INF. GIR. SV. N° 02/2021

Informe de Evaluación Técnica de la Gestión Integral de Riesgos de PCR Gestión 2020

San Salvador, 21 de abril de 2021

Índice de Contenido

INFORME

A: Oscar Jasaui
Karina Montoya
Daniela Urquizo
COMITÉ DE GESTIÓN INTEGRAL DE RIESGOS

DE: **RESPONSABLE DE GESTIÓN INTEGRAL DE RIESGOS**

REF: **INFORME DE EVALUACIÓN TÉCNICA DE LA GESTIÓN INTEGRAL DE RIESGOS AL 31 DE DICIEMBRE DE 2020**

FECHA: 21 de abril de 2021

I. ANTECEDENTES

- Artículo 31 del Capítulo VI "Transparencia de la Información" de las ***Normas Técnicas para la Gestión Integral de Riesgos de las Entidades de los Mercados Bursátiles (NRP-11)***, del Banco Central de la Reserva de El Salvador.

- Artículo 29, Capítulo IV "INFORMACIÓN Y CONTROL", de las ***Normas Técnicas para la Gestión de la Seguridad de la Información (NRP-23)***, del Banco Central de la Reserva de El Salvador.

- ***Manual de Gestión Integral de Riesgos*** de la Clasificadora de Riesgo Pacific Credit Rating (en adelante PCR), el cual señala que se debe mantener una adecuada comunicación entre la Junta Directiva, el Comité de GIR, y las demás áreas de la empresa, para la adecuada toma decisiones que permita gestionar los riesgos identificados.

II. OBJETIVOS

El presente informe tiene los siguientes objetivos:

- Exponer los resultados del proceso de gestión integral de riesgos de PCR durante la gestión 2020.

- Detallar el nivel de cumplimiento de los requisitos de la norma NRP-23 sobre Gestión de Seguridad de la Información hasta el cierre de la gestión 2020.

III. GESTIÓN INTEGRAL DE RIESGOS

III.a Estructura Organizativa para la gestión integral de riesgos

La estructura organizativa de PCR dedicada a la gestión integral de riesgos está conformada por la Junta Directiva, el Comité de Gestión Integral de Riesgos, la Alta Gerencia, y la Unidad de Riesgos.

A nivel específico, y de acuerdo con el tamaño y modelo de negocio de PCR, la Junta Directiva está compuesta por dos integrantes; el Comité de Gestión Integral de Riesgos está compuesto por tres integrantes, y la Unidad de Riesgos, por dos integrantes:

Órgano	Miembros	Puesto / Rol
Junta Directiva	• Oscar Jasaui • Victoria Fernández	• Presidente Ejecutivo • Director de Negocios
Comité de Gestión Integral de Riesgos	• Oscar Jasaui • Herbert Castro* • Daniela Urquizo** • Karina Montoya	• Presidente Ejecutivo • Jefe de la Unidad de Riesgos • Oficial de Gestión Integral de Riesgos • Coordinador País
Unidad de Gestión Integral de Riesgos	• Herbert Castro* • Daniela Urquizo** • Mauricio Jasaui	• Jefe de la Unidad de Riesgos • Oficial de Gestión Integral de Riesgos • Oficial de Cumplimiento

(*) : Desde el 23/04/2019 hasta el 22/07/2020
(**) : Desde el 23/07/2020 en adelante

Las funciones y responsabilidades de cada órgano se detallan a continuación:

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, debe 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 el responsable de proponer para aprobación de la Junta Directiva, las estrategias, manuales, metodologías, políticas y procedimientos a aplicar en la gestión integral de riesgos, considerando las etapas de identificación, medición, monitoreo, control, mitigación y divulgación de riesgos.
c) **La Alta Gerencia** de la entidad es la responsable de cumplir y hacer cumplir las políticas y procedimientos aprobados por la Junta Directiva para la gestión integral de riesgos.
d) **La Unidad de Gestión Integral de Riesgos** es la encargada de diseñar y proponer para aprobación del Comité de GIR, las estrategias, manuales, metodologías, planes de continuidad, políticas, y procedimientos a aplicar para la gestión

integral de riesgos, considerando las etapas de identificación, medición, monitoreo, control, mitigación y divulgación de riesgos.

También es función de la Unidad de Gestión Integral de Riesgos, el informar periódicamente a su Comité sobre la evolución de los principales riesgos asumidos por la entidad, emitiendo recomendaciones y dando seguimiento a los niveles de exposición, y tolerancia al riesgo.

III.b Detalle de los principales riesgos asumidos por las actividades de PCR

PCR reconoce que la gestión integral de riesgos consiste en un proceso estructurado para identificar, medir, monitorear, controlar, mitigar y divulgar todos los riesgos a los cuales está expuesta, pudiendo estos interrelacionarse entre sí.

Al tratarse de una empresa Clasificadora de Riesgos, PCR se encuentra expuesta a los siguientes tipos de riesgo:

- Riesgo Operativo (incluye el Riesgo Legal y el Riesgo Tecnológico)
- Riesgo de Seguridad de la Información
- Riesgo de Contraparte
- Riesgo de Liquidez
- Riesgo de Cumplimiento
- Riesgo de Gobierno Corporativo

A continuación, se describe los principales riesgos identificados por cada tipo de riesgo citado.

III.b.1 Riesgo Operativo (incluye Riesgo Legal y Riesgo Tecnológico)

Producto de la aplicación de las ***Metodologías para la Gestión Integral de Riesgos en PCR*** aprobadas en la Junta Directiva N°35 de fecha 29.04.2020, se identificaron y gestionaron los siguientes riesgos operativos inherentes al giro del negocio, los cuales cuentan con controles suficientes para prevenir su materialización:

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31-12-2020
R1	**Uso indebido de información del cliente para beneficio propio o de terceros**	Office 365 controla y previene que archivos cargados en la nube se envíen por cualquier correo electrónico que no sea el corporativo.	Se evaluará realizar un upgrade de la licencia de Office 365 para la implementación de controles más rigurosos. (Azure AD).	**Concluido.** Se realizó un upgrade a la licencia de Office 365 a Office 365 Premium Business desde julio de 2020.

