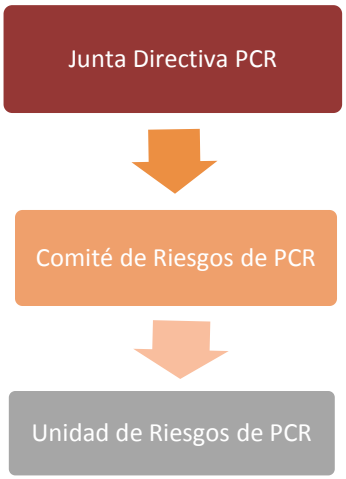
"INFORME DE EVALUACIÓN TÉCNICA
DE LA GESTIÓN INTEGRAL DE RIESGOS"
PACIFIC CREDIT RATING S.A. DE C.V.
Al 31 de diciembre de 2016

El informe se basa en el "***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.

1. Estructura organizativa para la gestión integral de riesgos



1.1 La estructura de PCR está diseñada de tal manera que le permite disminuir los posibles riesgos a los cuales puede estar expuesta producto del objeto de sus operaciones. El organigrama y el Manual de Organización y Funciones de PCR muestran la estructura para llevar a cabo las siguientes actividades de control:

- El Directorio, que es un órgano de administración entre los accionistas y la plana gerencial, ejecuta el seguimiento del desempeño de los controles internos. Adicionalmente, supervisará el funcionamiento de los siguientes Comités: de Negocios, de Operaciones, de Finanzas, y de Criterios y Metodologías.
- El Presidente Ejecutivo supervisa directamente al Jefe de Asuntos Regulatorios Globales, al Jefe de Cumplimiento Normativo y Auditoría Interna, y a los siguientes Directores: Negocios, Operaciones, Análisis, Relaciones con el Mercado. Establece estructuras, líneas de reporte, y autoridades apropiadas así como responsabilidades relacionadas a los objetivos.
- El Director de Negocios supervisa a las Gerencia País de todos los países donde PCR tiene operaciones.

1.2 El órgano máximo de administración de PCR ha delegado la responsabilidad primaria de la gestión integral de riesgos al Jefe de Cumplimiento Normativo y Auditoría Interna (JCNAI).

1.3 El Directorio u órgano competente es responsable de supervisar la efectividad del Sistema de Control Interno, y de establecer todo lo que sea necesario para que la persona encargada ejerza sus funciones y le reporte directamente.

1.4 En PCR tenemos mapeada nuestra exposición al riesgo, por ello, constantemente establecemos y actualizamos los procedimientos que rigen nuestro accionar y mitigan los riesgos.

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

2.1 Riesgos identificados:

2.1.1 **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 la compañía.	Medio	Retraso en los procesos para continuar con el desarrollo de las actividades de la empresa. Compromisos económicos por multas impuestas por los reguladores.	Medio
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

2.1.2 **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

2.1.3 **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

2.1.4 **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

2.1.5 **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

2.1.6 **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
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. Políticas y herramientas de mitigación para la gestión integral de riesgos

3.1 Fraude Interno

3.1.1 PCR mantiene y cumple 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.

3.1.2 PCR cumple 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 y Control de Calidad (JACC), y el comité de clasificación, formado por el Presidente de la compañía, el JACC, y otros miembros que se consideren para cada comité.

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

3.1.4 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.

3.1.5 El control de inventarios de activos y mobiliario es realizado anualmente. Asimismo, las órdenes de compra de insumos y equipo son justificadas y aprobadas por el Gerente País.

3.1.6 El proceso de clasificación será revisado por el JACC, así como las propuestas de clasificación previa 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.

3.2 Fraude externo

3.2.1 La información recibida de parte de los clientes, para el proceso de clasificación es 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.

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

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

3.3 Prácticas de empleo y seguridad ocupacional inadecuados

3.3.1 PCR mantiene y cumple las políticas del proceso de contratación de personal, contempladas en el Código de Conducta; las mismas que son revisadas periódicamente para actualizarlas de acuerdo a los requerimientos necesarios de competencias del personal.

3.3.2 PCR realiza evaluaciones anuales del desempeño de todo su personal, así como brinda 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.

