SISTEMA DE GESTIÓN DE RIESGOS

EQUIFAX CENTROAMÉRICA, S.A DE C.V.

Capítulo 1: Aspectos Generales

Introducción:

El presente 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.

Objetivos:

Gestión Eficiente de Riesgos

- Establecer un mecanismo eficiente que permita identificar, medir, controlar y monitorear los riesgos inherentes, con el fin de proteger la integridad de los datos y promover la confianza de los clientes.
- Mejorar la capacidad de respuesta ante situaciones de crisis o emergencias, implementando planes de contingencia efectivos y procesos de comunicación claros para minimizar el impacto en las operaciones y la reputación de la empresa.

Cumplimiento Normativo

- Garantizar la precisión, seguridad y transparencia en la gestión de riesgos, promoviendo la confianza del público en la empresa.
- Cumplir con los estándares regulatorios y de privacidad de datos aplicables, además de adherirse a las mejores prácticas de la industria para asegurar la conformidad legal y mitigar cualquier riesgo asociado con la no conformidad.

Cultura y Estrategia Organizacional

- Fomentar una cultura organizacional centrada en la gestión proactiva de riesgos, promoviendo la participación y responsabilidad de todos los empleados en la identificación, evaluación y mitigación de riesgos en sus áreas de trabajo.
- Impulsar la innovación y el crecimiento sostenible al aprovechar la gestión de riesgos como una herramienta estratégica para identificar oportunidades de mejora y optimización en todos los aspectos del negocio.

Proceso basado en Gobierno, Riesgos y Cumplimiento - GRC:

1. Gobierno:

- Establecimiento de un Comité de Gestión de Riesgos liderado por la dirección.
- Definición de políticas y procedimientos claros para la gestión de riesgos, incluyendo roles y responsabilidades.
- Revisión y aprobación de políticas y estrategias de riesgo por parte del Consejo de Administración.

2. Gestión de Riesgos:

- Identificación de riesgos: Realización de análisis exhaustivos para identificar los riesgos.
- Evaluación de riesgos: Cuantificación y evaluación de la probabilidad e impacto de los riesgos identificados.
- Mitigación de riesgos: Desarrollo e implementación de medidas para reducir la probabilidad e impacto de los riesgos identificados.
- Monitoreo y control de riesgos: Establecimiento de procesos para monitorear continuamente los riesgos y las medidas de mitigación.

3. Cumplimiento:

- Adherencia a estándares regulatorios: Garantizar el cumplimiento de las leyes y regulaciones aplicables en relación con la gestión de riesgos y la protección de datos.
- Auditoría y revisión: Realización de auditorías internas y externas periódicas para verificar el cumplimiento normativo y la eficacia de los controles internos.
- Informes y divulgación: Preparación y presentación de informes regulares sobre la gestión de riesgos a las autoridades reguladoras y partes interesadas.

Integración del Sistema de Gestión de Riesgos basado en Gobierno, Riesgo y Cumplimiento.

La integración de un sistema de gestión de riesgos ante la dirección guiado por una Oficina de Riesgos se establece como una práctica fundamental para garantizar la estabilidad, seguridad y conformidad normativa. Con este enfoque integrado se pretende identificar y mitigar los riesgos financieros, operativos y legales y además promover una cultura organizacional centrada en la transparencia, la responsabilidad y la excelencia en el cumplimiento de las regulaciones. La experiencia acumulada y la mejora continua contribuyen a fortalecer la capacidad para gestionar eficazmente los riesgos, al tiempo que se promueve una cultura organizacional resiliente y orientada hacia el futuro. A continuación, está el planteamiento de integración basado en mejora continua con eje de experiencia y tiempo:

