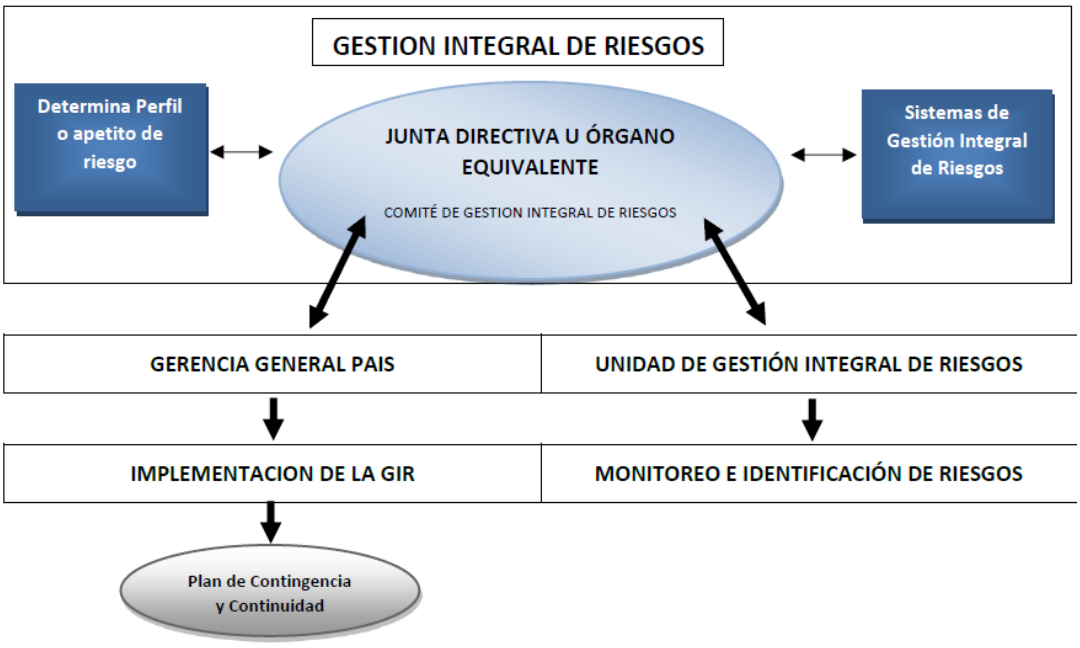
"INFORME DE EVALUACIÓN TÉCNICA
DE LA GESTIÓN INTEGRAL DE RIESGOS"
PACIFIC CREDIT RATING S.A. DE C.V.
Al 31 de diciembre de 2018

De acuerdo con las políticas y procedimientos establecidos en el Manual de Gestión Integral de Riesgos de PCR, el presente informe muestra las herramientas implementadas y las tareas ejecutadas para una adecuada gestión de riesgos en la entidad, de acuerdo con el tamaño y modelo de negocio de PCR.

Referido manual, define y delimita con claridad los posibles riesgos en que podría incurrir PCR y las políticas y procedimientos que deberán seguir los miembros de la institución para mitigar dichos riesgos.

1. Estructura organizativa para la gestión integral de riesgos



1.1 La estructura organizacional para la gestión integral de riesgos delimita claramente las obligaciones, funciones y responsabilidades, así como los niveles de dependencia. La Gestión Integral de Riesgos de PCR considera los requerimientos normativos del ente regulador en cuanto a la estructura y funciones para la Gestión de Riesgos.

a) La Junta Directiva es la responsable de establecer y supervisar el cumplimiento de las políticas y procedimientos para gestionar apropiadamente los riesgos que la entidad afronta. Además, velar por el cumplimiento de las disposiciones normativas

de los entes reguladores, así como de la aprobación del Manual de Gestión Integral de Riesgos y de sus respectivas modificaciones o actualizaciones.

b) El Comité de Gestión Integral de Riesgos es responsable de diseñar y proponer para la aprobación del Junta Directiva la estructura organizacional, estrategias, manuales, políticas y procedimientos para la gestión integral de riesgos, considerando las etapas de identificación, medición, monitoreo, control, mitigación y divulgación de riesgos, así como validar las metodologías para aplicar estas etapas

c) La Gerencia de la Entidad es la responsable de implementar la Gestión Integral de Riesgos de acuerdo con las políticas y procedimientos aprobadas por la Junta Directiva u órgano equivalente, velando por su adecuado seguimiento y cumplimiento al interior de la Entidad.

d) La Unidad de Gestión Integral de Riesgos será la encargada de ejecutar las políticas y procedimientos, de conformidad con lo establecido en la normativa del ente regulador y/o el Manual de Gestión Integral de Riesgos. Esta unidad tendrá como principal función la de identificar, medir, monitorear, controlar, mitigar y divulgar los diferentes tipos de riesgo y la interrelación que existe entre los mismos, en forma independiente de las áreas de negocios y de registro de operaciones.