3.3.3 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.

3.3.4 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.

3.4 Prácticas relacionadas con los clientes, productos y negocios

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

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

3.5 Daño a los activos físicos

3.5.1 PCR mantiene 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.

3.5.2 PCR actualiza el respaldo mencionado en el punto anterior de manera diaria, para asegurar su validez. Este respaldo se mantiene en un sistema local de almacenamiento,

así como en servidores fuera de la locación física de la compañía (web), protegiendo la información en caso de catástrofes o siniestros de causa mayor, de acuerdo a lo establecido por el Área de Sistemas.

3.6 Interrupción del negocio y fallas del sistema

3.6.1 La información creada en el respaldo es 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.

3.6.2 PCR cuenta 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.

3.7 Programas de capacitación

3.7.1 La Alta Gerencia es responsable de garantizar que los empleados y ejecutivos involucrados en la gestión de riesgos sean capacitados en dichos temas. Para ello, se elabora un Plan de Capacitación Anual que incorpora el personal a capacitar y los temas a desarrollar con su respectiva calendarización.

3.7.2 Se establecerá un programa de divulgación a toda la organización, a fin de concientizar la cultura organizacional del riesgo en todos los empleados y niveles jerárquicos.

3.8 Prestación de servicios por terceros

3.8.1 PCR establece procedimientos para evaluar, supervisar y monitorear el desempeño de los servicios críticos brindados por terceros.

3.8.2 Los servicios críticos son aquellos que pueden interrumpir el normal desarrollo de nuestras operaciones. Entendiéndose como tal a los siguientes: servicios de soporte informático, servicio contable y asesoría legal.

3.8.3 Mantenemos contratos firmados con nuestros proveedores en los cuales se establecen el alcance del servicio, las responsabilidades del proveedor, y las nuestras como entidad.

3.8.4 En estos contratos incluiremos una cláusula a fin de que el proveedor documente los servicios brindados y garantice el adecuado uso de la información confidencial, el establecimiento de planes de contingencia y de continuidad del servicio brindado.

3.8.5 Se lleva un control centralizado de todos los servicios prestados por terceros. El cual estará a disposición de la Superintendencia.

3.9 Políticas de Monitoreo

3.9.1 Los objetivos y metas establecidas en la evaluación de desempeño serán considerados en evaluaciones futuras. Si los objetivos de desarrollo establecidos para un empleado en su evaluacion no se logran al menos en un 60% o muestran una tendencia negativa, el Gerente País tomará las medidas pertinentes.

3.9.2 Se realiza una encuesta anual de clima laboral en las distintas oficinas. Adicionalmente el personal de PCR puede en todo momento expresar comentarios referentes al ambiente laboral; para poder establecer una discusión abierta y positiva.

3.9.3 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.

3.9.4 El JACC y el Jefe de Metodologías verifican que los procedimientos de la clasificación se sigan de acuerdo a los manuales de la compañía.

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

3.9.6 PCR, a través de su Jefatura de Cumplimiento Normativo y Auditoría Interna 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.

4. 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 nuestro Manual de Riesgos Operacionales y Reputacionales. Los resultados de esta evaluación son los siguientes:

4.1 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 ni encontró malas prácticas de los 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 de los Códigos de Conducta y ética - Canal de Comunicación directo e independiente para el reporte de operaciones ilícitas y sospechosas. - Evaluación acerca de los Códigos de conducta y ética a todo el personal
	No contar con personal idóneo para la calificación	No se reportó deficiencias en la contratación de personal.	- Código de conducta - Código de ética - Revisión exhaustiva de los curriculum vitae
	Desconocimiento de las metodologías y normativas del regulador.	No se reportó desconocimiento de las metodologías y normativas.	- Código de conducta - Metodología divulgada en la página web de PCR.
	Cliente oculte información sensible	No se reportó retención de información por parte del cliente.	- Código de 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. - Realización de inventario de activo fijo anual.
	Alteraciones de las calificaciones otorgadas	No se reportó ni encontró alteraciones en las calificaciones otorgadas	- Código de conducta - Código de ética - Administración y Control de Calificaciones.

