POLÍTICA PARA LA GESTIÓN DE RIESGOS

EQUIFAX CENTROAMÉRICA, S.A DE C.V.

I. GENERALIDADES

1. INTRODUCCIÓN

En un entorno dinámico, digital y altamente regulado, la adecuada gestión de riesgos se vuelve esencial para garantizar la sostenibilidad, confianza y resiliencia de Equifax como proveedor líder de soluciones de información y análisis de datos. La presente Política para la Gestión de Riesgos establece los principios, lineamientos, responsabilidades que guían el actuar de la empresa frente a los distintos riesgos a los que se encuentran expuesta.

Esta política busca fortalecer una cultura de gestión de riesgos proactiva, promoviendo la identificación temprana, análisis riguroso y tratamiento oportuno de los riesgos, de forma coherente con los objetivos estratégicos de la empresa facilitando una toma de decisiones informada y fortaleciendo la resiliencia empresa al frente a eventos disruptivos.

2. OBJETIVOS

2.1 Objetivo general

Establecer un marco integral y efectivo para la identificación, medición, control, mitigación, monitoreo y comunicación de los riesgos que pueden afectar el cumplimiento de los objetivos estratégicos, operativos, financieros, tecnológicos, legales y reputacionales de Equifax.

2.2 Objetivos específicos

- **Establecer lineamientos claros y uniformes:** Asegurar la gestión integral de riesgos en todos los niveles de la empresa.
- **Promover una Cultura de Gestión de Riesgos:** Fomentar entre todos los empleados una conciencia y comprensión sólidas de los riesgos asociados con las operaciones de la institución financiera, así como la importancia de su gestión adecuada.
- **Identificar y Evaluar Oportunamente los diferentes riesgos:** Asegurar los activos de información y los intereses de los AE, consumidores o clientes al identificar riesgos que podrían afectar la estabilidad financiera, la continuidad del negocio, el cumplimiento regulatorio y la reputación corporativa.
- **Implementar Mecanismos Eficaces de Control y Mitigación:** Priorizar los riesgos con mayor impacto o probabilidad de ocurrencia.
- **Monitorear y Reportar de Manera Continua:** Proporcionar información oportuna y precisa sobre los riesgos a los que se enfrenta la institución y la efectividad de los controles

implementados, lo que permite una toma de decisiones más informada y estratégica en todos los niveles de la empresa.

- **Cumplir con las Regulaciones y Estándares:** Asegurar el cumplimiento de las regulaciones financieras y los estándares de buenas prácticas en la gestión de riesgos, tanto a nivel nacional como internacional, para mantener la confianza del mercado y la integridad del sistema financiero.
- **Mejorar la Eficiencia Operativa:** Identificar y abordar las áreas de riesgo dentro de la institución para mejorar la eficiencia operativa y reducir los costos asociados con la gestión de riesgos y posibles pérdidas.
- **Promover la Mejora Continua del Sistema de Gestión de Riesgos:** Mantener una revisión periódica de políticas, metodologías y herramientas para la gestión de riesgos.
- **Garantizar la Continuidad del Negocio:** Preparar a la institución financiera para hacer frente a eventos disruptivos y de crisis, asegurando la continuidad del negocio y la capacidad de recuperación frente a situaciones de emergencia.

3. ALCANCE

La Política para la Gestión de Riesgos aplica a todas las unidades de negocio, procesos, productos o servicios de Equifax en la región, incluyendo a todos los colaboradores, AE, consumidores o clientes. Abarca todos los tipos de riesgos significativos a los que la empresa está expuesta, tales como riesgos operacionales, financieros, tecnológicos, estratégicos, legales, reputacionales, de ciberseguridad y continuidad del negocio.

En razón de mantener una gestión de riesgos acorde al contexto de las normativas vigentes y buenas prácticas internacionales, se realizará una revisión anual a la Política para la Gestión de Riesgos.

4. DEFINICIONES

- **Riesgo:** La posibilidad de que un evento ocurra y afecte negativamente los objetivos de la organización.
- **Identificación de Riesgos**: Proceso de reconocer y comprender los riesgos existentes en las operaciones, servicios y procesos de la organización.
- **Evaluación de Riesgos:** Proceso de cuantificar el impacto potencial y la probabilidad de ocurrencia de los riesgos identificados.
- **Control de Riesgos:** Implementación de medidas y acciones para reducir la probabilidad de ocurrencia o el impacto negativo de los riesgos.
- **Mitigación de Riesgos:** Acciones dirigidas a minimizar las consecuencias adversas de los riesgos identificados.
- **Monitoreo de Riesgos:** Proceso de seguimiento y supervisión continua de los riesgos para detectar cambios en su naturaleza o impacto.
- **Comunicación de Riesgos:** Divulgación de información relevante sobre los riesgos identificados a las partes interesadas internas y externas.

- **Tolerancia al Riesgo:** Nivel aceptable de exposición al riesgo que la organización está dispuesta a asumir en la consecución de sus objetivos.
- **Resiliencia Empresarial:** Capacidad de la organización para adaptarse y recuperarse de eventos adversos, minimizando el impacto en sus operaciones y activos.
- **Junta Directiva:** la(s) junta(s) directiva (s) estatutaria(s) de la Empresa.
- **Cliente:** las entidades a las que la Empresa brinda productos y servicios, y no consumidores individuales.
- **Empresa:** Se refiere a "Equifax" incluyendo Equifax Ltd, Equifax Commercial Services Ltd, TDX Group Ltd y AccountScore Limited a efectos de esta política
- **Consumidor:** una persona que actúa en su propio nombre. Entre los ejemplos se incluyen las personas que interactúan con Equifax para ver, comprar o discutir información crediticia sobre sí mismas o las personas con las que se ponen en contacto los proveedores de servicios de cobro de mora en relación con posibles deudas.
- **Usuario final:** una persona física ("Cliente D2C") o jurídica ("Cliente B2B") que actúa en su propio nombre y que tiene (o está en el mercado objetivo de) una relación contractual con la Empresa.
- **Empleado:** un empleado de la Empresa, incluyendo los empleados con contratos de duración determinada, temporales y del Director.