2. Detalle de los principales riesgos asumidos por las actividades de PCR

2.1 Riesgos identificados

Se identifica formalmente los tipos de riesgo a los cuales se encuentra expuesto PCR de acuerdo con el siguiente detalle y según su nivel de relevancia:

a) Riesgo Operacional
b) Riesgo de Gobierno Corporativo
c) Riesgo Reputacional
d) Riesgo Legal
e) Riesgo de Cumplimiento
f) Riesgo de Contraparte
g) Riesgo de Concentración
h) Riesgo Tecnológico

Por el modelo de negocio de PCR, el **Riesgo Operacional** se constituye en el más relevante:

Fraude Interno: Actos destinados a defraudar, usurpar la propiedad o evadir la regulación, la ley, o las políticas de la empresa que involucren al menos una parte interna (empleados, asesores, capital interno, etc.).

Riesgo	Probabilidad	Impacto	Grado de impacto
Robo o divulgación de información confidencial de los clientes.	Medio	• Compromisos legales y económicos con los clientes afectados y/o con los entes reguladores. • Podría afectar el riesgo reputacional de la empresa.	Alto
Servicios profesionales deficientes que	Medio	Retraso en los procesos para continuar con el desarrollo de las actividades de la empresa.	Medio

potencialmente dañen a la compañía.		Compromisos económicos por multas impuestas por los reguladores.	
Robo de activos de la compañía por parte de los miembros de la empresa.	Bajo	Erogaciones económicas no presupuestadas para remplazar los activos, así como el retraso en los procesos para continuar con el desarrollo de las actividades de la empresa.	Bajo
Alteración de las clasificaciones otorgadas.	Bajo	• Compromisos legales y económicos con los clientes afectados y/o con los entes reguladores. • Podría afectar el riesgo reputacional de la empresa.	Alto

Fraude Externo: Actos por parte de terceros destinados a defraudar, usurpar la propiedad o ley (robos y falsificaciones, intromisión a sistemas informáticos).

Riesgo	Probabilidad	Impacto	Grado de impacto
Entrega de información falsa por parte de los clientes o representantes,	Medio	• Sanciones por parte de los reguladores. Compromisos legales por las alteraciones en la información. • Podría afectar el riesgo reputacional de la empresa.	Alto
Robo de información confidencial de los clientes.	Medio	• Compromisos legales y económicos con los clientes afectados y/o con los entes reguladores. • Podría afectar el riesgo reputacional de la empresa.	Medio
Atraso de pago o impagos de los clientes o representantes.	Bajo	Falta de pago de los compromisos económicos con proveedores y otros. Perdida de liquidez interna. Perdida financiera de la compañía.	Bajo
Intromisión a los sistemas informáticos locales.	Bajo	• Perdida de información confidencial. Compromisos económicos y legales con clientes afectados e instituciones legales. • Podría afectar el riesgo reputacional de la empresa.	Bajo

Prácticas de empleo y seguridad ocupacional inadecuados: Actos ilegales frente a las normas laborales que resulten en pagos por perjuicios al personal, o reclamos por seguridad o por salud.

Riesgo	Probabilidad	Impacto	Grado de impacto
Incumplimiento de la legislación local y los códigos internos de la organización.	Medio	• Falta a los compromisos legales y económicos con los empleados e instituciones competentes, posibles demandas y perjuicios. • Podría afectar el riesgo reputacional de la empresa.	Alto
Exposición a riesgos ocupacionales u otros.	Medio	• Compromisos legales y económicos con los empleados e instituciones involucradas. • Podría afectar el riesgo reputacional de la empresa.	Bajo
Comportamientos inapropiados de los empleados.	Bajo	• Compromisos legales y económicos con los empleados e instituciones involucradas. • Podría afectar el riesgo reputacional de la empresa.	Bajo
Omisiones y/o errores en las obligaciones otorgadas a los empleados.	Bajo	Compromisos con el desarrollo de actividades internas, posibles multas por parte de los reguladores por incumplimiento a la normativa	Bajo

Prácticas relacionadas con los clientes, productos y negocios: Fallas negligentes o no intencionadas que impidan cumplir con las obligaciones profesionales con clientes específicos o derivadas de la naturaleza del diseño de un producto.

