"INFORME DE EVALUACIÓN TÉCNICA
DE LA GESTIÓN INTEGRAL DE RIESGOS"
PACIFIC CREDIT RATING S.A. DE C.V.
Al 31 de diciembre de 2015

El informe se basa en "***Manual de Riesgos Operacionales y Reputacionales"***, mismo que se rige por las normas y regulaciones estipuladas por los entes reguladores de cada mercado en los que PCR presta servicios. Dicho Manual, define y delimita con claridad los posibles riesgos en que podría incurrir, las políticas y procedimientos que deberán seguir todos los miembros de la institución para mitigar dichos riesgos.

i. La estructura organizativa para la gestión integral de riesgos:

ii. Detalle de los principales riesgos asumidos por las actividades de la entidad;

Riesgos: identificación y medición

1.1 Riesgos identificados:

1.1.1 **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 potencialmente dañen a	Medio	Retraso en los procesos para continuar con el desarrollo de las actividades de la empresa.	Medio

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

1.1.2 **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

1.1.3 **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

1.1.4 **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. • Podría afectar el riesgo reputacional de la empresa.	Medio

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

1.1.5 **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

1.1.6 **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
Perdida de información	Medio	• Interrupción en el proceso	Alto

por eventos fortuitos.		interno de la empresa. Compromisos legales y económicos con los clientes afectados. • Podría afectar el riesgo reputacional de la empresa.	
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

iii. Las políticas actualizadas para la gestión integral de riesgos.

2. Políticas de mitigación

2.1 Fraude Interno

2.1.1 PCR mantendrá y cumplirá una serie de políticas en el proceso de contratación de personal, contempladas en el código de conducta, asegurando la integridad de la información brindada por los candidatos a los puestos dentro de la compañía, revisión de referencias; así como la integridad moral y ética de los futuros empleados de la compañía.

2.1.2 PCR cumplirá con el proceso establecido para otorgar clasificaciones de riesgo sobre la base de la metodología previamente aprobada, bajo la supervisión y revisión del Jefe de Análisis, investigación y desarrollo (JAID), y el comité de clasificación, formado por el Presidente de la compañía, el JAID, y otros miembros que se consideren para cada comité.

2.1.3 El personal de PCR deberá compartir la información y métodos de análisis, que requieran sus supervisores para su revisión.

2.1.4 PCR contratará exclusivamente a agentes externos de alto reconocimiento en el sector al que pertenecen. Para cada contratación será obligatorio la verificación de referencias de dicho proveedor.

2.1.5 El control de inventarios de activos y mobiliario será realizado anualmente. Asimismo, las órdenes de compra de insumos y equipo deberán de ser justificadas y aprobadas por el Gerente País.

2.1.6 El proceso de clasificación será revisado por el JAID, así como las propuestas de clasificación previo a su discusión en el comité de clasificación, para verificar su validez y que su lógica corresponda a la metodología y a la información de manera objetiva.

2.2 Fraude externo

2.2.1 La información recibida de parte de los clientes, para el proceso de clasificación, será verificada con la información de otras fuentes oficiales, cuando estas apliquen y estén

disponibles para su revisión. Por ejemplo, la Bolsa de Valores de El Salvador, la Superintendencia del Sistema Financiero, entre otros.

2.2.2 PCR realiza las gestiones de cobro apropiadas que se determinan de acuerdo a lo convenido en los contratos firmados con cada cliente.

2.2.3 PCR cuenta con políticas de seguridad de la información, establecidas y aprobadas previamente por el Área de Sistemas.

2.3 Prácticas de empleo y seguridad ocupacional inadecuados

2.3.1 PCR mantendrá y cumplirá las políticas del proceso de contratación de personal, contempladas en el Código de Conducta; las mismas que serán revisadas periódicamente para actualizarlas de acuerdo a los requerimientos necesarios de competencias del personal.