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31-12-2020
R2	**Robo del know-how de PCR (metodologías, plantillas etc.) de PCR para beneficio propio o de terceros**	El Acuerdo de Confidencialidad de PCR determina que los analistas declaran y reconocen que cualquier documento, producto, base de datos o programa que se desarrolle es de exclusiva propiedad de PCR y están prohibidos de divulgar o comercializar cualquier producto, documentación o programa referido, salvo que medie autorización escrita por parte de PCR.	Se evaluará realizar una implementación del Azure AD para generar reglas de seguridad a nivel corporativo.	**Concluido.** Se implementó el Azure Active Directory a nivel corporativo para la configuración de políticas de seguridad de la información más rigurosas y que permitan la trazabilidad de eventos de riesgo.
		El Manual Operativo de Clasificación de Riesgo establece que toda información creada por PCR es de uso exclusivo de PCR, por lo tanto, no podrá ser entregada a clientes.		
		El acceso de la información de la entidad estará restringido a los Analistas responsables de la cuenta, Presidencia, el Director de Negocios, Director de Análisis y en el caso de los Gerente/Coordinador País, el Analista Senior del equipo, Analista de Soporte, y el Analista de Análisis y Control de Calidad.		
		Todo acceso que no corresponda a personal asignado a la cuenta debe ser autorizado por el Gerente/Coordinador País.		
R3	**Conflicto de Interés: Clasificaciones manipuladas en favor de un cliente o emisor por parte de un Analista**	Todo directivo, Analista y empleado debe adherirse al Código de Conducta y firmar su aceptación, con el fin de evitar situaciones de conflicto de interés, y de garantizar la transparencia en el tratamiento de la información confidencial.	Se evaluará la emisión de una Política Corporativa de Ética y Conducta reforzando las buenas prácticas establecidas por IOSCO.	**Concluido.** En julio de 2020 se emitió la primera versión de la Política Corporativa de Ética y Conducta de PCR, en reemplazo del antiguo Código de Conducta.
		El personal del Área de Análisis por ningún motivo		

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31-12-2020
		podrá involucrarse directa o indirectamente en la relación comercial y/o administrativa y/o negociaciones de tarifas con el prospecto o con algún cliente de la Clasificadora		
R4	**Informes emitidos con baja calidad de análisis (errores de cálculo, análisis sesgados, redacción pobre, errores de interpretación)**	El Manual Operativo de Clasificación de Riesgo establece como responsabilidad del Director de Análisis, el asegurar una adecuada calidad de los informes de Clasificación de Riesgo emitidos por las oficinas de la organización. El Analista Senior o Principal es responsable de dirigir a los analistas a su cargo para clasificar la fortaleza financiera de las empresas clientes según el Manual Operativo de Clasificación de Riesgo: cumpliendo con las disposiciones emitidas por los entes reguladores El Analista Senior o Principal es responsable de supervisar y apoyar a los analistas a su cargo en la realización de tareas. Los casos nuevos se asignarán preferentemente a analistas con 6 meses de antigüedad como mínimo en PCR ó con probada experiencia en Análisis de riesgo, aunque su contratación en PCR sea reciente En situaciones especiales o cuando exista duda sobre que metodología se debe aplicar, el Área de Metodologías deberá instruir sobre la Metodología a aplicar para el análisis y la Clasificación de riesgo. El Gerente/Coordinador País podrá solicitar en cualquier etapa de la Clasificación el formato para asegurarse que	Se evaluará la incorporación de una actividad de monitoreo para el proceso de Clasificación de Riesgo, en el que el Gerente/Coordinador País deba revisar la última versión del Informe antes de su envío al Cliente (delimitar ítems y periodicidad en el Manual de Clasificación de Riesgo). Se hará precisiones a uno de los controles del procedimiento, para evidenciar que el Gerente/Coordinador/Coordinador País esté revisando el cumplimiento del procedimiento de Clasificación de Riesgo.	**Parcialmente implementado.** Está en proceso de actualización el Manual de Clasificación de Riesgo para la determinación de más controles de calidad previo a la emisión de los Informes de la Clasificadora.

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31-12-2020
		el Analista está cumpliendo con el procedimiento.		
		Se establece que la racionalidad es un argumento, no una lista de puntos, que debe explicar fácilmente el nivel de riesgo del instrumento o institución.		
		La estructura del informe depende de las metodologías normativas de Clasificación de Riesgo de cada país		
		Los miembros del Comité de Clasificación podrían identificar de manera preventiva alertas tempranas con relación a la Calidad del informe Preliminar que pudieran presentarse durante la presentación en el Comité.		
		Se ejecutarán auditorías de Comité a frecuencias planificadas que tienen como objetivo asegurar que los Comités cumplan con la metodología de Clasificación de Riesgo definida.		
		El Analista Senior (o de Soporte) debe verificar que el Informe de Clasificación de Riesgo Preliminar no contenga errores.		
		El Analista Titular debe corregir o realizar ajustes al Informe de Clasificación de Riesgo preliminar si el Cliente presenta observaciones		
R5	**Retrasos en el proceso de Clasificación de Riesgo y en la emisión del Informe respectivo**	El contrato-solicitud de los servicios de Clasificación señala la información cuantitativa y cualitativa que el emisor deberá de reportar a la Clasificadora y la periodicidad con la que deberá de hacerlo	Se evaluará incluir a los Gerente/Coordinador en el requerimiento de información en el Zoho Project para que se lancen alertas automáticas, como recordatorio para la solicitud oportuna de información.	**Parcialmente implementado.** La Dirección de Análisis trabajando en la implementación de un flujo de trabajo en Sharepoint, el cual enviará una tarea al Gerente/Coordinador País en caso el analista titular y el analista senior
		El Comité de Clasificación de PCR podrá retirar o suspender alguna Clasificación si estima que no		

