Por otro lado, el Servicio de Atención al Consumidor enfrenta brechas importantes relacionadas con la gestión de usuarios y su comunicación interdepartamental. Además, la ausencia de alertas de control ante intentos fallidos de acceso y la limitada comunicación con el área de Tecnología agravan la vulnerabilidad del área. Implementar mecanismos de supervisión más eficientes y fortalecer los protocolos de auditoría son acciones esenciales para mitigar estos riesgos.

V. IDENTIFICACIÓN DE RIESGOS POR ÁREA

Operaciones: Riesgos asociados con la ausencia de planificación anual y la gestión reactiva de incidentes, lo que afecta la eficiencia y el cumplimiento de plazos regulatorios.

Legal: Vulnerabilidades ante proceso abierto por leve incidente.

Continuidad del Negocio: Limitaciones en la capacidad de respuesta ante emergencias, como la falta de respaldo total en la nube.

Recursos Humanos: Carencias en procesos de selección, capacitación y transferencia de conocimiento, afectando la gestión del talento.

Atención al Consumidor: Dependencia de proveedores.

Los recursos necesarios incluyen herramientas automatizadas de monitoreo de accesos, equipos especializados en auditorías y presupuesto para capacitaciones. El cronograma abarca un periodo inicial de tres meses para diseño y capacitación, seguido de auditorías semestrales de monitoreo.

XV. PRIORIZACIÓN DE RECURSOS PARA CIBERSEGURIDAD Y MANTENIMIENTO TECNOLÓGICO

Proteger la infraestructura tecnológica de la organización frente a riesgos internos y externos es esencial para garantizar la continuidad y sostenibilidad de las operaciones. La ciberseguridad y el mantenimiento tecnológico deben ser abordados como componentes estratégicos prioritarios.

El impacto esperado incluye una reducción significativa de vulnerabilidades frente a ciberataques, la mejora de la confiabilidad de los sistemas operativos y la protección de datos sensibles. Estas acciones incrementan la capacidad de respuesta frente a incidentes y aseguran la estabilidad operativa. Debe incluirse:

1. Realizar un diagnóstico integral que permita identificar puntos críticos en infraestructura tecnológica.

2. Priorizar la asignación de recursos para mantenimiento preventivo y correctivo.

3. Implementar herramientas avanzadas de detección y respuesta a incidentes, optimizando la seguridad proactiva de los sistemas.

Se requiere presupuesto para mejoras tecnológicas, contratación de expertos en ciberseguridad y adquisición de software especializado. El cronograma contempla un periodo inicial de diagnóstico y planificación de dos meses, seguido de una ejecución progresiva durante el resto del año.

XVI. POLÍTICAS Y MECANISMOS PARA LA GESTIÓN DE RIESGOS

Para el cumplimiento y control de la Gestión Integral de Riesgos, se cuenta con las siguientes políticas y mecanismos:

Sistema de Gestión de Riesgos: Basado en Gobierno, Riesgo y Cumplimiento (GRC) está integrado con un enfoque coherente para evaluar y mitigar los riesgos inherentes a la gestión de información crediticia, garantizando al mismo tiempo el cumplimiento normativo y la protección de los datos sensibles.

El Sistema de Gestión de Riesgos se fundamenta en los principios de transparencia, responsabilidad y excelencia operativa. Se presenta una visión general del enfoque estratégico, desarrollo e implementación de su Sistema de Gestión de Riesgos basado en GRC. Se detallan los principales componentes y procesos del sistema.

Además, se resalta el compromiso continuo con la mejora continua y la adaptación proactiva a un entorno empresarial en constante evolución.

✓ **Aprobado** por Junta Directiva a los diecinueve días del mes de marzo de dos mil veinticuatro.

Política de Gestión de Riesgos: La política de riesgos de Equifax abarca la promoción de una cultura de gestión de riesgos entre todos los empleados, la protección de los intereses de accionistas y clientes mediante la identificación y mitigación de riesgos, el cumplimiento con regulaciones financieras y estándares de buenas prácticas, la provisión de información precisa para una toma de decisiones estratégica, la mejora de la eficiencia operativa y la garantía de la continuidad del negocio en situaciones de crisis.

✓ **Aprobado** por Junta Directiva a los diecinueve días del mes de marzo de dos mil veinticuatro.

Mecanismos para la de Gestión de Riesgos: El cual propone un proceso estructurado para la identificación y evaluación de riesgos, que abarca la definición de criterios de riesgo y la priorización de acciones. Este proceso se basa en la implementación de controles adecuados para mitigar los riesgos identificados, con un enfoque en la eficiencia y la efectividad. Además, se establece una asignación clara de responsabilidades y se definen procesos de comunicación y reporte para garantizar una gestión transparente y coordinada de los riesgos.

✓ **Aprobado** por Junta Directiva a los diecinueve días del mes de marzo de dos mil veinticuatro.