Fase inicial Hasta los 6 meses	Fase aprendizaje Hasta el año	Fase Optimización Hasta los 2 años	Fase Madurez Desde los 2 años
En esta etapa inicial, la experiencia en la implementación de un sistema de gestión de riesgos y la administración por una Oficina de Riesgos podría ser limitada. El personal podría estar en proceso de familiarización con los conceptos, herramientas y procesos asociados.	A medida que pasa el tiempo, el equipo comienza a adquirir más experiencia en la Gestión de Riesgos y la administración de GRC. Se han identificado y abordado algunos riesgos iniciales, y se están estableciendo procesos más robustos para la gestión continua de riesgos.	Durante este período, el equipo ha ganado experiencia significativa en la aplicación práctica de las metodologías de Gestión de Riesgos y GRC. Se están implementando mejoras continuas en los procesos y se están utilizando lecciones aprendidas para optimizar la eficiencia y efectividad del sistema.	En esta etapa avanzada, el equipo posee una experiencia sólida en la Gestión de Riesgos y GRC. Los procesos están completamente integrados en las operaciones diarias de Equifax, y el sistema de gestión de riesgos está altamente optimizado y alineado con los objetivos estratégicos de la organización.

Tipos de Riesgos:

- Riesgo de Crédito: Relacionado con la posibilidad de que los clientes o instituciones financieras incumplan con los pagos por servicios de informes de crédito o servicios relacionados.
- Riesgo de Liquidez: Posibilidad en la cual no se pueda cumplir con sus obligaciones financieras debido a la falta de efectivo disponible o la incapacidad para convertir activos en efectivo rápidamente.
- Riesgo de Mercado: Relacionado con la exposición a cambios adversos en los mercados financieros, como fluctuaciones en las tasas de interés, tipos de cambio y precios de los activos.
- Riesgo Operativo: Relacionado con fallas en los procesos operativos, sistemas de información, recursos humanos, o eventos externos que puedan causar pérdidas financieras.
- Riesgo Legal y Regulatorio: Relacionado con la posibilidad de enfrentar sanciones legales o regulatorias debido al incumplimiento de las leyes de protección de datos, regulaciones de privacidad, o litigios relacionados con la gestión de la información crediticia.
- Riesgo de Reputación: Posibilidad de que la reputación se vea dañada debido a eventos negativos, como violaciones de seguridad de datos, prácticas comerciales cuestionables o mala gestión de incidentes.
- Riesgo de Fraude: Posibilidad de sufrir pérdidas financieras debido a actividades fraudulentas, como el robo de identidad, el fraude crediticio o el uso indebido de la información confidencial.
- Riesgo Tecnológico: Relacionado con la vulnerabilidad de los sistemas de información de Equifax a ataques cibernéticos, brechas de seguridad o fallas tecnológicas que podrían resultar en pérdidas financieras y daños a la reputación.

Identificación de Riesgos:

En una fase inicial, se debe llevar a cabo una evaluación exhaustiva de los riesgos financieros, operativos y regulatorios a los que se enfrenta. Se promoverá la participación de los diferentes equipos y áreas de la organización para identificar una amplia gama de riesgos potenciales. Se utilizarán herramientas como análisis de datos históricos, entrevistas con expertos y análisis de tendencias del mercado para garantizar la exhaustividad de la identificación de riesgos.

Criterios de éxito y métricas de rendimiento:

- Claridad en la identificación de riesgos clave: Asegurarse de identificar y comprender completamente los riesgos relevantes para sus operaciones.
- Efectividad en la implementación de medidas de mitigación: Implementar medidas efectivas para mitigar los riesgos identificados y reducir su impacto potencial.
- Reducción de exposición a riesgos significativos: Trabajar para reducir su exposición a riesgos significativos que puedan afectar negativamente sus operaciones o reputación.
- Mejora en la capacidad de respuesta ante riesgos emergentes: Prepararse para identificar y responder rápidamente a los nuevos riesgos que puedan surgir en su entorno operativo.
- Cumplimiento con los estándares regulatorios y de la industria: Asegurarse de cumplir con todas las regulaciones y estándares de la industria relacionados con la gestión de riesgos y la protección de datos.

Otros requerimientos adicionales:

Identificación de recursos necesarios: Se debe determinar los recursos humanos, financieros y tecnológicos necesarios para implementar y mantener un sistema efectivo de gestión de riesgos.

- Evaluación de tecnologías y herramientas: Evaluar y seleccionar las tecnologías y herramientas más adecuadas para facilitar la identificación, evaluación y mitigación de riesgos.
- Establecimiento de canales de comunicación efectivos: Establecer canales de comunicación claros y efectivos entre los diferentes equipos y departamentos involucrados en la gestión de riesgos.
- Desarrollo de programas de capacitación: Implementar programas de capacitación en gestión de riesgos para garantizar que su personal esté adecuadamente capacitado para identificar, evaluar y mitigar los riesgos en sus áreas respectivas.