II. RESPONSABILIDADES

Equifax define el siguiente organigrama para la gestión de riesgo, la cual está asignada en funciones a la Gerencia Legal para atender sus funciones.

1. JUNTA DIRECTIVA

La Junta Directiva de la entidad es el Órgano directamente responsable de la gestión del riesgo, por lo que debe:

- Aprobar las estrategias, políticas y manuales de la entidad para la gestión de riesgos y asegurarse que la Alta Gerencia los implemente efectivamente.
- Asignar y aprobar los recursos necesarios para implementar y mantener en funcionamiento la gestión de riesgos en forma efectiva y eficiente.
- Requerir a Auditoría Interna que verifique la existencia y el cumplimiento de la estructura del sistema de gestión de riesgos.
- Asegurarse que los Mecanismos para Gestionar Los Riesgos estén implementados y se mantengan adecuados para cumplir sus objetivos.
- Designar a un responsable de la comunicación de la ocurrencia de eventos de riesgos, pudiendo ser el mismo delegado para el reporte de eventos de continuidad del negocio.
- Asegurarse que el Sistema para Gestionar la Continuidad de Negocio está implementado y se mantiene adecuado para cumplir sus objetivos.
- Aprobar el programa de seguridad de la información y la estructura del SGSI.

2. COMITÉ DE RIESGOS – OFICINA GOBIERNO RIESGOS Y CUMPLIMIENTO

- Evaluar, revisar y proponer para aprobación de la Junta Directiva las estrategias, políticas y manuales para la gestión de riesgos.
- Supervisar que la gestión de riesgos sea efectiva y que los eventos de riesgos sean consistentemente identificados, medidos, evaluados, mitigados y monitoreados.
- Proponer los mecanismos para la implementación efectiva de medidas de mitigación de riesgos, asegurando que se adopten las acciones necesarias para abordar los riesgos identificados de manera adecuada y oportuna.
- Aprobar las metodologías y herramientas para la gestión de riesgos.
- Aprobar los planes de continuidad del negocio.
- Aprobar el programa de pruebas de continuidad de negocio a propuesta de la unidad, área o persona responsable de la gestión de la continuidad del negocio, recomendando acciones o mecanismos adicionales para la planificación y ejecución de las mismas.
- Efectuar el seguimiento de la gestión de continuidad del negocio
- Apoyar la labor de la Unidad de Riesgos en la implementación de la gestión de riesgos a nivel organizacional.
- Proponer a la Junta Directiva la estructura del SGSI.
- Efectuar el seguimiento de la gestión de la seguridad de la información.
- Promover una cultura de gestión de riesgos en toda la empresa, fomentando la conciencia sobre la importancia de la gestión de riesgos y la responsabilidad de todos los empleados en su identificación y mitigación.
- Informar a la Junta Directiva sobre el resultado de los informes elaborados por la Unidad de Riesgos.
- Informar a la Junta Directiva sobre los riesgos asumidos por la entidad, su evolución, sus efectos, en especial en los niveles patrimoniales y las necesidades adicionales de mitigación, así como sus acciones correctivas.

3. ALTA GERENCIA

- La Alta Gerencia es la responsable de la implementación de la gestión de riesgos, de las estrategias, políticas y manuales, autorizados por la Junta Directiva.

4. UNIDAD DE RIESGOS

- Diseñar y someter a la aprobación de la Junta Directiva, a través del Comité de Riesgos, las estrategias, políticas y manuales para la gestión de riesgos.
- Diseñar y someter a la aprobación del Comité de Riesgos la metodología para la gestión de riesgos.
- Apoyar y asistir a las demás unidades de gestión para la implementación de la metodología de riesgos.
- Elaborar una opinión sobre el riesgo de nuevos productos o servicios, previo a su lanzamiento; así como también ante cambios importantes en el ambiente operacional o informático.

- Reportar oportunamente y de forma completa y detallada las fallas en los diferentes factores y eventos de riesgo a la Junta Directiva a través del Comité de Riesgos.
- Asegurar que la gestión de seguridad de la información y la continuidad del negocio que realice la empresa sea consistente con las políticas, metodologías y procedimientos aplicados para la gestión de riesgos.

5. GERENCIA LEGAL

- Interpretación y Cumplimiento Normativo: La Gerencia Legal debe interpretar y aplicar las leyes, regulaciones y normativas relevantes que afectan a Equifax, asegurando el cumplimiento en todas las operaciones de la empresa.
- Identificación de Riesgos Legales: Debe identificar los riesgos legales potenciales asociados con las actividades de Equifax, incluyendo posibles litigios, disputas contractuales, incumplimientos regulatorios y otros riesgos legales.
- Evaluación y Mitigación de Riesgos: La Gerencia Legal debe evaluar la probabilidad y el impacto de los riesgos legales identificados, desarrollando y aplicando estrategias para mitigarlos de manera efectiva y proactiva.
- Elaboración de Políticas y Procedimientos: Es responsable de desarrollar políticas y procedimientos internos que promuevan el cumplimiento normativo y mitiguen los riesgos legales, asegurando que Equifax opere dentro de los límites legales y éticos establecidos.
- Asesoramiento Jurídico: Debe proporcionar asesoramiento jurídico a la alta dirección y otros departamentos de la empresa en asuntos legales y regulatorios, ayudando a tomar decisiones informadas y estratégicas que minimicen los riesgos legales.
- Gestión de Contratos: La Gerencia Legal es responsable de la revisión, negociación y gestión de contratos con clientes, proveedores y otras partes interesadas, asegurando que los términos y condiciones sean adecuados y cumplan con los requisitos legales.