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31-12-2020
		se dispone de información suficiente y/o fidedigna para mantener la misma, a solicitud del Analista Senior, quien expondrá las razones de la solicitud		no reciban la información del cliente.
		En el RI se solicita tanto información cualitativa como cuantitativa. La información financiera histórica, de ser posible, debe ser de los últimos 10 años (mínimo 3 años), las proyecciones, planes de inversión y otros informes relevantes para la Clasificación.		
		El plazo de la recepción de la información será de acorde a la regulación de c/ país y/o acuerdos comerciales para la recepción de la información, lo cual podrá ser ajustado de acuerdo con las necesidades de la entidad y de los plazos regulatorios en cada país		
		En caso excepcional, los Analistas titular y de soporte podrán visitar la oficina de la entidad para confirmar las fuentes de la información enviada por éste.		
		El analista responsable realizará seguimiento a que la información entregada por el cliente se encuentre completa.		
		El analista Senior realizará seguimiento a que la información recibida por parte del cliente cubra la información crítica y esta sea suficiente para comenzar con el análisis del caso.		
		En caso de no envío del segundo requerimiento el Gerente/Coordinador País gestionará con copia al cliente el envío de la información. Si después de		

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31-12-2020
		todas las gestiones realizadas no se ha recibido la información, el Gerente/Coordinador País deberá informar a la Presidencia y al Director de Análisis sobre el atraso en la entrega de la información y enviar un oficio al ente de control en el cual se comunique que no se llevará a cabo el proceso de Clasificación y no se convocará a Comité de Clasificación.		
		Controles de Debida Diligencia: Se debe verificar que toda la información provista por el cliente esté completa y cuente con las firmas de representantes legales, delegados, EEFF, Informes de Auditoría Externa, etc.		
R6	**Pérdida de información crítica relacionada con el proceso de Clasificación**	El Gerente/Coordinador País debe registrar en CRM la información relacionada a la Gestión de prospección con el cliente.	Fortalecer la gestión de copias de respaldo en OneDrive y/o NextCloud para prevenir este riesgo.	**Concluido.** Se migró toda la información de los procesos críticos al OneDrive de los colaboradores.
		Creación de carpetas en Zoho para carga de información a la nube		
		El Informe Final de Clasificación de Riesgo se almacena en formato PDF en el directorio del cliente creado en la Nube de PCR para el personal autorizado.		

III.b.2 Riesgo de Seguridad de la Información

PCR cuenta con una Política de Seguridad de la Información, cuyas herramientas de gestión resultaron en la identificación de los siguientes riesgos:

Riesgos de SI	Estrategia de respuesta al Riesgo	Herramientas de gestión/prevención
RSI-1: Información modificada, adulterada o eliminada (con o sin dolo). **RSI-2:** Errores en la entrada de datos	Evitación del riesgo **Se tiene establecido controles para la gestión de incidentes de seguridad de la información.**	Gestión de incidentes de seguridad de la información

Riesgos de SI	Estrategia de respuesta al Riesgo	Herramientas de gestión/prevención
RSI-3: Ataques internos / ciberataques externos.	Evitación del riesgo **Se capacitó al personal sobre tipos de ataque que podrían afectar la información que PCR genera y administra.**	Cursos de entrenamiento vía Learnsity. Gestión de vulnerabilidades técnicas (pruebas de intrusión internas y externas)
RSI-4: Fuga de información confidencial, utilización de información de la empresa para beneficio propio o de terceros.	Evitación del riesgo **Adicional al Acuerdo de Confidencialidad que firman los colaboradores, el MOF de cada uno señala la responsabilidad de** "*Velar por la organización y actualización de los archivos de información y documentación de su ámbito de responsabilidad, así como aplicar los controles pertinentes a fin de garantizar la confidencialidad, disponibilidad e integridad de la información que tiene a su cargo*"**.**	Manual de Organización y Funciones Configuración del Active Directory y de Políticas de Seguridad a nivel corporativo. Monitoreo de la Actividad de los Usuarios.
RSI-5: Pérdida de información sensible	Evitación del riesgo **La información que genera y administra PCR se almacena en los recursos habilitados en la nube (Office 365 y Zoho).**	Uso de recursos en la nube. Instructivo para Sincronizar archivos del disco duro al OneDrive. Plan de Continuidad del Negocio (incluye Plan de Contingencias Tecnológicas)

III.b.3 Riesgo de Contraparte

Durante el año 2020, se llevó a cabo una adecuada gestión de las cobranzas de PCR, por cuanto el riesgo de contraparte no fue significativo para la compañía durante esa gestión.

III.b.4 Riesgo de Liquidez

La entidad presentó niveles de liquidez superiores al 100% durante la gestión pasada, evidenciando el cumplimiento efectivo del pago de sus obligaciones, dentro de plazo.

III.b.5 Riesgo de Cumplimiento

PCR gestionó debidamente su riesgo de cumplimiento durante la gestión 2020, acatando sus obligaciones con el ente regulador según cronogramas definidos.

III.b.6 Riesgo de Gobierno Corporativo

La estructura organizativa de PCR permite una adecuada gestión del riesgo de gobierno corporativo (cumplimiento de metas, transparencia de la información,

aplicación de códigos de conducta, etc.), lo que se refleja en los niveles de rentabilidad alcanzados por la empresa durante el 2020, y en los Informes emitidos por sus órganos de control (Gestión Integral de Riesgos y Auditoría Interna).