Riesgo	Probabilidad	Impacto	Grado de impacto
Errores en las clasificaciones otorgadas a clientes.	Bajo	• Compromisos legales y económicos con los clientes afectados. Compromisos económicos por multas impuestas por los reguladores. • Podría afectar el riesgo reputacional de la empresa	Alto
Errores en los informes de clasificación	Bajo	• Incumplimiento a la normativa que deriven compromiso legal. • Podría afectar el riesgo reputacional de la empresa	Alto
Envío de información confidencial a terceras partes.	Bajo	• Compromisos legales y económicos con los clientes afectados. Compromisos económicos por multas impuestas por los reguladores.	Medio

		• Podría afectar el riesgo reputacional de la empresa.	
Incumplimiento de normas y/o leyes locales.	Bajo	• Compromisos económicos por multas impuestas por los reguladores. • Podría afectar el riesgo reputacional de la empresa.	Alto
Incumplimiento o errores en procesos internos de trabajo.	Bajo	• Compromisos legales y económicos con los clientes afectados. Compromisos económicos por multas impuestas por el sistema. • Podría afectar el riesgo reputacional de la empresa.	Bajo

Daño a los activos físicos: Perdida o daño a los activos físicos debido a desastres naturales u otros eventos.

Riesgo	Probabilidad	Impacto	Grado de impacto
Destrucción o daño de equipo.	Bajo	Compromisos económicos por remplazar total o parcial los equipos. Interrupción en el proceso interno de la empresa.	Bajo
Robo de equipo o materiales.	Bajo	Compromisos económicos por remplazar total o parcial los equipos. Interrupción en el proceso interno de la empresa.	Bajo

Interrupción del negocio y fallas del sistema: Interrupción en las actividades, el negocio o fallas en los sistemas de información.

Riesgo	Probabilidad	Impacto	Grado de impacto
Pérdida de información en los discos de respaldo	Bajo	Pérdida de la información financiera de las instituciones clasificadas.	Alto
Interrupción de actividades del negocio causadas por desastres naturales o eventos fortuitos	Medio	Interrupción en el proceso interno de la empresa. Compromisos legales y económicos con los clientes si resultaran afectados.	Bajo
Intromisión al sistema de correos y otros sistemas, por terceros	Medio	• Interrupción en el proceso interno de la empresa. Compromisos legales y económicos con los clientes si resultaran afectados. Compromisos económicos por multas impuestas por los reguladores. • Podría afectar el riesgo reputacional de la empresa.	Bajo

Pérdida de información por eventos fortuitos	Medio	• Interrupción en el proceso interno de la empresa. Compromisos legales y económicos con los clientes si resultaran afectados. • Podría afectar el riesgo reputacional de la empresa.	Alto
Daño de equipo e inoperatividad del mismo	Bajo	Compromisos económicos por remplazar total o parcial los equipos. Interrupción en el proceso interno de la empresa.	Bajo
Robo de equipo, sistemas u otros.	Bajo	Compromisos económicos por remplazar total o parcial los equipos. Interrupción en el proceso interno de la empresa.	Bajo
Perdida de comunicación con otros agentes por eventos fortuitos.	Bajo	Interrupción en el proceso interno de la empresa. Compromisos económicos por recobrar la comunicación entre la empresa y terceros.	Bajo

3. Las políticas actualizadas para la gestión integral de riesgos

Las políticas establecidas por PCR responden a la complejidad y al volumen de las operaciones que caracterizan al modelo de negocios y al perfil de riesgos que está asumiendo la entidad, estas políticas establecen los niveles de exposición considerados como aceptables para cada tipo de riesgo. Estos niveles pueden enunciarse de distinta forma, pudiendo entre otros, expresarse a través de restricciones para realizar determinadas operaciones o mediante la definición de límites de tolerancia al riesgo.

Políticas de identificación del Riesgo

Se identifica formalmente los tipos de riesgo a los cuales se encuentra expuesto PCR de acuerdo con el siguiente detalle y según su nivel de relevancia:

a) Riesgo Operacional
b) Riesgo de Gobierno Corporativo
c) Riesgo Reputacional
d) Riesgo Legal
e) Riesgo de Cumplimiento
f) Riesgo de Contraparte
g) Riesgo de Concentración
h) Riesgo Tecnológico

Por el modelo de negocio de PCR, el Riesgo Operacional se constituye en el más relevante

Políticas de medición del Riesgo

Según los tipos de riesgo identificados, se desarrollaron metodologías específicas para la cuantificación de niveles de exposición al Riesgo Operacional, Gobierno corporativo, Riesgo reputacional, Riesgo legal, Riesgo de cumplimiento, Riesgo de contraparte, Riesgo de concentración, y Riesgo Tecnológico, considerando toda la gama de operaciones que se realiza. La medición se basa en la determinación de la frecuencia e impacto de las pérdidas

que podrían ocurrir, como consecuencia de la materialización de los eventos adversos inherentes a cada uno de dichos riesgos.