Capítulo 3: Diseño del Sistema

La Oficina de Riesgos llevará a cabo una evaluación exhaustiva de las necesidades en términos de gestión de riesgos. Esto incluirá la revisión de los procesos existentes, la identificación de áreas de mejora y la recopilación de requisitos específicos de todas las partes interesadas involucradas.

Componentes del Sistema:

- Interfaz de Usuario: La Oficina de Riesgos diseñará una interfaz de usuario intuitiva y fácil de usar que permita a los usuarios acceder y manejar la información relacionada con la gestión

de riesgos. Esta interfaz proporcionará paneles de control personalizables, herramientas de análisis de datos y capacidades de generación de informes.

- Base de Datos: Se implementará una base de datos robusta y segura para almacenar toda la información relevante sobre riesgos, incluidos datos de clientes, datos financieros y registros de incidentes. Se garantizará la integridad, confidencialidad y disponibilidad de los datos en todo momento.
- Algoritmos de Análisis de Riesgos: La Oficina de Riesgos se encargará de desarrollar o adquirir algoritmos de análisis de riesgos avanzados que puedan identificar patrones, tendencias y correlaciones en los datos para evaluar y predecir los riesgos potenciales de manera eficiente y precisa.
- Mecanismos de Comunicación de Riesgos: Se establecerán mecanismos efectivos de comunicación interna y externa para informar sobre los riesgos identificados, los hallazgos del análisis de riesgos y las medidas de mitigación propuestas. Esto incluirá informes automatizados, alertas en tiempo real y reuniones periódicas.

Flujo de Trabajo:

- Etapa fase 0: Desarrollo de una encuesta. El objetivo de desarrollar la encuesta es recopilar datos de manera sistemática y objetiva de los empleados de diferentes departamentos de la empresa con el fin de identificar y analizar los posibles riesgos a los que se enfrenta la organización. Esta encuesta servirá como una herramienta para obtener una visión más amplia y completa de los riesgos percibidos desde diversas perspectivas dentro de la empresa. Además, facilitará la aplicación de una matriz de riesgos para categorizar y evaluar los datos recopilados, permitiendo así un análisis más estructurado y una mejor comprensión de los riesgos prioritarios que deben ser abordados.
- Identificación de Riesgos: La Oficina de Riesgos liderará la implementación de un proceso estructurado para identificar y documentar los riesgos en todas las áreas. Esto implica la realización de evaluaciones de riesgos periódicas, la revisión de incidentes pasados y la consulta con expertos en la materia.
- Evaluación de Riesgos: Una vez identificados, los riesgos serán evaluados en términos de su probabilidad de ocurrencia y su impacto potencial en las operaciones y la reputación. Se establecerán criterios claros para clasificar y priorizar los riesgos.
- Mitigación de Riesgos: Se desarrollarán estrategias y medidas específicas para mitigar los riesgos identificados. Esto puede incluir la implementación de controles internos adicionales, la transferencia de riesgos a través de seguros o contratos, y la mejora de los procesos operativos.
- Comunicación de Riesgos: Se establecerán canales de comunicación efectivos para informar a todas las partes interesadas sobre los riesgos identificados y las acciones de mitigación propuestas. Esto puede incluir informes periódicos, reuniones de revisión de riesgos y actualizaciones de políticas y procedimientos.

Matriz de riesgos.

La Oficina de Riesgos definirá una matriz de riesgos que servirá como herramienta fundamental para la evaluación y priorización de los riesgos identificados. Esta matriz asignará valores a los riesgos en función de su probabilidad de ocurrencia y su impacto potencial.

La matriz de riesgos permitirá categorizar los riesgos en diferentes niveles de gravedad y establecer criterios claros para determinar la necesidad de acciones de mitigación. Esto facilitará la toma de decisiones informadas y la asignación de recursos adecuados para abordar los riesgos prioritarios.

La matriz de riesgos será revisada y actualizada periódicamente para reflejar cambios en el entorno empresarial y asegurar su relevancia continua en la gestión de riesgos.