III.c Políticas actualizadas para la gestión integral de riesgos

Las políticas establecidas por PCR son afines a la complejidad y al volumen de las operaciones que caracterizan a su modelo de negocios y a su perfil de riesgos. Dichas políticas establecen los niveles de exposición considerados como aceptables para cada tipo de riesgo, cuyos niveles se reflejan en los límites de apetito, tolerancia y capacidad de riesgo definidos a nivel integral.

- **Políticas de identificación del Riesgo**

Tanto la Unidad de Gestión Integral de Riesgos, como los niveles jerárquicos representativos de cada área, son responsables de la identificación de los riesgos a los que está expuesto PCR.

- **Políticas de medición del Riesgo**

Según los tipos de riesgo identificados, se desarrollaron metodologías específicas para la cuantificación de niveles de exposición al riesgo. La medición se basa en la determinación de la frecuencia e impacto de las pérdidas o daño a PCR que podría materializarse, por cada tipo de riesgo.

- **Políticas de Monitoreo y Control**

Cada instancia de PCR inmersa en la gestión de riesgos (Gerente/Coordinador / Coordinador País, Analistas, personal administrativo, etc.), debe reportar la ocurrencia de eventos de riesgo que ayuden a detectar y corregir rápidamente deficiencias en las políticas, procesos y procedimientos. Se instrumenta este reporte con el envío electrónico periódico para este fin.

La Unidad de Gestión Integral de Riesgos debe recomendar las acciones que permitirán disminuir la frecuencia o el impacto de los eventos materializados, y registrados en la Base de Eventos de Riesgo Operacional. Como medida preventiva, además, se destaca el proceso de seguimiento que realiza la Unidad de Riesgos al Calendario de Obligaciones de PCR, lo cual permite anticiparse a potenciales incumplimientos de normas regulatorias.

- **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 Continuidad que le permita administrar esta situación. Dicho Plan, consigna las estrategias para manejar situaciones de crisis, así como escenarios de riesgo extremo.

- **Políticas de divulgación / comunicación**

La Junta Directiva, Comité de Gestión Integral de Riesgos y el Coordinador País, son informados periódicamente sobre los eventos de riesgo que se presentan en la entidad. De manera continua, el Coordinador País de PCR comunica al Oficial de GIR si se generaron eventos de riesgo que pudieran afectar negativamente a la Clasificadora, en cuyo caso también se analiza en conjunto las causas raíz del evento y las alternativas para prevenir que éste vuelva a suscitarse.

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

PCR cuenta con un documento normativo titulado ***Metodologías para la Gestión Integral de Riesgos en PCR***, en el cual se define las herramientas a utilizar para la identificación y medición de los riesgos, según el tipo de riesgo:

Tipo de Riesgo	Herramientas / Metodologías
Riesgo Operativo u Operacional (incluye el riesgo legal y el riesgo tecnológico)	Las principales herramientas que se debe utilizar para gestionar y evaluar el riesgo operativo son: la Evaluación de Procesos (Matriz de Riesgos) y la Base de Eventos de Riesgo Operativo. La evaluación de procesos se constituye en una de las herramientas más utilizadas para la identificación, medición y evaluación del riesgo operativo, basada en un análisis riguroso de los procesos de la entidad a fin de identificar sus riesgos potenciales, las causas o factores que los originan, sus consecuencias, y los controles que permiten prevenirlos y/o corregirlos. Al tratarse de una herramienta completa y compleja, requiere de un análisis conjunto entre el Jefe de la Unidad de Riesgos y de los colaboradores a cargo de ejecutar los procesos a partir de entrevistas de relevamiento que permitan el llenado una Matriz de Riesgos. Cada vez que se materializa un evento de riesgo, el Portavoz de Riesgo y/o el Gerente/Coordinador/Coordinador País, deberá reportarlo al Jefe de la Unidad de Riesgos vía correo electrónico, con los siguientes datos mínimamente: -Fecha de inicio del evento -Fecha de finalización del evento (si corresponde) -Descripción del Evento -Acciones correctivas adoptadas

Tipo de Riesgo	Herramientas / Metodologías
	-Personal involucrado (nombre y puesto)
Riesgo de Seguridad de la Información	El análisis y evaluación de riesgos de seguridad de la información se basa en los resultados obtenidos de la aplicación de un conjunto de herramientas: • Gestión de Vulnerabilidades Técnicas • Gestión de Incidentes de Seguridad de la Información • Monitoreo de la Actividad de Usuarios • Revisión de roles y privilegios
Riesgo de Contraparte	La principal herramienta para la gestión del riesgo de contraparte es el seguimiento al índice de mora. En términos monetarios, se define a la mora como el incumplimiento al que incurren los clientes de PCR en el pago de sus obligaciones por el servicio prestado de Clasificación /Clasificación de Riesgos. En tal sentido, todo impago superior a los 30 días a partir de la fecha de pago pactada mediante contrato es considerado cartera en mora.
Riesgo de Liquidez	El riesgo de liquidez se gestiona mediante el seguimiento a los límites del ratio de liquidez estructural de cada Oficina: $$Ratio\ de\ Liquidez = \frac{Activos\ Líquidos}{Total\ Obligaciones\ (Pasivos)}$$ Donde: *Activos líquidos:* Comprenden todo el efectivo disponible en cuentas de ahorro, cuentas corrientes y CDFs con vencimiento menor o igual a 30 días. *Total Obligaciones:* Comprende al total de pasivos de cada Oficina País, tanto aquellos de corto plazo, como aquellos de largo plazo.
Riesgo de Cumplimiento	La gestión del riesgo de cumplimiento se realiza mediante el seguimiento mensual de las obligaciones regulatorias de cada Oficina País, según calendarios definidos para el año en curso.
Riesgo de Gobierno Corporativo	Cada año, las Oficinas del Grupo realizan el planteamiento de nuevas metas para el incremento de su rentabilidad, ya sea mediante estrategias de incremento de las ventas, como mediante la mejora en los niveles de eficiencia administrativa (disminución de gastos). Al tratarse de un esfuerzo conjunto que parte de la Dirección, la Alta Gerencia y los cargos ejecutivos para su cumplimiento, la gestión del riesgo de gobierno corporativo se enfoca en el cumplimiento de las metas planteadas para alcanzar los niveles de rentabilidad deseados, por cada Oficina País.

