POLÍTICAS PARA LA GESTIÓN DE RIESGOS

EQUIFAX CENTROAMÉRICA, S.A DE C.V.

I. GENERALIDADES

1. OBJETIVOS

1.1 Objetivo general

Establecer un marco integral y efectivo para identificar, medir, controlar, mitigar, monitorear y comunicar los riesgos a los que se enfrenta la institución. Los siguientes son los objetivos específicos que se persiguen con la implementación de esta política.

1.2 Objetivos específicos

- **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.
- **Proteger los Intereses de los Accionistas y Clientes:** Salvaguardar los activos y los intereses de los accionistas y clientes al identificar y mitigar los riesgos que podrían afectar negativamente la estabilidad financiera y la reputación de la institución.
- **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.
- **Optimizar la Toma de Decisiones:** Proporcionar información oportuna y precisa sobre los riesgos a los que se enfrenta la institución financiera, lo que permite una toma de decisiones más informada y estratégica en todos los niveles de la organización.
- **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.
- **Garantizar la Continuidad del Negocio:** Preparar a la institución financiera para hacer frente a eventos adversos y crisis, asegurando la continuidad del negocio y la capacidad de recuperación frente a situaciones de emergencia.

2. ALCANCE

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.

3. 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

- Aprobar y Revisar la Política de Riesgos: La junta directiva es responsable de aprobar la política de riesgos de la empresa y de revisar periódicamente para garantizar su relevancia y eficacia en la gestión integral de los riesgos.
- Supervisar la Implementación de la Política de Riesgos: Es responsabilidad de la junta directiva supervisar la implementación efectiva de la política de riesgos, asegurándose de que se cumplan los objetivos y que se adopten las medidas adecuadas para abordar los riesgos identificados.
- Evaluar y Mitigar Riesgos Estratégicos: La junta directiva debe evaluar y mitigar los riesgos estratégicos que puedan afectar la capacidad de Equifax para alcanzar sus objetivos a largo plazo, asegurando que se tomen las decisiones adecuadas para proteger los intereses de la empresa y sus partes interesadas.

2. COMITÉ DE RIESGOS – OFICINA GOBIERNO RIESGOS Y CUMPLIMIENTO

- Asesoramiento a la Junta Directiva: Proporciona asesoramiento a la junta directiva sobre cuestiones relacionadas con la gestión de riesgos, incluyendo recomendaciones sobre políticas, procedimientos y estrategias para mitigar los riesgos identificados.
- Fomento de una Cultura de Gestión de Riesgos: El comité debe promover una cultura de gestión de riesgos en toda la organización, fomentando la conciencia sobre la importancia de la gestión de riesgos y la responsabilidad de todos los empleados en su identificación y mitigación.
- Revisión y Supervisión de la Política de Riesgos: El comité de riesgos es responsable de revisar y supervisar la política de riesgos de la empresa, asegurándose de que esté alineada con los objetivos estratégicos y cumpla con las regulaciones y estándares relevantes.
- Identificación y Evaluación de Riesgos: Debe liderar el proceso de identificación y evaluación de los riesgos a los que se enfrenta Equifax, tanto internos como externos, considerando aspectos como el riesgo crediticio, operativo, legal, reputacional y tecnológico.
- Revisión de Informes de Riesgos: El comité debe revisar los informes periódicos sobre los riesgos identificados, evaluaciones de riesgos y medidas de mitigación propuestas, asegurando que la información sea precisa, oportuna y relevante para la toma de decisiones.
- Supervisión de la Implementación de Medidas de Mitigación: Es responsable de supervisar 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.
- Monitoreo Continuo de Riesgos: Debe realizar un monitoreo continuo de los riesgos para identificar cambios significativos en el entorno de riesgos y asegurarse de que se tomen medidas correctivas según sea necesario.

3. ALTA GERENCIA

Identificación y Evaluación de Riesgos: La alta gerencia debe participar activamente en la identificación y evaluación de riesgos, tanto en términos de amenazas potenciales como de oportunidades, utilizando información interna y externa para una evaluación exhaustiva.

Toma de Decisiones Informadas: Deben tomar decisiones informadas sobre la gestión de riesgos, basadas en análisis de datos y evaluaciones de riesgos, considerando el impacto potencial en los objetivos comerciales y financieros de la empresa.

Implementación de Medidas de Mitigación: La alta gerencia es responsable de liderar la implementación de medidas de mitigación de riesgos, asegurando que se tomen acciones apropiadas para abordar los riesgos identificados de manera oportuna y efectiva.