6. AUDITORIA INTERNA

- La Auditoría Interna debe evaluar, al menos anualmente, el cumplimiento de los procedimientos utilizados para la gestión de riesgos y dar seguimiento al cumplimiento del plan de trabajo de la Unidad de Riesgos.
- Reporte a la Alta Gerencia y Junta Directiva: Informa regularmente a la alta gerencia y a la junta directiva sobre los hallazgos de las auditorías internas, incluyendo el estado de los controles internos y los riesgos identificados, así como las acciones tomadas para mitigarlos.

Equifax ha establecido una estructura de gobernanza robusta para asegurar una gestión eficaz y coherente de los riesgos en toda la empresa. Esta estructura contempla la existencia de órganos y roles que supervisan, asesoran y toman decisiones estratégicas en materia de riesgos.

La gestión de riesgos se articula en tres líneas de defensa:

- **Primera Línea:** Las áreas operativas y de negocio, responsables de identificar y gestionar los riesgos asociados a sus áreas. Asimismo, son responsables de la mitigación de éstos por medio del desarrollo e implementación de controles efectivos, y verificando que estos controles están debidamente diseñados y operando efectivamente en línea con los objetivos Estratégicos de Equifax.
- **Segunda Línea:** La Unidad de Riesgos, encargada de definir directrices (Manuales, Políticas y metodologías) de riesgo y control para la Primera Línea de defensa y los gestiona y supervisa activamente en toda la entidad con el fin de proteger a la Institución de riesgos Operacionales, Regulatorios, de Seguridad de la Información y Ciberseguridad, Continuidad del Negocio. de reputación y mitigar riesgos emergentes.
- **Tercera Línea:** Auditoría interna, que evalúa de forma independiente y objetiva, aplicando un enfoque sistemático y disciplinado en la evaluación y mejora de la efectividad y eficiencia de los procesos de gestión de riesgos y controles implementados.

III. PRINCIPIOS DE LA GESTIÓN DE RIESGOS

Equifax, consciente de la importancia de la gestión de riesgos, lleva a cabo las actuaciones que, dentro del ámbito de sus competencias permite que los riesgos corporativos relevantes de todas las actividades y negocios de la empresa se encuentren adecuadamente identificados, medidos, gestionados y controlados, y a establecer, bajo la supervisión de la Unidad de Riesgos quien coordinará para ello con las funciones que corresponden en relación con el control y gestión de riesgos conforme al marco corporativo de la presente Política de Gestión de Riesgos, los mecanismos y principios básicos para un adecuado control y gestión de los mismos con un nivel de riesgo que permita:

- Integrar la visión del riesgo en la gestión de la empresa, incorporando una perspectiva consciente del riesgo en todos los niveles de la empresa, permitiendo que todos los procesos y decisiones consideren los riesgos inherentes para así gestionarlos de manera efectiva a través de la definición de controles adecuados que tenga en cuenta el nivel de riesgo aceptable para la empresa.

- Mantener una ajustada segregación de funciones dentro de la empresa, todos los colaboradores tienen un rol en la gestión de riesgo. La función de riesgos establece lineamientos, pero cada unidad es responsable de gestionar los riesgos propios de su operación, proporcionando un nivel de independencia adecuado.

- Dar cumplimiento a los requerimientos legales y normativa aplicable, la gestión de riesgos se realiza en conformidad con las leyes, regulaciones y estándares internacionales aplicables, así como con el código de ética corporativo.

IV. SISTEMA DE GESTIÓN DE RIESGOS

El sistema de gestión de riesgos de Equifax considera la evaluación integral de los procesos y junto a ello, los riesgos a los que se ve expuesta la empresa, además del cumplimiento normativo. Por ello, la empresa ha definido como riesgos principales:

- **Riesgo Operacional:** posibilidad de incurrir en pérdidas financieras, regulatorias o de reputación como resultado de procesos internos inadecuados o fallidos, errores humanos, fallas en los sistemas, o eventos externos. Abarca una amplia gama de incidentes que pueden afectar la eficiencia y la efectividad de las operaciones diarias de la empresa.
- **Riesgo Legal:** posibilidad de sufrir pérdidas financieras, sanciones regulatorias o daño a la reputación como consecuencia del incumplimiento de leyes, regulaciones, contratos, normas internas o jurisprudencia. Incluye riesgos relacionados con litigios, cambios legislativos, interpretación de leyes y la falta de asesoramiento legal adecuado.
- **Riesgo Reputacional:** posibilidad de experimentar una pérdida de confianza por parte de los stakeholders (clientes o consumidores, empleados, AE, reguladores, público en general) como resultado de eventos negativos, reales o percibidos, que afecten la imagen, la credibilidad y la buena voluntad de la empresa. Este riesgo puede tener un impacto significativo en la lealtad del cliente, la atracción de talento, el valor de la marca y la sostenibilidad del negocio.
- **Riesgo Estratégico:** posibilidad de que las decisiones o la implementación de la estrategia de negocio no permitan alcanzar los objetivos organizacionales a largo plazo. Esto puede surgir de factores como cambios en el entorno competitivo, decisiones estratégicas erróneas, falta de adaptación a las tendencias del mercado, o una ejecución deficiente de la estrategia definida.
- **Riesgo de Seguridad:** se refiere a la probabilidad de que un evento o una acción cause daño, pérdida o interrupción a un activo, sistema o proceso, comprometiendo su integridad, confidencialidad o disponibilidad. Este concepto abarca una variedad de áreas, y para comprenderlo de manera integral, podemos desglosarlo en tres subconceptos clave:
    - **Seguridad de la información:** posibilidad de que se produzcan pérdidas o daños a la confidencialidad, integridad y disponibilidad de la información de la empresa. Esto incluye amenazas internas y externas, como accesos no autorizados, divulgación de datos sensibles, manipulación de información, interrupciones de sistemas y pérdida de datos, con consecuencias financieras, operativas, legales y reputacionales.
    - **Ciberseguridad:** subconjunto del riesgo de seguridad de la información que se centra específicamente en las amenazas y vulnerabilidades en el entorno digital y conectado de una empresa. Esto incluye ataques maliciosos a sistemas informáticos, redes, software y datos a través de medios cibernéticos, como malware, phishing, ransomware, ataques y otras técnicas de intrusión.
    - **Seguridad Ocupacional:** (o seguridad y salud en el trabajo) se ocupa de la protección de los empleados y otras personas dentro del entorno laboral, previniendo lesiones, enfermedades y accidentes.
- **Riesgo de Continuidad del Negocio:** posibilidad de una interrupción significativa de las operaciones del negocio (debido a desastres naturales, fallas tecnológicas, pandemias, etc.) Afecte la capacidad de la empresa para entregar sus servicios críticos. Este riesgo se relaciona