2.3.2 PCR realizará evaluaciones anuales del desempeño de todo su personal, así como brindará una retroalimentación de acuerdo a los niveles alcanzados por cada trabajador. En caso un trabajador muestre desempeño menor a lo esperado, podrá ser capacitado para su mejora. Si un trabajador obtiene notas de rendimiento por debajo de lo esperado se evaluará tomar acciones correctivas, incluye el término de la relación laboral.

2.3.3 Luego de cada evaluación de desempeño, la gerencia de PCR determinará metas y objetivos para cada empleado, de acuerdo a sus resultados y necesidades. El logro de estas metas será verificado en evaluaciones posteriores. Cada meta deberá ser medible, a realizarse en un tiempo determinado, y alcanzable.

2.3.4 El Gerente País se asegurará que se cumpla en su totalidad, la normativa local de trabajo, políticas de contratación, seguridad ocupacional, y otras normativas locales.

2.4 Prácticas relacionadas con los clientes, productos y negocios

2.4.1 El comité de clasificación será conformado por las áreas de análisis, presidencia, y representantes regionales de PCR, para asegurar la imparcialidad de los informes y las clasificaciones otorgadas.

2.4.2 La información confidencial de los clientes, clasificaciones y procedimientos internos será resguardada de acuerdo a los manuales internos del manejo de la información, asegurando su cumplimiento y seguridad.

2.5 Daño a los activos físicos

2.5.1 PCR mantendrá un respaldo de toda la información digital de los clientes, así como los informes creados internamente, plantillas de análisis, correos con información importante, entre otros.

2.5.2 PCR actualizará el respaldo mencionado en el punto anterior cada tres meses, para asegurar su validez. Este respaldo se mantendrá en un sistema local de almacenamiento, así como en servidores fuera de la locación física de la compañía, protegiendo la información en caso de catástrofes o siniestros de causa mayor, de acuerdo a lo establecido por el Área de Sistemas.

2.6 Interrupción del negocio y fallas del sistema

2.6.1 La información creada en el respaldo será accesible para otros analistas, manteniendo la continuidad de los procesos internos, en caso las instalaciones locales sean inaccesibles para los trabajadores de PCR El Salvador, o estos sean dañados e inutilizables, o en caso sean los empleados los que estén fuera de la disposición de realizar sus funciones.

2.6.2 PCR contará con un árbol de llamadas, para verificar el estado del personal en caso de emergencia. Una vez ubicado el personal, esta información será brindada al Gerente País para su conocimiento, y que este gestione la continuidad de las funciones en otras instalaciones.

3. Políticas de Monitoreo

3.1 Los objetivos y metas establecidas en la evaluación de personal serán considerados en evaluaciones futuras. Si los objetivos logrados por un empleado no superan el 60% o muestran una tendencia negativa, el Gerente País tomará las medidas pertinentes.

3.2 El personal de PCR podrá, en todo momento, expresar comentarios referentes al ambiente laboral; para poder establecer una discusión abierta y mejorar.

3.3 Todo cambio de clasificación de una entidad o instrumento financiero, será revisado bajo los parámetros establecidos en el Código de Ética y Código de Conducta de PCR.

3.4 El JAID verificará que los procedimientos de la clasificación se sigan de acuerdo a los manuales de la compañía.

3.5 Los clientes de PCR podrán, en todo momento, expresar comentarios referentes al servicio prestado. Estos serán de conocimiento directo e inmediato de la Presidencia.

3.6 El Jefe de Sistemas es responsable de verificar que la información se haya resguardado de forma segura, tanto en el sistema local como en servidores externos.

3.7 PCR, a través de su Gerente País podrá realizar auditorías internas para verificar el cumplimiento de estas políticas. Estas auditorías se realizaran al menos una vez por año, sin fechas previamente establecidas.

3.8 La Unidad de Riesgos, deberá monitorear diariamente todas las actividades que conlleven un riesgo para PCR a través de una matriz integral de riesgos (Anexo No.1).