Monitoreo y Mejora Continua

La Oficina de Riesgos debe establecer un cronograma detallado para la implementación del sistema de gestión de riesgo, asignando los recursos y responsabilidades a cada fase de la implementación. Además, se deberá establecer un plan de capacitación y comunicación involucrado en el proceso.

- Implementación de Herramientas de Monitoreo: Se debe implementar herramientas de monitoreo que les permitan supervisar continuamente el desempeño del sistema de gestión de riesgos. Estas herramientas pueden incluir sistemas de alerta temprana, paneles de control en tiempo real y registros de auditoría.
- Definición de Métricas de Desempeño: Es importante definir métricas de desempeño claras y específicas para evaluar la efectividad del sistema de gestión de riesgos. Estas métricas pueden incluir la frecuencia de identificación de riesgos, el tiempo de respuesta a incidentes y la tasa de cumplimiento de políticas y procedimientos.

1. Encuesta Interna sobre Identificación de Riesgos

Nota: previo al envío de la encuesta es necesario enviar un correo informativo sobre los diferentes tipos de riesgo explicados en este documento.

Estimado colaborador,

Agradecemos su participación en esta encuesta interna diseñada para identificar posibles riesgos en nuestras operaciones. Sus respuestas son fundamentales para ayudarnos a comprender mejor los desafíos que enfrentamos y tomar medidas proactivas para mitigarlos. Por favor, tómese unos minutos para completar esta encuesta de manera honesta y reflexiva.

1. ¿En qué departamento trabajas?

(Crear combo de opciones de los departamentos actuales)

2. ¿Qué tipo de riesgos crees que podrían afectar a nuestra empresa? (Selecciona todas las opciones que consideres aplicables)

Nota: no debe ser de respuesta obligatoria

Riesgos Financieros

Riesgos Operativos

Riesgos de Seguridad de la Información

Riesgos de Cumplimiento Legal y Regulatorio

Riesgos de Reputación

Riesgos de Salud y Seguridad Ocupacional

Otro (Especificar): _____

3. ¿Qué áreas específicas consideras que están más expuestas a riesgos en nuestro día a día? (Selecciona todas las opciones que consideres aplicables)

Gestión de Datos

Procesos Operativos

Seguridad Cibernética

Relaciones con Clientes

Relaciones con Proveedores

Gestión de Proyectos

Otro (Especificar): _____

4. ¿Cuáles consideras que son los riesgos más críticos para nuestra empresa en este momento?

Riesgos Financieros

Riesgos de Seguridad de la Información

Riesgos Operativos

Riesgos de Cumplimiento Legal y Regulatorio

Riesgos de Reputación

Otro (Especificar): _____

5. ¿Cuál es tu nivel de conocimiento sobre la gestión de riesgos en el trabajo?

Bajo

Moderado

Alto

6. ¿Qué sugerencias o recomendaciones tienes para mejorar la gestión de riesgos en nuestra empresa?

(Pregunta abierta)

7. ¿Tienes algún evento de riesgo que reportar?

Sí / No

8. ¿Te gustaría recibir capacitación adicional sobre gestión de riesgos?

Sí / No

Gracias por tu colaboración. Tus respuestas serán confidenciales y nos ayudarán a fortalecer nuestra capacidad para gestionar riesgos de manera efectiva.

2. Matriz evaluativa de resultados en preguntas claves sobre fase 0:

Interpretación de resultados sobre preguntas concretas.

Pregunta 2.

La no selección de esta pregunta permitirá establecer la participación porcentual general y por departamento de la lectura de correos informativos, ya que previamente se tuvo que haber enviado información sobre los tipos de riesgos.

El desconocimiento de los tipos de riesgos hace más probable que no reconozcan las señales de advertencia o no tomen las precauciones necesarias para mitigar los riesgos. Esto puede llevar a una

mayor exposición a situaciones de riesgo y aumentar la probabilidad de que ocurran incidentes perjudiciales.

Lectura de resultados.

Escenario 1: Riesgo Bajo

Porcentaje de Conocimiento: 80% - 100%

Implicaciones: El personal tiene un alto nivel de conocimiento sobre los tipos de riesgos a los que se enfrenta la organización. Esto permite reconocer las señales de advertencia, tomar medidas preventivas y responder adecuadamente ante situaciones de riesgo. La organización está bien preparada para gestionar y mitigar los riesgos internos de manera efectiva.