con la planificación y la capacidad de recuperación para asegurar la continuidad de las funciones esenciales y minimizar el impacto de dichas interrupciones.

Aspecto	Factores Internos	Factores Externos
Proceso de Identificación	Establecer un proceso estructurado interno para identificar riesgos internos específicos.	Incorporar fuentes externas de información como informes financieros, análisis de mercado, informes de auditoría y tendencias del sector.
Fuentes de Información	Utilizar datos y recursos internos como informes internos, datos financieros de la empresa, registros de incidentes, etc.	Recopilar información de fuentes externas como informes de organismos regulatorios, publicaciones especializadas y análisis de mercado.
Análisis Periódico y Actualización Continua	Realizar análisis de riesgos y evaluaciones de vulnerabilidad de manera regular, actualizando la lista de riesgos identificados.	Realizar evaluaciones trimestrales de riesgos y vulnerabilidades, incorporando nuevos datos y tendencias en el entorno externo.

Equifax adopta un enfoque estructurado y sistemático para la gestión de riesgos, basado en las normativas vigentes y mejores prácticas internacionales. El proceso contempla las siguientes etapas:

- **Identificación:** Consiste en detectar los eventos potenciales que pueden afectar negativamente el logro de los objetivos.

  La identificación de riesgos debe ser abordada de forma metódica, para garantizar que todas las actividades significativas son incluidas y todos los riesgos catalogados. Se debe trabajar sobre las actividades existentes en Equifax.

  Todos aquellos proyectos desarrollados por la empresa, deberán considerar la identificación de riesgos asociados y sus controles respectivos, previo a su presentación, la que deberá ser permanentemente monitoreada durante la ejecución del mismo.

- **Medición:** Se analiza la probabilidad de ocurrencia y el impacto potencial de los riesgos identificados.

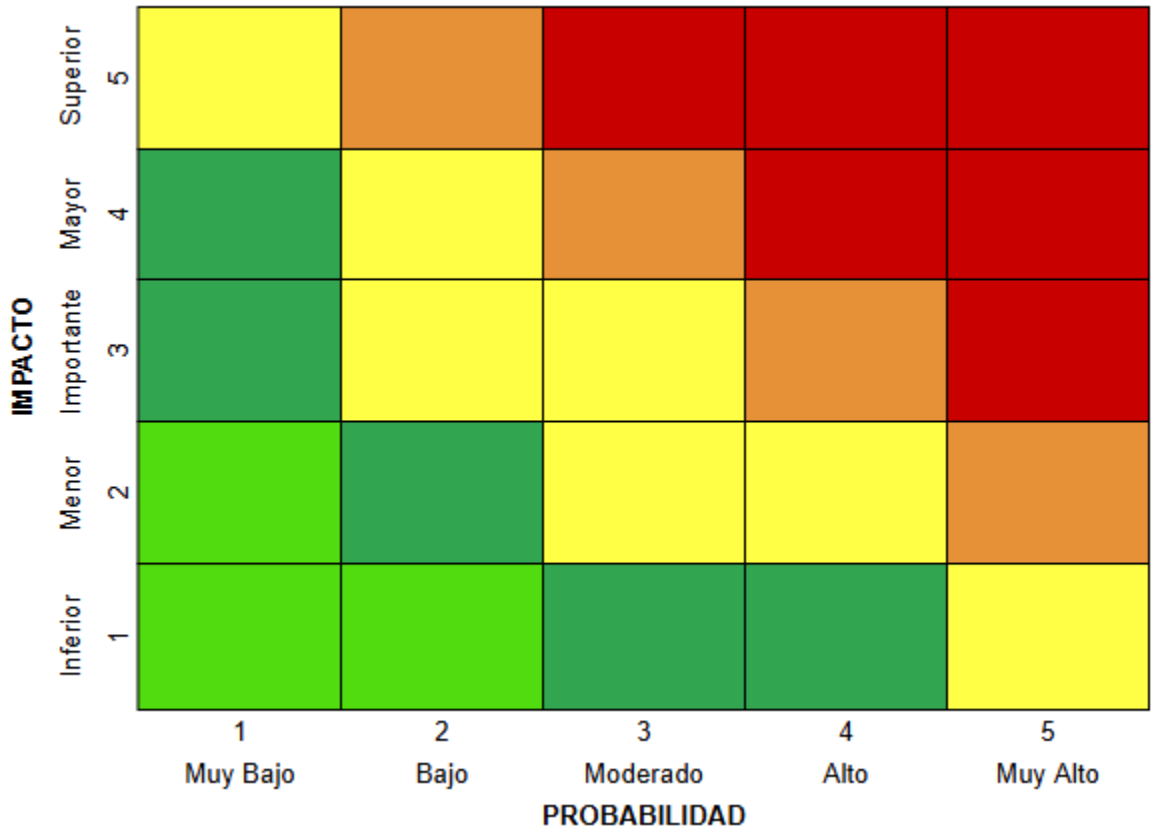
  Los riesgos se analizan bajo un enfoque cualitativo y/o cuantitativo, considerando la identificación y evaluación sobre la existencia de controles manuales y/o automáticos, siendo las respuestas dimensionadas con base en el impacto (severidad) y en la probabilidad de ocurrencia (frecuencia), lo que nos permitirá indicar el grado de exposición al riesgo (nivel de riesgo).