3.9 La Unidad de Riesgos informará al Comité de Riesgos al existir eventos con grado de impacto medio y alto el mismo día que sucedan los mismos.

3.10 La Unidad de riesgos informará mensualmente al Comité de Riesgo a través de un resumen, los eventos sucedidos en el período.

3.11 El Comité de Riesgos informará trimestralmente a Junta Directiva, un resumen de los eventos de riesgos sucedidos en el período.

iv) Descripción de las metodologías, sistemas y herramientas utilizadas para cada uno de los riesgos;

La Unidad de Riesgos elaboró una matriz de seguimiento de los indicadores medibles, con el fin de tener la estadística de todos los eventos y de una manera diaria.

El seguimiento que se realizó para todos los meses del año 2015 fueron:

Riesgo de Fraude Interno	Probabilidad	Grado de impacto	1	2	3	4	5	6	7	8	9	10	11	12	Total Eventos
Robo o divulgación de información confidencial de los clientes.	Medio	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Servicios profesionales deficientes que potencialmente dañen a la compañía.	Medio	Medio	0	0	0	0	0	0	0	0	0	0	0	0	0
Robo de activos de la compañía por parte de los miembros de la empresa.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Alteración de las clasificaciones otorgadas.	Bajo	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Riesgo de Fraude Externo	**Probabilidad**														
Entrega de información falsa por parte de los clientes o representantes.	Medio	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Robo de información confidencial de los clientes.	Medio	Medio	0	0	0	0	0	0	0	0	0	0	0	0	0
Atraso de pago o impagos de los clientes o representantes.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Intromisión a los sistemas informáticos locales.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Riesgo por prácticas de empleo y seguridad ocupacional inadecuados	**Probabilidad**														**0**
Incumplimiento de la legislación local y los códigos internos de la organización.	Medio	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Exposición a riesgos ocupacionales u otros.	Medio	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Comportamientos inapropiados de los empleados.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Omisiones y/o errores en las obligaciones otorgadas a los empleados.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Riesgo por prácticas relacionadas con los clientes, productos y negocio	**Probabilidad**														
Errores en las clasificaciones otorgadas a clientes.	Bajo	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Envío de información confidencial a terceras partes.	Bajo	Medio	0	0	0	0	0	0	0	0	0	0	0	0	0
Incumplimiento de normas y/o leyes locales.	Bajo	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Incumplimiento o errores en procesos internos de trabajo.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Riesgo por daño a los activos físicos	**Probabilidad**														
Destrucción o daño de equipo.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Robo de equipo o materiales.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Riesgo por interrupción del negocio y fallas del sistema	**Probabilidad**														
Pérdida de información de discos de respaldo	Bajo	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Interrupción de actividades del negocio causadas por desastres naturales o eventos fortuitos.	Medio	Bajo	0	0	0	0	0	0	0	0	0	0	0	1	1
Intromisión al sistema de correos y otros sistemas, por terceros.	Medio	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Perdida de información por eventos fortuitos.	Medio	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Daño de equipo e inoperatividad del mismo.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	1	0	0	1
Robo de equipo, sistemas u otros.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Perdida de comunicación con otros agentes por eventos fortuitos.	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Total			**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**2**

Otros riesgos	Probabilidad														Total Eventos
Fallas en el back-up de información	Medio	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
No pago de proveedores	Medio	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Incapacidad por enfermedad de analista	Medio	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Falta de energía eléctrica	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Fallas en conexión de internet	Bajo	Bajo	0	0	0	0	0	0	0	0	0	0	0	0	0
Suspensión de Comités	Bajo	Medio	0	0	0	0	0	0	0	0	0	0	0	0	0
Observaciones a informes de clasificación por parte de SSF	Bajo	Alto	0	0	0	0	0	0	0	0	0	0	1	0	1
Observaciones de la SSF por auditoría	Bajo	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Observaciones a informes por parte de clientes	Bajo	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Comités programados y no realizados	Bajo	Medio	0	0	0	0	0	0	0	0	0	0	0	0	0
No entrega de informes de clasificación en tiempo legal requerido	Bajo	Alto	0	0	0	0	0	0	0	0	0	0	0	0	0
Renuncia o despido de analista	Bajo	Medio	0	0	0	0	0	0	0	0	0	0	1	0	1
Total			**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**0**	**2**

v) Los resultados de las evaluaciones efectuadas a la gestión integral de riesgos; y