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

El 14 de enero de 2021, el área de Auditoría Interna emitió el Informe INF. AI. SV. N° 004/2020, en el que se incluyó la revisión al proceso de gestión de riesgos de PCR.

Resultado de la evaluación del Auditor Interno, se emitieron las siguientes observaciones, cuyas acciones correctivas presentan como plazo máximo el 30 de junio de 2021:

Aspecto Evaluado	Observaciones	Planes de Acción
Manual y Procedimientos de Gestión de Riesgos	*Se constató que el Manual de Gestión Integral de Riesgos de PCR se encuentra en proceso de actualización, toda vez que existen actividades que se vienen realizando dentro del proceso de gestión que deben ser formalizadas, como la definición de estrategias frente a los niveles de exposición de riesgos, su medición, tolerancia y capacidad de riesgo de PCR, entre otros.* *Consiguientemente, se identificó que los "Procedimientos de Gestión Integral de Riesgos", también se encuentran en proceso de actualización, ya que las directrices definidas deben ser consistentes con lo establecido en el Manual de Gestión de Riesgos, y deben dejar establecido formalmente los reportes o resultados de la aplicación de la normativa interna de riesgos de PCR.*	Se concluirá la actualización del ***Manual para la Gestión Integral de Riesgos en PCR*** y la formalización de los ***Procedimientos para la Gestión Integral de Riesgos en PCR***, con alcance a nivel corporativo para su estricto cumplimiento.

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

- Se capacitará al personal nuevo de la entidad con relación a los conceptos básicos de gestión integral de riesgos que deben conocer para dar cumplimiento a su rol como colaboradores.
- Se fortalecerá la cultura de riesgos de la entidad a través de una capacitación que ponga en práctica los principios establecidos en el Manual de Gestión Integral de Riesgos de PCR.
- Actualizar los documentos normativos internos referentes a la gestión integral de riesgos, en concordancia con el nivel de madurez del proceso.

III.g Ejecución del Plan de Capacitación relacionado a la gestión integral de riesgos establecidos en el Artículo 15 de la NRP-11.

Tema de la Capacitación	Responsable	Periodo
Gestión Integral de Riesgos	Oficial de Gestión Integral de Riesgo	Febrero 2020
Seguridad de la Información	Oficial de Gestión Integral de Riesgo	Mayo-Junio 2020

Tema de la Capacitación	Responsable	Periodo
Plan de Continuidad del Negocio	Oficial de Gestión Integral de Riesgo	Agosto-Septiembre 2020

III.h Conclusiones generales sobre la gestión de riesgos

Durante la gestión 2020 se realizó una efectiva gestión integral de riesgos a nivel corporativo, lo que permitió la identificación, medición, monitoreo, control, mitigación y divulgación de los principales riesgos a los que PCR se encuentra expuesta.

Así también, con el apoyo de la Coordinador País, se logró fortalecer la cultura de gestión de riesgos al interior de la entidad, sin reportar ningún evento que pudiera afectar los resultados financieros esperados por la empresa.

IV. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

IV.a Estrategias y principales políticas utilizadas para la gestión de la seguridad de información y de la ciberseguridad

La **estrategia de seguridad de la información** de PCR se compone de los siguientes elementos:

- **Usuarios.** Todo el personal firma un Contrato de Trabajo y un Acuerdo de Confidencialidad que señala su obligación de proteger y no divulgar la información que genera y administra la empresa PCR. Del mismo modo el Manual de Organización y Funciones de la empresa señala la responsabilidad de los colaboradores de velar por la disponibilidad, integridad y confidencialidad de la información que tienen a su cargo.
- **Analista de TI**. Es la instancia responsable de dar de alta a los usuarios y personal nuevo de la entidad, así como dar de baja oportunamente al personal desvinculado, en el marco de los niveles de acceso autorizados para cada perfil de usuario.
- **Oficial de Gestión Integral de Riesgos**. Es la instancia que analiza y evalúa los riesgos de seguridad de la información a los que se halla expuesto PCR, proponiendo mejoras en los casos que corresponda.
- **Comité de Tecnología:** La entidad ha conformado un Comité Corporativo de Tecnología en el cual se coordina la implementación de iniciativas para el uso eficiente de los recursos tecnológicos de PCR, dentro del marco de la gestión de seguridad de la información.

Así también, desde el 2020 PCR cuenta con una Política de Seguridad de la Información a nivel corporativo, en la cual se definen los pilares de gestión que se debe cumplir para preservar la confidencialidad, integridad y disponibilidad de la información que la entidad genera y administra, cuyos elementos son los siguientes:

- Administración del Control de Accesos
- Gestión Incidentes de Seguridad de la Información
- Administración de Servicios y Contratos con Terceros
- Gestión de los sistemas de la información
- Gestión de la continuidad del negocio

IV.b Principales requisitos logrados del SGSI

Durante el 2020 se logró cumplir los siguientes requisitos de la Norma Técnica NRP-23 para la Gestión de la Seguridad de la Información:

Capítulo	Artículo	Literal	Romano	Descripción del Cumplimiento
II	**9**	a	-	El Comité de Gestión Integral de Riesgos aprobó la Política de seguridad de la Información y las Metodologías para la Gestión Integral de Riesgos (que incluyen las herramientas del SGSI), considerando lo establecido en el Art. 9, literal a.
III	**11**	d	-	Los usuarios de PCR cuentan con factores de autenticación de uso personal, de tal manera que las responsabilidades asignadas puedan ser seguidas e identificadas. En este sentido, todos los activos de información de PCR se protegen a través de los citados factores.
III	**11**	h	-	Se cuenta con controles sobre accesos remotos y dispositivos móviles que interactúan con la infraestructura de tecnología de PCR.
III	**11**	i	-	Se cuenta con controles para la configuración segura de hardware, software, equipos de comunicación, dispositivos móviles en PCR, limitados según protocolos, puertos y usuarios.
III	**17**	a	-	Los procesos de selección del personal incluyen la verificación de los antecedentes de cada empleado, de conformidad con la legislación laboral vigente.
III	**25**	-	-	PCR no cuenta con un Centro de Datos propio puesto que terciariza este servicio con Microsoft. Asimismo, al haber contratado la licencia de Office 365 Premium para trabajar procesando información en línea y en la nube, se cuenta con los debidos Acuerdos de Nivel de Servicio (SLAs) del proveedor que corresponden a una empresa de clase mundial como Microsoft.
III	**26**	-	-	PCR cuenta con una herramienta de evaluación de proveedores de servicios relacionados con TI.
V	**35**	-	-	PCR remitió el Plan de Adecuación a la Norma NRP-23 al ente regulador vía los sistemas habilitados para el efecto.

Por otra parte, de acuerdo con lo declarado a la SSF en enero de 2021, existen cuarenta y siete (47) requisitos que fueron parcialmente cumplidos hasta el cierre de 2020 (el detalle de los citados requisitos se encuentra en el Anexo 1).

IV.c Programa de Seguridad de la Información

El Programa de Seguridad de la Información de PCR para el 2021 se basa primordialmente en la implementación de los planes de acción aprobados por la Junta Directiva y remitidos a la SSF en diciembre de 2020, cuyos plazos están descritos en dicho reporte.

Es cuanto tengo a bien informar, para los fines consiguientes.

Daniela Urquizo Rojas
OFICIAL DE GESTION INTEGRAL DE RESGOS

ANEXO 1
Requisitos de la Norma NRP-23 que presentan "Cumplimiento Parcial"
por parte de PCR al 31/12/2020

N°	Capítulo	Artículo	Literal	Romano	Descripción del Requisito	Nivel de Cumplimiento de PCR
1	**II**	**4**	-	-	Las entidades deberán contar con una estructura organizacional acorde a sus productos, servicios, operaciones, tamaño, perfil de riesgos y modelo de negocio, de tal forma que delimite claramente las funciones, roles, responsabilidades y facultades asociadas a la seguridad de la información y la ciberseguridad, así como los niveles de dependencia e interrelación que corresponde con cada una de las demás áreas de la entidad.	Cumple parcialmente
2	**II**	**4**	-	-	Asimismo, las entidades deberán asegurarse de que todo su personal reconozca a la seguridad de la información y ciberseguridad como una de sus responsabilidades, aplicando las medidas de confidencialidad que fueran necesarias. La información cuya seguridad deberá preservarse, será la que de acuerdo a la clasificación de los activos de información que realice la entidad, requiera un tratamiento de aseguramiento o protección.	Cumple parcialmente
3	**II**	**5**	a	-	**La Junta Directiva u órgano equivalente será la responsable de establecer un adecuado gobierno y gestión de la seguridad de la información por lo que deberá realizar como mínimo lo siguiente:** Aprobar los recursos necesarios para el establecimiento, implementación, monitoreo y mantenimiento de la gestión de la seguridad de la información, a fin de contar con la infraestructura, metodología, tácticas y personal apropiados. Asimismo, deberá nombrar a una persona responsable de gestionar la seguridad de la información, el cual tendrá una comunicación permanente y directa con la Alta Gerencia, quien a su vez informará directamente a la Junta Directiva. La Junta Directiva hará constar en Punto de Acta su nombramiento, el cual deberá ser remitido a la Superintendencia a más tardar diez días hábiles después de dicho nombramiento	Cumple parcialmente
4	**II**	**5**	b	-	**La Junta Directiva u órgano equivalente será la responsable de establecer un adecuado gobierno y gestión de la seguridad de la información por lo que deberá realizar como mínimo lo siguiente:** Aprobar el programa de seguridad de la información y la estructura del SGSI	Cumple parcialmente
5	**II**	**5**	c	-	**La Junta Directiva u órgano equivalente será la responsable de establecer un adecuado gobierno y gestión de la seguridad de la información por lo que deberá realizar como mínimo lo siguiente:** Requerir a Auditoría Interna que verifique la existencia y el cumplimiento de la estructura del SGSI	Cumple parcialmente