Escenario 2: Riesgo Medio

Porcentaje de Conocimiento: 50% - 79%

Implicaciones: El personal tiene un nivel moderado de conocimiento sobre los tipos de riesgos, pero existen algunas lagunas en su comprensión. Esto puede resultar en una capacidad limitada para identificar y abordar eficazmente ciertos riesgos internos. Se requiere una mayor concienciación y capacitación para mejorar la gestión de riesgos y reducir la vulnerabilidad de la organización.

Escenario 3: Riesgo Alto

Porcentaje de Conocimiento: 0% - 49%

Implicaciones: El personal tiene un bajo nivel de conocimiento sobre los tipos de riesgos, lo que aumenta significativamente la exposición de la organización a amenazas internas. Existe una alta probabilidad de que el personal no reconozca las señales de advertencia o no tome las medidas adecuadas para mitigar los riesgos, lo que puede conducir a incidentes graves y pérdidas significativas para la organización. Se requiere una acción inmediata para mejorar la concienciación y la capacitación en materia de gestión de riesgos.

Pregunta 3.

Debe utilizarse una matriz de riesgos para asignar una puntuación a cada área específica mencionada en la encuesta. Una vez obtenidas las puntuaciones de cada área, se puede realizar un análisis comparativo para identificar las áreas de mayor riesgo y priorizar la asignación de recursos para su gestión y mitigación. Este enfoque permite a la empresa centrarse en abordar los riesgos más críticos para proteger sus intereses y promover una cultura de gestión proactiva de riesgos.

Se asignará una puntuación de hasta 5 puntos, cada una de las respuestas consiste en:

Gestión de Datos (5 puntos):

Esta área es crítica debido a la naturaleza sensible de la información que se maneja. Los riesgos pueden incluir brechas de seguridad, pérdida de datos, incumplimiento de normativas de privacidad, entre otros. Se asigna una puntuación alta en la matriz de riesgos.

Procesos Operativos (4 puntos):

Los riesgos asociados con los procesos operativos pueden incluir errores humanos, fallas en los procesos, interrupciones del servicio, entre otros. Se puede asignar una puntuación moderada en la matriz de riesgos.

Seguridad Cibernética (5 puntos):

Dada la creciente amenaza de ciberataques y la dependencia de la tecnología en las operaciones comerciales, la seguridad cibernética puede considerarse un área de alto riesgo. Los riesgos pueden incluir ataques de malware, phishing, robo de datos, etc. Se asigna una puntuación alta en la matriz de riesgos.

Relaciones con Clientes (3 puntos):

Los riesgos en esta área pueden incluir insatisfacción del cliente, disputas contractuales, pérdida de clientes, etc. Dependiendo de la importancia de las relaciones con los clientes para la empresa, se puede asignar una puntuación moderada en la matriz de riesgos.

Relaciones con Proveedores (3 puntos):

Los riesgos relacionados con los proveedores pueden incluir problemas de calidad, incumplimiento de contratos, interrupciones en la cadena de suministro, entre otros. Dependiendo de la dependencia, se puede asignar una puntuación moderada en la matriz de riesgos.

Gestión de Proyectos (3 puntos):

Los riesgos asociados con la gestión de proyectos pueden incluir retrasos en la entrega, sobrecostos, fallas en la ejecución, etc. Dependiendo de la importancia de los proyectos para la empresa, se puede asignar una puntuación moderada en la matriz de riesgos.

Otro (Especificar):

Se deben evaluar los riesgos específicos mencionados en esta categoría y asignarles una puntuación en función de su impacto potencial en la organización.

Pregunta 4.

Las respuestas serán obligatorias. Su resultado debe ser comparable con la pregunta 2, a fin de determinar la sinceridad de las respuestas. El uso de otros debería ser la ausencia de respuestas en el comparativo con la pregunta 2.

Pregunta 5.