1. Fraude Interno

Riesgo	Probabilidad	Eventos presentados durante el año 2015
Robo o divulgación de información confidencial de los clientes.	Medio	Ningún evento reportado
Servicios profesionales deficientes que potencialmente dañen a la compañía.	Medio	Ningún evento reportado
Robo de activos de la compañía por parte de los miembros de la empresa.	Bajo	Ningún evento reportado
Alteración de las clasificaciones otorgadas.	Bajo	Ningún evento reportado

2. Fraude Externo

Riesgo	Probabilidad	Eventos presentados durante el año 2015
Entrega de información falsa por parte de los clientes o representantes,	Medio	Ningún evento reportado
Robo de información confidencial de los clientes.	Medio	Ningún evento reportado.
Atraso de pago o impagos de los clientes o representantes.	Bajo	Ningún evento reportado
Intromisión a los sistemas informáticos locales.	Bajo	Ningún evento reportado

3. Prácticas de empleo y seguridad ocupacional inadecuados

Riesgo	Probabilidad	Eventos presentados durante el año 2015
Incumplimiento de la legislación local y los códigos internos de la organización.	Medio	Ningún evento reportado.
Exposición a riesgos ocupacionales u otros.	Medio	Ningún evento reportado.
Comportamientos inapropiados de los empleados.	Bajo	Ningún evento reportado.
Omisiones y/o errores en las obligaciones otorgadas a los empleados.	Bajo	Ningún evento reportado.

4. Prácticas relacionadas con los clientes, productos y negocios

Riesgo	Probabilidad	Eventos presentados durante el año 2015
Errores en las clasificaciones otorgadas a clientes.	Bajo	Ningún evento reportado.
Envío de información confidencial a terceras partes.	Bajo	Ningún evento reportado.

Incumplimiento de normas y/o leyes locales.	Bajo	Ningún evento reportado.
Incumplimiento o errores en procesos internos de trabajo.	Bajo	Ningún evento reportado.

5. Daño a los activos físicos

Riesgo	Probabilidad	Eventos presentados durante el año 2015
Destrucción o daño de equipo.	Bajo	Ningún evento reportado.
Robo de equipo o materiales.	Bajo	Ningún evento reportado.

6. Interrupción del negocio y fallas del sistema

Riesgo	Probabilidad	Eventos presentados durante el año 2015
Interrupción de actividades del negocio causadas por desastres naturales o eventos fortuitos.	Medio	Internet inestable provocó retrasos en algunas actividades relacionadas al proceso de calificación.
Intromisión al sistema de correos y otros sistemas, por terceros.	Medio	Ningún evento reportado
Perdida de información por eventos fortuitos.	Medio	Ningún evento reportado
Daño de equipo e inoperatividad del mismo.	Bajo	Una máquina enviada a reparación.
Robo de equipo, sistemas u otros.	Bajo	Ningún evento reportado
Perdida de comunicación con otros agentes por eventos fortuitos.	Bajo	Ningún evento reportado

En conclusión, para el año 2015 no existieron eventos que afectaran la continuidad del negocio en los diferentes riesgos que se miden en la institución.

vi) Proyectos asociados a la gestión de riesgos a desarrollar en el ejercicio siguiente al reportado.

Dentro del plan de trabajo de la Unidad de Riesgo para el año 2016, contempla lo siguiente:

a. Revisión constante del manual de riesgos operacionales y reputacionales.
b. Actualización de la matriz integral de riesgos.
c. Realizar una capacitación al personal sobre los diferentes riesgos que se expone la institución y como mitigarlos.