  A continuación, se explica con mayor detalle el proceso:

  - Cuantificar el impacto y probabilidad (para mayor detalle ver Anexo 1).
  - Identificar la existencia de controles establecidos

- Estimar el riesgo asumido como resultado de relacionar los dos parámetros anteriores (Riesgo Residual)

La evaluación de riesgos en Equifax, realizada desde la perspectiva inherente y residual, tiene como propósito presentar un panorama amplio de la administración de los riesgos relevantes para los objetivos de todas las actividades de la empresa, y el mantenimiento de los respectivos controles internos. Una de las herramientas que nos permiten visualizar de mejor manera los resultados de las evaluaciones son los “Mapas de Riesgos”, el que se ha definido como:



De acuerdo a lo definido por Equifax, el nivel de riesgo se define de la siguiente manera:

Nivel de Riesgo		Descripcion
Riesgo Muy Bajo		Activos Equifax con dependencia insignificante en los procesos y áreas del negocio, el impacto es nulo.
Riesgo Bajo		Activos Equifax tiene una dependencia mínima en el desempeño de un proceso comercial o componente donde podría haber un impacto mínimo debido a la pérdida o corrupción de los datos de Equifax.
Riesgo Moderado		Activos Equifax coloca un grado limitado de dependencia comercial en el desempeño de un proceso comercial o componente donde podría haber un impacto moderado a través de la pérdida o corrupción de los datos de Equifax. Cualquier interrupción, falla o lapso de seguridad podría tener un impacto moderado en la reputación, las finanzas, las operaciones o la regulación.
Riesgo Alto		Activos Equifax pone un alto grado de dependencia en el desempeño de un proceso comercial o componente de donde podría haber un impacto significativo a través de la pérdida o corrupción de los datos de Equifax. Cualquier interrupción, falla o lapso de seguridad podría tener un impacto significativo en la reputación, las finanzas, las operaciones o la regulación.
Riesgo Muy Alto		Los Activos de Equifax otorgan un grado sustancial de dependencia en el desempeño de un proceso comercial o componente donde podría haber un impacto severo a través de la pérdida o corrupción de los datos de Equifax. Cualquier interrupción, falla o lapso de seguridad podría tener un impacto inmediato y material en la reputación, las finanzas, las operaciones o las regulaciones.

- **Control y Mitigación:** Se definen acciones, planes o controles para mitigar, transferir, aceptar o evitar los riesgos, priorizando aquellos con mayor exposición dentro de parámetros establecidos, desarrollando una serie de acciones (planes de mitigación) que persigue alinear el resultado de la evaluación con el nivel de riesgo residual aceptado y definido por Equifax.

- **Monitoreo y Comunicación:** Se realiza un seguimiento continuo a los riesgos, controles y planes de acción. Asimismo, la información relacionada a riesgos es documentada y reportada de manera oportuna a los niveles apropiados de la empresa (Junta Directiva, Comité de Riesgos y Alta Gerencia) y al ente regulador según lo solicitan las normativas vigentes, de esta manera, se promueve la transparencia y la toma de decisiones informadas.

V. MECANISMOS PARA LA GESTIÓN DE RIESGOS

Para la efectiva implementación y seguimiento del proceso de gestión de riesgos, la empresa utilizará las siguientes herramientas principales:

a. Matriz de Riesgos

- Esta herramienta fundamental se utiliza para la identificación, análisis y evaluación de los riesgos a los que está expuesta la empresa en sus diferentes áreas. La matriz permitirá visualizar la probabilidad e impacto de cada riesgo, facilitando la priorización de controles y la asignación de responsabilidades para su tratamiento. Se revisará y actualizará anualmente, o con mayor frecuencia si las circunstancias lo requieren.

b. Base de Eventos

- Se establece una base de datos para el registro y seguimiento de los eventos de riesgo que ocurran o sean reportados en las actividades diarias de la empresa. Esta base permitirá documentar la naturaleza del evento, sus causas (procesos, personas, tecnología, eventos externos), los planes de acción implementados y el resultado en términos de materialización

monetaria. Se realizará una revisión y análisis de esta base de datos de forma mensual para identificar tendencias y áreas de mejora.

c. Matriz de Controles

- Derivada de la Matriz de Riesgos, esta herramienta definirá los controles establecidos para mitigar los riesgos identificados. Para cada control, se especificarán los responsables de su ejecución, la periodicidad de ejecución, el tipo de control (preventivo, detectivo, correctivo), su diseño y la documentación asociada. La Matriz de Controles permitirá evaluar la calidad y efectividad de los controles implementados.