Políticas de Monitoreo y Control

Cada instancia de PCR inmersa en la gestión de riesgos (Gerencia de País, Analistas u otro personal), deberá reportar la ocurrencia de eventos de riego que ayuden a detectar y corregir rápidamente deficiencias en las políticas, procesos y procedimientos. Se instrumenta este reporte con el envío electrónico semanal (o diario si el evento lo amerita) de formularios específicamente creados para este fin. La unidad de Gestión Integral de Riesgos establecerá controles preventivos con la finalidad de disminuir la probabilidad de ocurrencia de un evento, que podría originar pérdidas, considerando todos los riesgos a los que se enfrenta la entidad. Dado el modelo de negocio de PCR, se deberá contar con un Calendario de Obligaciones, el cual permita hacer un seguimiento permanente a todas las obligaciones, normativas y no normativas, de la entidad.

Políticas de Mitigación

Ante la presencia de un evento de riesgo que pueda generar pérdidas a la entidad y comprometer sus operaciones, PCR deberá aplicar un Plan de Contingencia que le permita administrar esta situación. El plan de contingencia debe consignar estrategias para manejar situaciones de crisis, así como escenarios de riesgo extremo.

Deberá considerar como mínimo los siguientes aspectos:

a) Las Situaciones que activan su aplicación
b) Las estrategias y procedimientos para administrar situaciones eventuales
c) Un análisis de costos de las diversas alternativas asumidas
d) Los funcionarios responsables de su aplicación.
e) Políticas y procedimientos comunicacionales con grupos de interés

Políticas de divulgación

La Junta Directiva, Comité de Riesgos y la Gerencia son informados periódicamente sobre los eventos de riesgo que se presentan en la entidad, la Unidad de Riesgos recibe reportes semanales de la unidad de Análisis y a partir de estos se elaboran los reportes mensuales e informes trimestrales.

4. Descripción de las metodologías, sistemas y herramientas para la Gestión de Riesgos

PCR cuanta con una matriz de factores de riesgo, la cual describe los riesgos a los cuales está expuesta la entidad y su interrelación. Al presentarse en la entidad uno o más de estos riesgos, esto es reportado semanalmente (o de inmediato si el evento lo amerita) por los funcionarios de PCR al Responsable de la Gestión Integral de Riesgos a través del llenado y envío del “Reporte de Factores de Riesgo”. La Unidad de Riesgos procede a monitorear el evento e implementar las medidas para poder mitigar el efecto que pudiera tener. Dado que PCR es una entidad que opera en el mercado de valores, debe cumplir diferentes obligaciones (laborales, impositivas, regulatorias, etc.), para asegurar esto, se estableció un “Sistema de Control de Obligaciones” a través del cual se monitorea el cumplimiento de obligaciones en los plazos y condiciones requeridas por los diferentes entes reguladores. La Unidad de Riesgos emite informes mensuales, trimestrales y anuales (de acuerdo con la regulación local) para divulgar a las instancias que corresponde

5. Resultados de las evaluaciones efectuadas a la gestión integral de riesgos y acciones tomadas

La unidad de riesgos realiza de manera trimestral las evaluaciones a los riesgos descritos en el Manual de Gestión Integral de Riesgos, en concordancia a la normativa local regulatoria. Los resultados de esta evaluación son los siguientes:

5.1 Riesgos Operativos

Tipo de riesgo	Riesgos Reales	Resultados de las evaluaciones	Controles /acciones tomadas
Operacional	Uso indebido de la información de los clientes	No se reportó malas prácticas de analistas con respecto a la información de los clientes	- Acuerdo de Confidencialidad. - Plan de Seguridad de la Información. - Acceso al correo corporativo. - Salvaguarda de la información física
	Falta de Objetividad e independencia de criterios	No se reportó falta de objetividad e independencia	- Firma de recepción del Código de Ética y Conducta. - Canal de comunicación directo e independiente para el reporte de operaciones ilícitas y sospechosas. - Evaluación del Código de Ética y Conducta a todo el personal.
	No contar con personal idóneo para la calificación	No se reportó deficiencias en la contratación de personal	- Código de Ética y Conducta. - Revisión exhaustiva de los Curriculum vitae.
	Desconocimiento de metodologías y normativas del regulador	No se reportó	- Código de Ética y Conducta. - Programa de capacitación anual.
	Cliente oculte información sensible	No se reportó retención de información por parte del cliente.	- Código de Ética y Conducta. - Acuerdo de confidencialidad - Administración y Control de Calificaciones.
	Robo de activos de la compañía	No se reportó robo de activos fijos	- Procedimientos aprobados para la capitalización, movimiento e inventario del activo fijo. - Inventario de activo fijo anual.
	Alteraciones de las calificaciones otorgadas	No se reportó alteraciones en las calificaciones otorgadas	- Código de Ética y Conducta. - Administración y Control de Calificaciones.