N°	Capítulo	Artículo	Literal	Romano	Descripción del Requisito	Nivel de Cumplimiento de PCR
6	**II**	**7**	a	-	**Las entidades deberán contar con un Comité de Riesgos el cual observará lo establecido en las presentes Normas y en las Normas Técnicas de Gobierno Corporativo" (NRP-17) aprobadas por el Banco Central, por medio de su Comité de Normas.** **En materia de gestión de riesgos de la seguridad de la información, el Comité de Riesgos, o quien haga sus veces, será el responsable de llevar a cabo como mínimo, lo siguiente:** Proponer a la Junta Directiva la estructura del SGSI	Cumple parcialmente
7	**II**	**7**	b	-	Revisar, evaluar y proponer para aprobación de la Junta Directiva el programa y recursos de seguridad de la información, dichos recursos deberán estar separados de los presupuestos destinados a cualquier otra área de la entidad	Cumple parcialmente
8	**II**	**7**	c	-	Efectuar el seguimiento de la gestión de la seguridad de la información	Cumple parcialmente
9	**II**	**8**	a	-	**En cuanto a la gestión de la seguridad de la información, la Unidad de Riesgos, o quien haga sus veces, deberá realizar lo siguiente:** Proponer al Comité de Riesgos o quien haga sus veces, la creación de Comités, áreas o cargos especializados para el cumplimiento de las responsabilidades relacionadas con la gestión de la seguridad de la información	Cumple parcialmente
10	**II**	**8**	b	-	Velar que la gestión de la seguridad de la información sea consistente con las políticas y metodologías aplicadas para la gestión de riesgos	Cumple parcialmente
11	**III**	**10**	a	i	**Las entidades deben establecer, mantener y documentar un SGSI que guarde consistencia con el Sistema de Gestión de la Continuidad del Negocio y con la gestión de los riesgos operacionales. Las actividades mínimas que las entidades deberán realizar para desarrollar un SGSI serán las siguientes:** Establecimiento de un SGSI: Especificar el alcance del SGSI de acuerdo a las características del negocio de la entidad, sus activos, tecnología, entre otros.	Cumple parcialmente
12	**III**	**10**	a	ii	Instaurar una política de seguridad de la información y ciberseguridad en relación a la naturaleza, tamaño o volumen de operaciones del negocio de la entidad	Cumple parcialmente
13	**III**	**10**	a	iii	Identificar, analizar, evaluar y mitigar los riesgos asociados a los activos, procesos, personas, proyectos y servicios de tecnología de la información, a través de la metodología aprobada por la Junta Directiva, considerando las amenazas y las vulnerabilidades a los que están expuestos, identificando los impactos	Cumple parcialmente

N°	Capítulo	Artículo	Literal	Romano	Descripción del Requisito	Nivel de Cumplimiento de PCR
14	**III**	**10**	a	iv	Definir controles de seguridad de la información, debidamente documentados	Cumple parcialmente
15	**III**	**10**	b	ii	Especificar cómo medirá la efectividad de dichos controles	Cumple parcialmente
16	**III**	**10**	b	iii	Establecer programas de capacitación y concientización para todo el personal de la entidad, al menos, una vez al año	Cumple parcialmente
17	**III**	**10**	b	iv	Administrar los recursos que componen el SGSI	Cumple parcialmente
18	**III**	**10**	b	v	Aplicar las instrucciones y controles que sean efectivos para la inmediata detección y respuesta a incidentes de seguridad de la información	Cumple parcialmente
19	**III**	**11**	b	-	Establecer una adecuada segregación de funciones, de tal manera que una misma persona no tenga varios roles o privilegios que puedan poner en peligro la seguridad de la información	Cumple parcialmente
20	**III**	**11**	c	-	Revisiones periódicas sobre los derechos concedidos a los usuarios y el uso real de los derechos	Cumple parcialmente
21	**III**	**12**	d	-	Monitorear y verificar el cumplimiento de las políticas y procedimientos que se establezcan en materia de ciberseguridad, sin perjuicio a aquellas tareas que realiza la auditoría interna.	Cumple parcialmente
22	**III**	**14**	-	-	Las entidades deberán incluir en los contratos de tercerizaciones de servicios críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de ciberseguridad y seguridad de la información. Asimismo, verificar periódicamente el cumplimiento de las obligaciones y medidas establecidas en dichos contratos, para lo cual debe implementar los mecanismos adecuados para tales efectos. Para el caso de las entidades que se rigen conforme a lo dispuesto en la Ley de Adquisiciones y Contrataciones de la Administración Pública, realizarán esta actividad sin contravención a dicha Ley. En ningún caso la seguridad del tercero debe ser inferior que la del cliente. Por tanto, los contratos deberán especificar los requerimientos mínimos de seguridad de la información aceptados por las entidades.	Cumple parcialmente
23	**III**	**16**	a	ii	Adoptar políticas, procedimientos, mecanismos y herramientas manuales o automatizadas para la protección de la información	Cumple parcialmente
24	**III**	**16**	a	vii	Identificación de los activos de información críticos que estén expuestos al ciberespacio	Cumple parcialmente

N°	Capítulo	Artículo	Literal	Romano	Descripción del Requisito	Nivel de Cumplimiento de PCR
25	**III**	**16**	b	i	**Protección y detección: En esta etapa, las entidades deben desarrollar e implementar actividades apropiadas para identificar, analizar y controlar eventos de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos, para lo cual, las entidades deberán aplicar como mínimo, lo siguiente:** Adoptar procedimientos y mecanismos para identificar, analizar y mitigar las amenazas y los incidentes de ciberseguridad que se presenten	Cumple parcialmente
26	**III**	**16**	b	ii	Gestionar las vulnerabilidades informáticas de las plataformas tecnológicas que soporten activos de información y que estén expuestos a ciberataques o riesgos tecnológicos internos, fortaleciendo los eslabones de seguridad en los servicios informáticos relacionados a productos o servicios financieros brindados por la entidad	Cumple parcialmente
27	**III**	**16**	b	iii	Realizar un monitoreo continuo de la infraestructura tecnológica de la entidad, haciendo uso de herramientas automatizadas y una estructura organizativa, con el propósito de identificar y mitigar comportamientos inusuales que puedan evidenciar ciberataques o incidentes de ciberseguridad contra la entidad	Cumple parcialmente
28	**III**	**16**	c	i	**Respuesta: Aún con las medidas de seguridad adoptadas, las entidades deben desarrollar e implementar actividades para mitigar los incidentes relacionados con ciberseguridad. Para hacerle frente a esta situación, las entidades deberán realizar, al menos, las actividades siguientes:** Establecer procedimientos de respuesta a incidentes de ciberseguridad tales como: desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP o cualquier otro que determine la entidad	Cumple parcialmente
29	**III**	**16**	d	ii	Considerar dentro del plan de continuidad del negocio la recuperación y reanudación de la operación	Cumple parcialmente
30	**III**	**16**	d	iii	Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos	Cumple parcialmente
31	**III**	**17**	b	-	Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad	Cumple parcialmente
32	**III**	**17**	c	-	Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución formal de activos	Cumple parcialmente