Comunicación y Transparencia: Deben comunicar de manera clara y transparente los riesgos y las estrategias de gestión de riesgos a todas las partes interesadas pertinentes, incluyendo empleados, accionistas, clientes y reguladores.

Asignación de Recursos: Deben asignar los recursos necesarios, incluyendo personal, tecnología y presupuesto, para apoyar la implementación efectiva de la estrategia de gestión de riesgos y las iniciativas relacionadas.

4. GERENCIAL 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.

5. AUDITORIA INTERNA

- Evaluación de Controles Internos: La auditoría interna evalúa la efectividad de los controles internos existentes para mitigar los riesgos operativos, financieros y de cumplimiento en Equifax.
- Identificación de Riesgos y Vulnerabilidades: Participa en la identificación y evaluación de riesgos y vulnerabilidades en los procesos y operaciones de la empresa, proporcionando recomendaciones para mejorar los controles y reducir los riesgos.
- Auditorías Especiales: Realiza auditorías especiales centradas en áreas de alto riesgo o en respuesta a incidentes específicos, con el fin de identificar problemas y recomendar medidas correctivas.
- Monitoreo y Seguimiento: Monitorea continuamente la implementación de las recomendaciones de auditoría y realiza un seguimiento para garantizar que se aborden adecuadamente los riesgos identificados.
- Reporte a la Alta Dirección y Junta Directiva: Informa regularmente a la alta dirección 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.

III. POLÍTICAS

1. Política de Gestión de Riesgos

- Establecimiento de un Marco y Principios: Definir un marco integral para la gestión de riesgos en toda la organización, junto con principios fundamentales que guíen esta gestión.
- Identificación y Evaluación de Riesgos: Implementar procesos estructurados para identificar y evaluar riesgos potenciales en todas las áreas y procesos.
- Tratamiento de Riesgos: Establecer criterios claros para priorizar riesgos y desarrollar acciones específicas para mitigarlos.
- Desarrollar planes de acción detallados para abordar los riesgos prioritarios, asignando responsabilidades claras, estableciendo plazos de ejecución y asignando recursos adecuados.
- Monitorear continuamente la efectividad de los controles implementados y realizar ajustes según sea necesario para garantizar que sigan siendo apropiados y eficaces.

2. Etapas de gestión de riesgos:

a) Identificación de Factores de Riesgo

Los factores de riesgo pueden generar un aumento en la exposición, ya sea de origen interno o externo. Los factores internos se refieren a aquellos específicos, mientras que los externos están relacionados con situaciones sistémicas o que afectan al entorno en general.

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 periódicas de riesgos y vulnerabilidades, incorporando nuevos datos y tendencias en el entorno externo.

b) Metodologías de Medición de Riesgos

De acuerdo a los factores de riesgo identificados, a continuación, se detalla la medición a realizarse:

Riesgo de Crédito:

- Porcentaje de ingresos perdidos debido al incumplimiento en el pago de servicios de informes de crédito por parte de clientes.
- Porcentaje de ingresos perdidos debido al incumplimiento en el pago de servicios relacionados con el crédito por parte de instituciones financieras.
- Ratio de cobertura de riesgo de crédito, comparando los activos líquidos con las obligaciones de crédito pendientes.

Riesgo de Liquidez:

- Ratio de liquidez actual, comparando los activos líquidos con las obligaciones a corto plazo.
- Tiempo promedio requerido para convertir activos en efectivo en caso de necesidad.
- Prueba de estrés de liquidez para evaluar la capacidad de la empresa para hacer frente a escenarios de falta de liquidez.
- Porcentaje de activos fácilmente líquidos en relación con el total de activos de la empresa.

Riesgo de Mercado:

- Valoración de sensibilidad a las tasas de interés, midiendo el impacto en el valor de los activos ante cambios en las tasas.

- Valoración de sensibilidad a los tipos de cambio, midiendo el impacto en el valor de las inversiones extranjeras ante fluctuaciones en los tipos de cambio.
- Volatilidad del mercado, medida por la desviación estándar de los rendimientos de los activos.
- Evaluación de riesgo de liquidez del mercado, considerando la disponibilidad de contrapartes para la compra y venta de activos financieros.

Riesgo Operativo:

- Tiempo de inactividad del sistema, medido como la cantidad de tiempo que los sistemas críticos están fuera de servicio.
- Tasa de error en procesos operativos clave, como el procesamiento de transacciones o la generación de informes.
- Frecuencia de incidentes operativos, registrando el número de eventos adversos que afectan las operaciones comerciales.
- Costo promedio por incidente operativo, calculando los gastos asociados con la resolución de problemas operativos.
- Evaluación de la efectividad de los planes de contingencia mediante simulacros de crisis y evaluaciones post-evento.