5.2 Riesgos Informáticos y Continuidad del negocio

Tipo de riesgo	Riesgos Reales	Resultados de las evaluaciones	Controles / acciones tomadas
Informáticos y	Pérdida de información		- Plan de Seguridad de la información. - Se realizan copias de back-up.

Continuidad del negocio	en los discos de respaldo	No se reportó pérdidas de información en los discos de respaldo	- Toda nuestra información comercial y de análisis de riesgos se encuentra almacenada en un software de alta calidad.
	Interrupción de actividades del negocio por desastres naturales o eventos fortuitos	No se reportó la interrupción de las actividades del negocio por desastres naturales o eventos fortuitos	- Plan de Seguridad de la información - Evaluación y Ejecución del Plan de Contingencia
	Intromisión al sistema de correos y otros sistemas, por terceros	No se reportó intromisiones no permitidas a los correos electrónicos y sistemas	-Se tiene controles de accesos a redes, gestión de privilegios y claves de usuario. - Acuerdos de confidencialidad
	Pérdida de información por eventos fortuitos	No se reportó pérdida de información por eventos fortuitos	- Plan de Seguridad de la información - Evaluación y Ejecución del Plan de Contingencia
	Robo de equipo o inoperatividad del mismo	No se reportó	- Inventario anual de activo fijo físico. - Inventario anual de software. - Controles para la seguridad de los recursos.
	Perdida de comunicación con otros agentes por eventos fortuitos	No se reportó	-Plan de seguridad de la información - Evaluación y Ejecución del Plan de Contingencia

5.3 Otros riesgos

Tipo de riesgo	Riesgos Reales	Resultados de las evaluaciones	Controles / acciones tomadas
Otros	Fallas en el back-up de información	No se reportó fallas	Plan de seguridad de la información
	No pago de proveedores	No se presentó	Gestión de cobranza
	Fallas en conexión de internet	En pocas situaciones se presenta lentitud del correo electrónico	
	Suspensión de comités	No se presentó suspensión de comités	
	Observaciones a informes de clasificación por parte de SSF	No se presentó observación	
	Observaciones de la SSF por auditoria	No se presentó observación	

	Observaciones a informes por parte de clientes	No se presentó	
	Comités programados y no realizados	No se presentó	
	No entrega de informes de clasificación en tiempo requerido	No se presentó	
	Renuncia o despido de integrante	Se produjo el retiro repentino del Auditor Interno de la entidad	El evento fue mitigado con la rápida incorporación de nuevo personal

6. Proyectos asociados a la gestión de riesgos a desarrollar en el siguiente ejercicio

6.1 Se promoverá la cultura de riesgos en todos los funcionarios de la institución mediante cursos de capacitación programados que apoyen la identificación y mitigación de riesgos, de acuerdo con el plan de trabajo anual de la Unidad de Riesgos y los programas de capacitación de PCR.

6.2 PCR realizará anualmente el Análisis de Vulnerabilidades (Ethical Hacking), el cual consta de un informe técnico por la realización de pruebas, análisis y resultados obtenidos con base a las herramientas utilizadas para el análisis y gestión de los riesgos encontrados, así como las posibles fallas, amenazas o vulnerabilidades que pueden afectar directa o indirectamente la seguridad de la información de PCR.

7. Establecimiento del plan de capacitación relacionado a la gestión integral de riesgos

Área Responsable	Actividad	Cronograma de evaluación de lectura
Unidad de Riesgos	Capacitación: Gestión Integral de Riesgos	Febrero y marzo 2019

8. Conclusiones generales sobre la gestión de riesgos

Por el año 2018 no se presentaron eventos de riesgo que pudieran afectar los resultados esperados por la entidad o la continuidad de operaciones, la gestión interna fue eficiente y los instrumentos internos de control fueron aplicados correctamente.

Yessid Ergueta Soruco
Responsable de la Unidad de Riesgos