N°	Capítulo	Artículo	Literal	Romano	Descripción del Requisito	Nivel de Cumplimiento de PCR
33	**III**	**19**	a	-	**Inventario de activos de información y clasificación de la información** **Para el inventario de activos de información y clasificación de la información, la entidad debe realizar al menos lo siguiente:** Realizar y mantener un inventario de activos de información y asignar responsabilidades respecto a la protección de dichos activos	Cumple parcialmente
34	**III**	**20**	a	-	**Administración de las operaciones y comunicaciones** **Las entidades deben implementar una administración de las operaciones y comunicaciones de servicios o productos financieros que se ofrecen a los clientes o usuarios, de tal forma que les permita contar con políticas y planes de renovación de infraestructura tecnológica, y así poder mitigar los riesgos de seguridad asociados a la obsolescencia de dicha infraestructura, para la cual establecerá como mínimo, lo siguiente:** Procedimientos aprobados y documentados para la operación de los sistemas informáticos	Cumple parcialmente
35	**III**	**20**	f	-	Controles preventivos y de detección sobre el uso de programas informáticos de procedencia dudosa, virus, malware, denegación de servicios, phishing y otros similares	Cumple parcialmente
36	**III**	**20**	g	-	Seguridad sobre protocolos, puertos de redes y redes inalámbricas, navegadores, medios de almacenamiento, perímetro y documentación de sistemas, intercambio de la información a nivel interno y externo, incluido el correo electrónico brindado por la entidad como el de uso personal, tanto a nivel local como remoto, y sobre los canales electrónicos	Cumple parcialmente
37	**III**	**20**	h	-	Resguardo de registros de auditoría y monitoreo del uso de los sistemas	Cumple parcialmente
38	**III**	**20**	i	-	Pruebas o evaluaciones de vulnerabilidad e intrusión sobre los componentes de infraestructura de tecnología y mitigar las brechas de seguridad identificadas. Estas deberán realizarse al menos una vez al año y cuando existan cambios en la infraestructura referida. Dichas actividades podrán ser realizadas por proveedores de este tipo de servicios y serán documentadas de acuerdo a lo dispuesto en el artículo 29 de las presentes Normas.	Cumple parcialmente
39	**III**	**21**	b	-	Aplicar las técnicas de cifrado que garanticen efectivamente la protección del almacenamiento y transporte de la información crítica de acuerdo a la clasificación de la entidad	Cumple parcialmente
40	**III**	**21**	c	-	Definir controles sobre la implementación de aplicaciones antes del ingreso a producción	Cumple parcialmente

N°	Capítulo	Artículo	Literal	Romano	Descripción del Requisito	Nivel de Cumplimiento de PCR
41	**III**	**21**	d	-	Controlar el acceso al código fuente de los sistemas informáticos que son propiedad de la entidad	Cumple parcialmente
42	**III**	**21**	e	-	Mantener un estricto y formal control de cambios y versiones, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios	Cumple parcialmente
43	**III**	**21**	f	-	Contar con mecanismos de desarrollo seguro que permita analizar y corregir las vulnerabilidades de seguridad existentes en las aplicaciones informáticas de la entidad. Deberá efectuarse este tipo de análisis en el ciclo de vida del desarrollo de dichas aplicaciones y establecer los procedimientos de corrección adecuados; asimismo, cuando dichos sistemas se encuentren en producción	Cumple parcialmente
44	**III**	**21**	g	-	Establecer un procedimiento de instalación de actualización de software, de forma segura y controlada, con el objeto de prevenir vulnerabilidades y sin afectar el desempeño de la infraestructura.	Cumple parcialmente
45	**III**	**23**	-	-	**Procesamiento, procedimientos de respaldo y restauración de la información** Las entidades deben contar con procedimientos de respaldo regular y periódicamente validados. Estos procedimientos deberán incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada, en forma oportuna y eficiente, en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad del negocio de la entidad. Las entidades conservarán la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro de datos principal de procesamiento de la información, de tal forma que se mitiguen amenazas de índole geográfica, física y ambiental. La distancia se determinará de acuerdo a la evaluación de riesgos que realice la entidad. Las entidades deben almacenar sus respaldos de información, debiendo notificar a la Superintendencia el lugar específico donde se almacena o procesa la información de sus clientes. Dicha notificación deberá realizarla 10 días hábiles posteriores al haberse iniciado operaciones o cuando ocurra un cambio de ubicación de los mismos.	Cumple parcialmente

N°	Capítulo	Artículo	Literal	Romano	Descripción del Requisito	Nivel de Cumplimiento de PCR
46	**IV**	**28**	-	-	**Privacidad de la información** Las entidades deben adoptar medidas que aseguren la protección y confidencialidad de la información bajo su responsabilidad, como datos personales, e información que reciben de sus clientes, usuarios de servicios, proveedores, entre otros; sin perjuicio de lo establecido en el marco legal vigente.	Cumple parcialmente
47	**V**	**34**	-	-	**Contrataciones posteriores a la entrada en vigencia** Las entidades que después de la fecha de entrada en vigencia de las presentes Normas deseen adquirir sistemas informáticos o encomendar en un tercero el desarrollo de los mismos y que estén relacionados con productos o servicios financieros de dicha entidad, deberán cumplir con lo dispuesto en el artículo 22, literal c) de las presentes Normas.	Cumple parcialmente