Riesgo Legal y Regulatorio:

- Número de infracciones legales o regulatorias identificadas en un período determinado.
- Costo de multas y sanciones por incumplimiento de regulaciones.
- Evaluación de la calidad y eficacia de los programas de cumplimiento a través de auditorías internas y externas.
- Índice de cumplimiento regulatorio, comparando el grado de cumplimiento con las regulaciones aplicables.
- Frecuencia y costo de litigios relacionados con la gestión de la información crediticia.

Riesgo de Reputación:

- Índice de satisfacción del cliente, evaluando la percepción y la satisfacción del cliente con los productos y servicios.
- Monitorización de redes sociales y medios de comunicación para identificar menciones negativas sobre la empresa.
- Evaluación de la reputación de la marca mediante encuestas de opinión pública y estudios de mercado.
- Número de quejas y reclamaciones de clientes relacionadas con la calidad de servicio y productos.

- Evaluación de la percepción pública de la empresa mediante encuestas de percepción de la marca y evaluaciones de imagen corporativa.

Riesgo de Fraude:

- Índice de detección de fraudes, midiendo la eficacia de los sistemas de detección de fraudes.
- Monto total de pérdidas por fraudes detectados en un período determinado.
- Ratio de fraude por tipo de fraude, identificando las áreas de mayor vulnerabilidad.
- Porcentaje de recuperación de fondos perdidos por fraude.
- Evaluación de la eficacia de los controles internos para prevenir y detectar fraudes a través de auditorías y revisiones periódicas.

Riesgo Tecnológico:

- Número de incidentes de seguridad cibernética reportados en un período determinado.
- Tiempo de respuesta a incidentes de seguridad, evaluando la eficiencia en la gestión de crisis.
- Evaluación de vulnerabilidades de seguridad mediante pruebas de penetración y evaluaciones de seguridad.
- Ratio de actualización de sistemas y aplicaciones críticas para mitigar vulnerabilidades.
- Costo de recuperación de desastres y restauración de sistemas después de incidentes tecnológicos.

c) Mecanismos de Control y Mitigación de Riesgos

1) **Implementar controles internos y procedimientos** para reducir la probabilidad de ocurrencia y el impacto de los riesgos identificados, en línea con las políticas y procedimientos establecidos por la organización.
2) **Monitoreo y Mejora Continua:** Establecer sistemas de monitoreo para evaluar la efectividad de los controles y realizar ajustes según sea necesario.
3) **Cumplimiento y Supervisión:** Asegurar el cumplimiento de normativas y estándares relacionados con la gestión de riesgos, supervisando continuamente la implementación de la política de riesgos.

D. Procesos de Monitoreo y Comunicación de Riesgos

Los eventos de riesgos serán registrados y trabajados por un formulario donde las respuestas pueden ser: [a] abiertas; [c] cerradas o con opciones definidas, [p] parámetro de fecha

Los campos a capturar: fecha del evento [p], descripción del evento [a], ubicación del evento [c], tipo de evento [c], impacto del evento [c], causa del evento [a], acciones tomadas [a], responsable del evento [a], estado del evento [c], comentarios adicionales [a]

Resultados para preguntas con respuestas [c].

Ubicación del evento	Tipo de evento	Impacto del evento	Estado del evento
Acorde a los departamentos internos	Según el tipo de riesgo (conjunto i).	Bajo Moderado Alto Crítico	Abierto En Investigación Resuelto Cerrado

Conjunto (i):

Riesgo de Crédito:

- Incumplimiento en el pago de servicios de informes de crédito por parte de clientes.
- Incumplimiento en el pago de servicios relacionados con el crédito por parte de instituciones financieras.

Riesgo de Liquidez:

- Falta de efectivo disponible para cumplir con obligaciones financieras.
- Incapacidad para convertir activos en efectivo rápidamente para cumplir con obligaciones financieras.

Riesgo de Mercado:

- Fluctuaciones adversas en las tasas de interés que afectan el valor de los activos financieros.
- Fluctuaciones adversas en los tipos de cambio que afectan el valor de las inversiones extranjeras.
- Cambios adversos en los precios de los activos financieros que afectan el valor de las inversiones.

Riesgo Operativo:

- Fallas en los procesos operativos que provocan interrupciones en la prestación de servicios.
- Fallas en los sistemas de información que comprometen la integridad o disponibilidad de los datos.
- Eventos externos imprevistos que causan pérdidas financieras, como desastres naturales o crisis económicas.