Dependerá del resultado por cada respuesta el plan de acción:

Nivel de conocimiento Bajo

Porcentaje de Respuestas: 0% - 33%

Plan de Acción:

- ➔ Realizar una evaluación detallada de las necesidades de capacitación del personal en gestión de riesgos.
- ➔ Desarrollar e implementar programas de capacitación específicos sobre gestión de riesgos adaptados a las necesidades identificadas.
- ➔ Proporcionar recursos adicionales, como materiales educativos y sesiones de formación, para mejorar la comprensión y concienciación sobre la gestión de riesgos en el trabajo.
- ➔ Establecer un sistema de seguimiento para evaluar regularmente el progreso y el nivel de conocimiento del personal en gestión de riesgos.

Nivel de Conocimiento: Moderado

Porcentaje de Respuestas: 34% - 66%

Plan de Acción:

Reforzar la formación existente sobre gestión de riesgos mediante la implementación de sesiones de actualización y talleres prácticos.

- Fomentar la participación activa del personal en actividades relacionadas con la gestión de riesgos, como simulacros de emergencia y revisiones periódicas de riesgos.
- Promover una cultura organizacional que valore y fomente la comunicación abierta sobre los riesgos y la responsabilidad compartida en su gestión.
- Proporcionar recursos adicionales, como herramientas y guías de referencia, para facilitar la aplicación de conceptos de gestión de riesgos en el trabajo diario.

Nivel de Conocimiento: Alto

Porcentaje de Respuestas: 67% - 100%

Plan de Acción:

Reconocer y recompensar el conocimiento y el compromiso del personal en la gestión de riesgos.

- Facilitar oportunidades para que el personal asuma roles de liderazgo en la identificación, evaluación y mitigación de riesgos en sus áreas de trabajo.
- Promover la colaboración y el intercambio de buenas prácticas entre los empleados con un alto nivel de conocimiento en gestión de riesgos.
- Establecer un sistema de retroalimentación continua para capturar y compartir lecciones aprendidas y casos de éxito en la gestión de riesgos dentro de la empresa.

3. Propuesta de registro de eventos de riesgo.

[a] abiertas; **[c]** cerradas o con opciones definidas, **[p]** parámetro de fecha

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 a).	Bajo Moderado Alto Crítico	Abierto En Investigación Resuelto Cerrado

Conjunto a:

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.

Matriz de evaluación de resultados del evento:

Criterio	Peso del criterio	Escala de Valoración
Descripción del Evento	20%	Una vez analizado: Crítico (5) - Bajo (1)
Impacto del Evento	30%	Crítico (5) - Bajo (1)
Causas del Evento	20%	Significativas (5) - Menores (1)
Acciones Tomadas	20	Eficaces (5) - Insuficientes (1)
Estado del Evento	10%	Resuelto (5) - Abierto (1)

La nota ponderada del evento será comparada con el tipo de riesgo.

Tipo de Riesgo	1	2	3	4	5
Riesgo de Crédito.					
Riesgo de Liquidez.					
Riesgo de Mercado.					
Riesgo Operativo.					
Riesgo Legal y Regulatorio.					
Riesgo de Reputación.					
Riesgo de fraude.					
Riesgo Tecnológico.					

Nivel de riesgo	Tipología	Acción
Baja	Tolerancia permitida	• Monitoreo continuo del riesgo para detectar cambios significativos. • Implementación de medidas de mitigación adicionales para reducir el riesgo a un nivel aceptable. • Revisión regular de los controles y procedimientos para garantizar su eficacia. • Comunicación proactiva con las partes interesadas sobre el estado del riesgo y las acciones tomadas.
Media	Moderado y de intervención rápida	• Activación inmediata de los planes de contingencia y respuesta ante riesgos críticos. • Movilización rápida de recursos adicionales y asignación de responsabilidades claras. • Comunicación urgente y transparente con todas las partes interesadas sobre la naturaleza y el impacto del riesgo crítico. • Implementación de acciones correctivas inmediatas para minimizar el impacto y restaurar la estabilidad operativa.
Alta	Crítico y de intervención inmediata	• Acción inmediata para activar los planes de contingencia y respuesta ante riesgos críticos. • Movilización inmediata de todos los recursos necesarios y asignación de responsabilidades prioritarias. • Comunicación urgente, clara y transparente con todas las partes interesadas. • Implementación inmediata de medidas correctivas para mitigar el riesgo y restaurar la estabilidad operativa.