4.2 Riesgos Informáticos y Continuidad del negocio

Tipo de riesgo	Riesgos Reales	Resultados de las evaluaciones	Controles / acciones tomadas
Informáticos y Continuidad del negocio	Pérdida de información en los discos de respaldo	No se reportó pérdidas de información en los discos de respaldo	- Instructivo: Plan de Seguridad de la información. - Se realizan copias de back-up. - Toda nuestra información comercial y de análisis de riesgos se encuentra almacenada en un software de alta calidad.
	Interrupción de actividades del negocio causadas por desastres naturales o eventos fortuitos	No se reportó ni se evidenció la interrupción de las actividades del negocio por desastres naturales o eventos fortuitos	- Instructivo: Plan de Seguridad de la información - Instructivo: Evaluación y Ejecución del Plan de Contingencia

	Intromisión al sistema de correos y otros sistemas, por terceros	No se reportó intromisiones e ingresos no permitidos 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.	- Instructivo: Plan de Seguridad de la información - Instructivo: Evaluación y Ejecución del Plan de Contingencia
	Robo de equipo o inoperatividad del mismo	No se reportó robo de equipo ni inoperatividad del mismo.	- Realización de inventario anual de activo fijo físico. - Realización de inventario anual de software. - Controles para la seguridad de los recursos.
	Perdida de comunicación con otros agentes por eventos fortuitos	No se reportó pérdida de comunicación con otros agentes por evento fortuito	-Plan de seguridad de la información - Instructivo: Evaluación y Ejecución del Plan de Contingencia

4.3 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	
	No pago de proveedores	No se observó problemas de liquidez.	Gestión de los vencimientos de activos y pasivos para lograr el calce entre el flujo de ingresos y pagos futuros.
	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	Se observó una notificación a fin de mejorar nuestra adecuación a la normativa NRP-11	
	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	El Gerente de Centroamérica, el Sr. Francisco Santa Cruz renunció al cargo.	Se tomaron todas las medidas preventivas ante la desvinculación y sustitución.

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

5.1 Para el 2017 se procederá actualizar la estructura organizativa para la gestión integral de riesgos según la normativa vigente NRP-11, siendo la estructura de la siguiente manera:

5.1.1 El Comité de Riesgos de PCR estará integrado de la siguiente manera:

- Miembro de la Junta Directiva
- Gerente País
- Encargado de la Unidad de Riesgos

5.1.2 La Unidad de Riesgos de PCR está representada por la Jefatura de Cumplimiento Normativo y Auditoría Interna.

5.2 Se actualizará constantemente los números telefónicos personales de cada uno de nuestros integrantes a fin de mantener comunicación oportuna, y se trabajará en alternativas para determinar locales eventuales a fin de no interrumpir nuestras actividades producto de desastres naturales o eventos fortuitos.

5.3 PCR realizará anualmente el Análisis de Vulnerabilidades (Ethical Hacking), el cual consta de un informe técnico con 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.

5.4 Dentro del plan de trabajo de la Unidad de Riesgo para el año 2017 se contempla lo siguiente:

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

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

Integrante	**Posición**	**Procedimientos internos**				**Ente de regulación**
Karina Montoya	Coordinador País	*Metodologías * Procedimientos de análisis	Gobierno corporativo	Manual de Riesgos Operaciones y Reputacionales	* Manual de Control Interno * Plan de Seguridad de la información * Evaluación y Ejecución del Plan de Contingencias	Gestión Integral de Riesgos
Wilfredo Galicia	Analista Senior					
Luis Vega Villalobos	Analista Principal					
Yenci Mireya Sarceño Jimenez	Analista de Riesgo					
Waldo Adonay Arteaga Cornejo	Analista de Riesgo					
Wilfredo Vasquez Perez	Analista de Riesgo					
Alejandro Ulises Mejía Quintero	Analista de Riesgo					
Josué David Cortéz Gochez	Analista					
Programación 2017		II, III y IV Trimestre	III y IV Trimestre	III y IV Trimestre	III Trimestre	III Trimestre

7. Conclusiones generales sobre la gestión de riesgos

En el año 2016 no existieron eventos que afectaran la continuidad del negocio en ninguno de los diferentes riesgos que se miden en la institución.