Riesgo Legal y Regulatorio:

- Multas o sanciones legales por incumplimiento de regulaciones de protección de datos.
- Litigios relacionados con la gestión de la información crediticia.
- Sanciones regulatorias por violación de normativas de privacidad u otras regulaciones financieras.

Riesgo de Reputación:

- Violaciones de seguridad de datos que afectan la confianza de los clientes.
- Prácticas comerciales cuestionables que generan una percepción negativa en el público.
- Mala gestión de incidentes que socava la credibilidad y confianza en la empresa.

Riesgo de Fraude:

- Robo de identidad que resulta en transacciones fraudulentas.
- Fraude crediticio que causa pérdidas financieras a la empresa.
- Uso indebido de información confidencial para cometer actividades fraudulentas.

Riesgo Tecnológico:

- Ataques cibernéticos que comprometen la seguridad de los sistemas de información.
- Brechas de seguridad que exponen datos confidenciales de los clientes.
- Fallas tecnológicas que interrumpen la prestación de servicios y causan pérdidas financieras.
- Establecer sistemas de monitoreo periódico para supervisar la evolución de los riesgos identificados y detectar cambios significativos en su nivel o naturaleza.
- Desarrollar informes de riesgos periódicos para informar a la alta dirección y a los órganos de gobierno sobre el estado de los riesgos y las acciones tomadas para gestionarlos.
- Comunicar de manera proactiva la información sobre riesgos a los diferentes niveles de la organización, incluyendo la alta dirección, los empleados y las partes interesadas externas, utilizando canales de comunicación adecuados y asegurando la confidencialidad de la información sensible.
- Con el sistema de monitoreo periódico se puede implementar el siguiente control cuando sobrepase el nivel de riesgo en la escala de 1 a 5 diseñada:

Tipo de Riesgo	Medición	Tolerancia	Control rápido	Control inmediato
Riesgo de Crédito.	Cada evento de riesgo tendrá una ponderación evaluada por criterio en una escala de 1 a 5. Descripción del evento 20% Impacto del evento 30% Causa del evento 20% Acciones tomadas 20% Estado del evento 20%	De 1 a 3	4	5
Riesgo de Liquidez.		1 y 2	3	4 y 5
Riesgo de Mercado.		1	2	De 3 a 5
Riesgo Operativo.		1 y 2	3	5
Riesgo Legal y Regulatorio.		1	De 2 a 4	5
Riesgo de Reputación.		1	De 2 a 4	5
Riesgo de Fraude.		1	2 y 3	4 y 5
Riesgo Tecnológico.		1	2 y 3	4 y 5

3. Capacitación y Comunicaciones

a. Programas de Capacitación en Gestión de Riesgos

- Diseñar programas de capacitación específicos en gestión de riesgos para todos los niveles de la organización, desde la alta dirección hasta los empleados operativos.
- Establecer un plan de capacitación periódico que incluya sesiones de formación presenciales o virtuales, material educativo, talleres prácticos y actividades de aprendizaje continuo.
- Asegurar que el personal reciba formación sobre las políticas, procedimientos y herramientas relacionadas con la gestión de riesgos, así como sobre los roles y responsabilidades individuales en este proceso.
- Evaluar regularmente la efectividad de los programas de capacitación y realizar ajustes según sea necesario para garantizar que cubran las necesidades de formación identificadas.

b. Comunicación Interna de Políticas y Procedimientos

- Establecer canales de comunicación interna efectivos para difundir las políticas, procedimientos y mejores prácticas relacionadas con la gestión de riesgos en toda la organización.
- Desarrollar materiales de comunicación claros y accesibles, como manuales, guías de referencia y boletines informativos, para asegurar que todos los empleados estén familiarizados con las políticas y procedimientos de gestión de riesgos.
- Organizar reuniones periódicas, sesiones de retroalimentación y actividades de sensibilización para promover una cultura de gestión de riesgos dentro de la organización y fomentar la participación de los empleados en este proceso.
- Establecer mecanismos para recopilar comentarios y sugerencias de los empleados sobre la efectividad de las políticas y procedimientos de gestión de riesgos, con el fin de realizar mejoras continuas.

c. Comunicación Externa sobre la Gestión de Riesgos

- Desarrollar un plan de comunicación externa para informar a las partes interesadas externas, como clientes, proveedores, reguladores y accionistas, sobre la estrategia y los procesos de gestión de riesgos de la organización.
- 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 organización.
- Establecer mecanismos para recibir retroalimentación de las partes interesadas externas sobre la percepción de la gestión de riesgos de la organización y utilizar esta información para mejorar los procesos y la comunicación.

IV. 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.

V. 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	NataliaNavarro	JUNTA DIRECTIVA	19/03/24