d. Planes de Acción

- Para cada evento de riesgo reportado a través de la Base de Eventos, se elaborará un plan de acción detallado para contener el evento y definir las medidas correctivas y preventivas necesarias para evitar su recurrencia o minimizar su impacto futuro. Estos planes incluirán responsables, plazos de ejecución y mecanismos de seguimiento.

e. Indicadores Clave de Riesgos (KRI)

- Se define y se realiza un seguimiento periódico de los indicadores que permitan monitorear la exposición a riesgos y la efectividad de los controles clave en las áreas de negocio que lo requieran. Estos indicadores proporcionarán alertas tempranas sobre posibles incrementos en el nivel de riesgo y facilitarán la toma de decisiones oportuna. La frecuencia de seguimiento de los KRI los definen las áreas del negocio en apoyo con la Unidad de Riesgos.

f. Análisis de Nuevos Riesgos (ANR)

- Se elabora una opinión sobre el riesgo de nuevos servicios, previo a su lanzamiento; así como también ante cambios importantes en el ambiente operacional o informático para identificar y evaluar los riesgos potenciales asociados. Este análisis se integrará en el proceso de toma de decisiones para asegurar que los riesgos y controles sean considerados desde la etapa inicial.

g. Análisis de Proveedores

- Se implementa un proceso para evaluar los riesgos asociados con los proveedores críticos de la empresa. Este análisis considerará aspectos como la estabilidad financiera del proveedor, su cumplimiento normativo, sus prácticas de seguridad de la información y su capacidad de continuidad del negocio, con el fin de mitigar los riesgos de dependencia y posibles interrupciones en la cadena de suministro.

h. Matriz de Litigios

- Se mantendrá una matriz actualizada de todos los procesos legales en curso que puedan representar un riesgo financiero o reputacional significativo para la empresa. Esta matriz incluirá el estado del proceso, la evaluación del riesgo legal, las posibles contingencias financieras y las estrategias de defensa.

Esta sección describe las herramientas clave que la empresa emplea para gestionar sus riesgos de manera sistemática y proactiva. La aplicación efectiva de estas herramientas es fundamental para alcanzar los objetivos estratégicos y proteger el valor de la empresa. Para mayor detalle de estas herramientas consultar el *Manual para la Gestión de Riesgos*.

Equifax podrá implementar otras herramientas y metodologías complementarias que se consideren necesarias para fortalecer el proceso de gestión de riesgos y adaptarse a las necesidades específicas del negocio.

VI. CULTURA Y CONCIENTIZACIÓN

Equifax reconoce que una cultura de gestión de riesgos sólida y una conciencia generalizada sobre los riesgos son elementos fundamentales para la efectividad de esta política y para el logro de sus objetivos. Por lo tanto, se promoverán las siguientes acciones para fomentar una cultura proactiva de gestión de riesgos en todos los niveles de la empresa:

- **Comunicación y Sensibilización:** Se establecerán canales de comunicación efectivos para asegurar que todos los empleados comprendan la importancia de la gestión de riesgos, conozcan la presente política y los procesos asociados, y estén informados sobre los riesgos relevantes para sus funciones y la empresa en general. Se utilizarán diversos medios, como una capacitación anual, campañas de sensibilización trimestrales a través de cápsulas informativas, para reforzar la conciencia sobre los riesgos y las responsabilidades individuales en su identificación y gestión.

- **Capacitación y Formación:** Se proporcionará programa de capacitación anual y formación continua a los empleados en todos los niveles sobre los principios, procesos y herramientas de gestión de riesgos relevantes para sus roles, asegurando que los empleados adquieran el conocimiento y las habilidades necesarias para identificar, evaluar, reportar y gestionar los riesgos de manera efectiva.

- **Fomento de la Participación y el Reporte:** Se alentará a todos los empleados a participar activamente en el proceso de gestión de riesgos, reportando de manera oportuna cualquier evento de riesgo potencial o real, así como cualquier debilidad en los controles existentes. Se establecerán canales seguros y accesibles para facilitar la comunicación y el reporte de riesgos.

A través de estas acciones, la empresa busca construir una cultura de gestión de riesgos sólida y arraigada, donde la conciencia de los riesgos sea una parte integral del comportamiento diario de todos

los empleados, contribuyendo así a la protección de sus activos, la consecución de sus objetivos y su sostenibilidad a largo plazo.

VI. COMUNICACIÓN

Comunicación Interna sobre la Gestión de Riesgos

La eficacia de la gestión de riesgos depende intrínsecamente de una comunicación interna robusta y fluida. Es por ello que se ha establecido un marco de comunicación que asegura que la información relevante sobre los riesgos fluya adecuadamente a los niveles decisorios clave de la organización. La información sobre la gestión de riesgos será presentada de forma periódica y estructurada tanto al Comité de Riesgos como a la Junta Directiva. Estas presentaciones incluirán:

- Se informará sobre cualquier riesgo emergente o previamente identificado cuya materialidad haya cambiado significativamente.
- Se reportará el progreso de las acciones y herramientas destinadas a mitigar los riesgos identificados, incluyendo la efectividad de los controles implementados.
- Se proporcionará una visión integral de la exposición general al riesgo de la entidad.

Estas comunicaciones se realizan de forma trimestral como mínimo, asegurando una revisión constante y sistemática del panorama de riesgos. No obstante, la frecuencia de la comunicación se ajustará a la criticidad y urgencia de la información. En caso de que se identifique un riesgo de alta materialidad o inminencia que pueda tener un impacto significativo en la empresa, en sus operaciones o en sus partes interesadas, la comunicación al Comité de Riesgos y a la Junta Directiva se realizará de manera inmediata, fuera de los ciclos trimestrales establecidos, para facilitar una toma de decisiones ágil y oportuna.