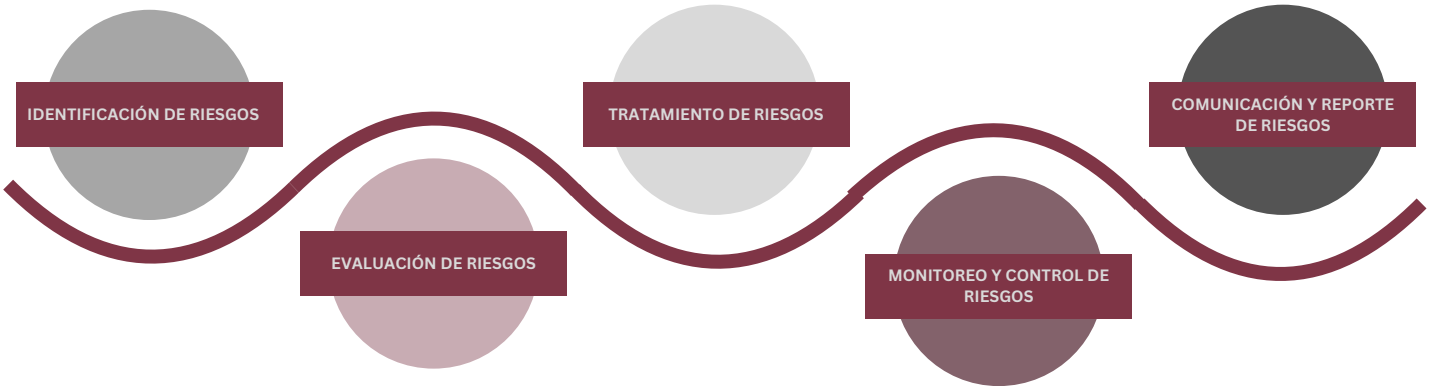
Reportería, Informes y Mecanismos de Divulgación para la de Gestión de Riesgos: Garantiza una comunicación transparente y oportuna con la alta dirección y ente regulador, proporcionando información precisa y completa sobre los riesgos identificados y las medidas adoptadas para mitigarlos. Además, se busca promover la transparencia y la confianza entre los interesados al ofrecer una visión clara de las políticas y mecanismos implementados para gestionar los riesgos de manera efectiva.

✓ **Aprobado** por Junta Directiva a los diecinueve días del mes de marzo de dos mil veinticuatro.

XVII. METODOLOGÍAS PARA LA GESTIÓN DE RIESGOS

Los procedimientos definen la metodología de Gestión de Riesgos proporcionando una sólida estructura de protección y garantizar la continuidad de las operaciones.

Al emplear con cada fase un enfoque integral que abarca desde la identificación inicial de riesgos hasta la comunicación transparente con las partes interesadas, fue posible anticipar, mitigar y responder eficazmente a las amenazas emergentes en un entorno de seguridad cada vez más complejo, según se detalla a continuación:



La metodología implementada ofrece un enfoque adaptado a las necesidades específicas de la organización, desde la identificación y evaluación de riesgos hasta la implementación de controles y la mejora continua. Se centra en promover una cultura organizacional orientada a la seguridad, fomentando la colaboración entre diferentes áreas y la participación activa de todos los miembros del equipo.

XVIII. CONCLUSIONES

La gestión de riesgos requiere un enfoque integral y detallado que permita abordar áreas críticas como la ciberseguridad, la continuidad del negocio, las regulaciones emergentes y las tendencias tecnológicas. Para la gestión 2025 es necesario realizar un análisis exhaustivo de cada uno de estos aspectos, alineado con los objetivos estratégicos.

En el ámbito de la ciberseguridad, la creciente sofisticación de los ciberataques y la dependencia de sistemas digitales hacen imprescindible fortalecer las defensas tecnológicas. Es necesario mantener las buenas prácticas, controles de acceso y el monitoreo activo. Para mitigar estos riesgos, es fundamental implementar sistemas de autenticación multifactor en todas las cuentas críticas, establecer políticas estrictas de gestión de credenciales y adoptar herramientas avanzadas de monitoreo continuo. Estas medidas no solo reducirán la vulnerabilidad ante ataques, sino que también reforzarán la confianza de los clientes y reguladores en la capacidad de la institución para proteger información sensible.

La continuidad del negocio es otro pilar esencial en la gestión de riesgos. La falta de respaldo total en la nube y de infraestructura alterna en 2024 subrayó la necesidad de estrategias más robustas para garantizar la resiliencia operativa. La implementación de un plan de continuidad del negocio que contemple infraestructura de respaldo en la nube, sitios físicos alternativos y certificaciones es crucial. Además, es necesario establecer un calendario de revisión y aprobación del plan por parte del cuerpo directivo, asegurando su alineación con las prioridades estratégicas. Estas acciones permitirán a Equifax responder de manera efectiva ante emergencias, minimizando interrupciones y protegiendo su reputación.

En cuanto a las regulaciones emergentes, el panorama normativo se vuelve cada vez más complejo, especialmente en áreas como la privacidad de datos y la sostenibilidad.

Por último, las tendencias tecnológicas como la automatización y las herramientas de detección y respuesta avanzada representan tanto oportunidades como desafíos. La adopción de estas tecnologías puede mejorar significativamente la eficiencia operativa y la capacidad de respuesta ante incidentes. Sin embargo, su implementación requiere una planificación cuidadosa, incluyendo la capacitación del personal y la integración con los sistemas existentes. Además, es fundamental evaluar continuamente el impacto de estas tecnologías en la gestión de riesgos, asegurando que se alineen con los objetivos estratégicos de Equifax.