Comunicación Externa sobre la Gestión de Riesgos

La organización reconoce la importancia fundamental de una comunicación externa transparente y proactiva en materia de gestión de riesgos. Nuestro compromiso es proporcionar a nuestros Agentes Económicos (AE), consumidores y clientes, así como al regulador, información clara y oportuna que fomente la confianza y la comprensión de nuestras estrategias de mitigación.

Para ello, se mantiene una sección dedicada en nuestro sitio web y plataformas electrónicas, donde se publicará un resumen conciso y de fácil comprensión de nuestras políticas de gestión de riesgos, los mecanismos implementados para identificarlos y evaluarlos, y las medidas relevantes adoptadas para controlarlos y monitorearlos. Esta información será actualizada periódicamente para reflejar cualquier cambio significativo en el panorama de riesgos o en las estrategias de gestión. El objetivo es que esta comunicación sea accesible y comprensible para todos los públicos interesados, priorizando la claridad.

En cuanto al regulador, la empresa mantendrá una comunicación inmediata y completa ante el conocimiento de cualquier aspecto relacionado con la exposición a riesgos que, de forma cualitativa o cuantitativa, pueda impactar la prestación de productos y servicios a nuestros AE y a nuestros

consumidores o clientes. Esto incluye, pero no se limita a, riesgos operacionales, financieros, estratégicos, de seguridad: ocupacional, información y ciberseguridad . Se realizará énfasis en cualquier situación que amenace la confidencialidad, disponibilidad, integridad o funcionalidad de las plataformas tecnológicas, dada su criticidad para la continuidad de las operaciones y la protección de los datos de los usuarios.

También se remitirá al regulador en los primeros 120 días posteriores a la finalización del año calendario el informe de gestión de riesgos previa aprobación del Comité de Riesgos y Junta Directiva.

Esta comunicación se realizará siguiendo los protocolos y canales establecidos por el regulador, asegurando la entrega de toda la información relevante:

- Utilizar diferentes canales de comunicación, como sitios web corporativos, informes anuales, comunicados de prensa y redes sociales, para divulgar información relevante sobre la gestión de riesgos y las medidas adoptadas para mitigarlos.
- Garantizar la transparencia y la precisión en la comunicación externa sobre la gestión de riesgos, cumpliendo con los requisitos legales y regulatorios aplicables y protegiendo la confidencialidad de la información sensible de la empresa.
- Establecer mecanismos para recibir retroalimentación de las partes interesadas externas sobre la percepción de la gestión de riesgos de la empresa y utilizar esta información para mejorar los procesos y la comunicación.

VII. MARCO REGULATORIO

- **Ley de Supervisión y Regulación del Sistema Financiero:** Establece los principios, normas y disposiciones para la supervisión y regulación de las entidades financieras autorizadas.
- **Normas Técnicas para la Gestión de Riesgos y Políticas de las AID (NRP-30):** Define los requisitos y procedimientos para la gestión integral de riesgos en las entidades financieras autorizadas.
- **Reglamento Interno de la Organización:** Documento interno que establece las políticas, procedimientos y responsabilidades relacionadas con la gestión de riesgos.
- **Normativa del Banco Central de Reserva:** Directrices emitidas por la autoridad monetaria y financiera del país que regulan aspectos específicos de la gestión de riesgos.

- **Legislación sobre Protección de Datos Personales:** Leyes y regulaciones que establecen los requisitos para el manejo y protección de la información personal de los clientes y empleados.

VIII. ANEXOS

Anexo 1 - Determinación del Nivel del Riesgo

A continuación, se presentan los criterios de evaluación de impactos:

EQUIFAX®

Nivel		Categorías							
		Legal	**Operativo**	**Reputacional**	**Estratégico**	**Seguridad de la Información**	**Ciberseguridad**	**Continuidad del Negocio**	**Financiero**
1	Inferior	Incumplimiento menor de normativas o regulaciones sin consecuencias significativas (ej. errores administrativos subsanables). Costos legales mínimos o inexistentes.	Interrupciones menores en procesos o actividades sin afectar significativamente la entrega de servicios. Recuperación rápida y sencilla.	Comentarios negativos aislados o rumores sin impacto visible en la imagen pública o la confianza de los stakeholders.	Desviaciones menores en la ejecución de la estrategia sin afectar los objetivos a largo plazo.	Incidentes menores de seguridad sin acceso a información sensible o impacto en la confidencialidad, integridad o disponibilidad de los datos.	Intentos fallidos de ciberataques o incidentes menores sin éxito en la intrusión o el daño a los sistemas.	Interrupciones menores de las operaciones con planes de contingencia efectivos y tiempos de recuperación mínimos.	Pérdida de ingresos anuales hasta el 1% del objetivo. Hasta $100k de multas o costos inesperados. Sin impacto en la cuota de mercado.
2	Menor	Incumplimiento de normativas o regulaciones con posibles sanciones leves (ej. multas pequeñas, requerimientos de corrección). Costos legales moderados.	Interrupciones moderadas en procesos o actividades que generan retrasos menores o ineficiencias temporales. Necesidad de recursos adicionales para la recuperación.	Publicidad negativa limitada o incidentes menores que generan preocupación en algunos stakeholders pero no afectan significativamente la imagen general.	Desafíos moderados en la implementación de la estrategia que requieren ajustes tácticos pero no comprometen los objetivos principales.	Incidentes de seguridad que resultan en acceso no autorizado a información no crítica o interrupciones menores en los sistemas.	Ciberataques exitosos que resultan en interrupciones menores de los servicios o acceso limitado a información no crítica.	Interrupciones moderadas de las operaciones que requieren la activación de planes de continuidad y generan retrasos en la recuperación.	Pérdida de ingresos anuales de hasta el 3% del objetivo. Multas superiores a $100k o costos inesperados. Impacto potencial
3	Importante	Incumplimiento de normativas o regulaciones con sanciones significativas (ej. multas elevadas, investigaciones regulatorias, litigios). Daño a la imagen pública limitado. Costos legales importantes.	Interrupciones significativas en procesos o actividades que afectan la entrega de servicios o la calidad. Pérdidas económicas moderadas. Impacto en la satisfacción del cliente.	Publicidad negativa significativa, cobertura mediática desfavorable o incidentes que dañan la imagen pública y la confianza de los stakeholders. Pérdida de clientes o proyectos importantes.	Obstáculos significativos en la ejecución de la estrategia que amenazan el logro de algunos objetivos clave a largo plazo. Necesidad de reconsiderar ciertos aspectos de la estrategia.	Incidentes de seguridad que comprometen la confidencialidad, integridad o disponibilidad de información sensible, con posibles consecuencias legales o regulatorias menores. Interrupciones significativas de los sistemas.	Ciberataques que comprometen la confidencialidad, integridad o disponibilidad de datos importantes, causan interrupciones significativas de los servicios y generan costos de recuperación moderados.	Interrupciones significativas de las operaciones que afectan la capacidad de la empresa para entregar servicios críticos durante un período prolongado. Pérdidas económicas moderadas.	Pérdida de ingresos anuales de hasta el 5% del objetivo. Multas superiores a $500k o costos inesperados. Impacto mínimo en la cuota de mercado.

4	Mayor	Incumplimiento grave de normativas o regulaciones con consecuencias legales severas (ej. demandas colectivas, sanciones penales, revocación de licencias). Daño significativo a la imagen pública. Costos legales muy elevados.	Interrupciones graves en procesos o actividades que paralizan áreas críticas del negocio. Pérdidas económicas significativas. Daño a la reputación operativa. Incumplimiento de contratos.	Crisis de reputación importante con cobertura mediática negativa sostenida, pérdida significativa de clientes, socios o inversores, y daño duradero a la imagen pública.	Fracaso significativo en la implementación de la estrategia que impide el logro de los objetivos principales y pone en riesgo la ventaja competitiva de la empresa	Violaciones de seguridad graves que resultan en la pérdida o el robo de información crítica, daño significativo a los sistemas, interrupciones prolongadas de las operaciones y consecuencias legales o regulatorias importantes.	Ciberataques sofisticados que paralizan sistemas críticos, roban información sensible a gran escala, causan pérdidas financieras significativas y dañan gravemente la reputación. Posibles sanciones regulatorias.	Interrupciones graves de las operaciones que amenazan la supervivencia de la empresa debido a la incapacidad de recuperarse en un tiempo razonable. Pérdidas económicas significativas y daño reputacional importante.	Pérdida de ingresos anuales de hasta el 10% del objetivo. Multas superiores a $1 millón o costos inesperados. Impacto en la cuota de mercado
5	Superior	Incumplimiento sistemático o generalizado de la ley con consecuencias catastróficas (ej. cierre de operaciones, quiebra, daño irreparable a la reputación). Costos legales extremadamente altos y prolongados.	Fallas operativas catastróficas que impiden la continuidad de las operaciones principales. Pérdidas económicas masivas. Daño irreparable a la reputación operativa y a la confianza del cliente. Posibles consecuencias regulatorias.	Crisis de reputación catastrófica que amenaza la viabilidad de la empresa, genera un boicot generalizado y causa un daño irreparable a la marca y la confianza de los stakeholders.	Error estratégico fundamental que amenaza la supervivencia de la empresa o la obliga a un cambio radical de dirección con incertidumbre sobre su futuro.	Ataques de seguridad catastróficos que paralizan las operaciones, destruyen información esencial, causan un daño reputacional irreparable y generan graves consecuencias legales y financieras.	Ciberataques catastróficos que amenazan la continuidad del negocio, destruyen datos esenciales, compromete la seguridad nacional o la vida de las personas (dependiendo del sector) y generan consecuencias legales y financieras masivas.	Interrupciones catastróficas de las operaciones que impiden la recuperación del negocio, llevando al cierre o la insolvencia.	Pérdida de ingresos anuales superior al 10% del objetivo. Multas superiores a $10 millones o costos inesperados. Impacto considerable en la cuota de mercado.

A continuación, se presentan los criterios de evaluación de probabilidad:

Escala	Grado	Nivel de Probabilidad
1	Muy Bajo	Puede ocurrir sólo en circunstancias excepcionales (ej. en caso de catástrofe)
2	Bajo	Es poco probable que pueda ocurrir
3	Moderado	Es posible que ocurra en algún momento

4	Alto	Probablemente ocurrirá y/o ha ocurrido alguna vez
5	Muy Alto	Existe un alto grado de certeza que ocurra y/o ya ha ocurrido varias veces

Todos los valores de Impacto y Probabilidad deben ser calculados anualmente.

IX. DISPOSICIONES FINALES

A. Registro de revisiones y modificaciones realizadas a la política de riesgos

versión	Descripción	Editado por	Aprobado por	fecha
1.0	Creación de la política de riesgos	Natalia Navarro	JUNTA DIRECTIVA	2023
2.0	Revisión y actualización de políticas	Natalia Navarro	JUNTA DIRECTIVA	19/03/24
3.0	Actualización completa de la política	Masciel Canizalez	JUNTA DIRECTIVA	02/05/2025