INF. GIR. SV. N° 02/2022

Informe de Evaluación Técnica de la Gestión Integral de Riesgos de PCR Gestión 2021

San Salvador, 13 de abril de 2022

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: 13 de abril de 2022

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 2021.

- 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 2021.

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 • Daniela Urquizo • Karina Montoya	• Presidente Ejecutivo • Oficial de Gestión Integral de Riesgos • Coordinador País
Unidad de Gestión Integral de Riesgos	• Daniela Urquizo	• Oficial de Gestión Integral de Riesgos

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 31.12.2021
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. Al 31.12.2021 se continúan aplicando las

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31.12.2021
				políticas de seguridad definidas el 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. Al 31.12.2021 se continúa generando reportería para verificar la aplicabilidad y efectividad de las políticas configuradas.
		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.

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31.12.2021
		El personal del Área de Análisis por ningún motivo 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		Al 31.12.2021 no se reportaron eventos de incumplimiento a la Política Corporativa de Ética y Conducta.
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.	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.	**Concluido.** Se finalizó la etapa de pruebas a un flujo configurado en SharePoint para la mejora de los controles. En junio/2021 se comenzaron a generar las órdenes de servicio de todos los contratos vigentes y a partir de julio los informes se realizarán a través del flujo de Negocios.
		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		

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31.12.2021
		etapa de la Clasificación el formato para asegurarse que 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.	**Concluido.** Se incluyó en el Manual de Clasificación el plazo de dos semanas antes del vencimiento para informar al regulador, en caso de no contar con la información requerida al cliente.
		El Comité de Clasificación de PCR podrá retirar o suspender		

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31.12.2021
		alguna Clasificación si estima que no se dispone de información suficiente y/o fidedigna para mantener la misma, a solicitud del Analista Senior, quien expondrá las razones de la solicitud		
		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		

N°	Descripción	Controles asociados	Planes de Acción	Seguimiento al 31.12.2021
		después de 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 2021, 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

Se evidenció un (1) evento registrado bajo la codificación ROPE-002, cuya descripción se detalla a continuación:

Código Evento	**ROPE-002**
Fecha Inicio	22-10-2021
Referencia	Informe de Clasificación

Sub-tipo de evento	Seguimiento y presentación de informes
Descripción del evento	El cliente FONDO DE TITULARIZACIÓN HENCORP VALORES - ALCALDIA MUNICIPAL DE SONSONATE 01 envió de manera extemporánea la información solicitada por PCR para la elaboración del Informe de Clasificación correspondiente.
Acciones correctivas adoptadas	*El 22 de julio de 2021 PCR envió el primer requerimiento de información al cliente. *El 22 de octubre de 2021, luego de reiteradas solicitudes, PCR envió un recordatorio del requerimiento al cliente mediante Oficio. *El 10 de diciembre de 2021 PCR recibió el Oficio IV-DSMI-25741 de la SSF en el cual se solicita justificación de la NO presentación del Informe. *El 13 de diciembre PCR solicitó nuevamente la información al cliente. *El mismo 13 de diciembre PCR recibió la información del cliente y procedió con iniciar la elaboración del informe. *El 16 de diciembre PCR respondió a la solicitud de la SSF mediante Oficio SV_FTSO01_SSF_FIN, remitiendo la documentación de soporte necesaria para respaldar las justificaciones de la no elaboración del Informe referido.
Estado	En seguimiento
Descripción Seguimiento	*A la fecha de elaboración del presente Informe, PCR continúa atento a cualquier comunicación por parte del regulador sobre este caso.

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 2021, 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 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.

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 -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.

Tipo de Riesgo	Herramientas / Metodologías
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.
Riesgo de Seguridad de la Información	**Medición de la efectividad de los controles de seguridad de la información** El Oficial de GIR evalúa la efectividad de los controles implementados para la gestión de la seguridad de la información al menos una vez al año a través de un Informe que contiene un resumen de los resultados de cada control durante la gestión en curso. Para este fin, se debe considerar como mínimo: - Tipo de control o Herramienta de Gestión evaluada. - Reporte / Informe revisado - Autor(es) - Fechas de generación / elaboración de los reportes o informes - Resultados obtenidos (descripción) - Tipo de Alerta: o Roja: cuando el control presenta o nula efectividad para la que fue creado o Amarilla: cuando el control demuestre haber detectado fallas o problemas en la gestión de la información, Verde: Cuando el control demuestre que no se presentaron fallas ni problemas derivados de la gestión de la información en PCR.

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

El 26 de julio de 2021, el área de Auditoría Interna emitió el Informe INF. AI. SV. N° 002/2021, 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 se concluyeron el 31 de julio del mismo año:

Aspecto Evaluado	Observaciones de Auditoría Interna	Planes de Acción
Formalización de controles de seguridad de la información	*Formalización en la definición de perfiles de acceso para PCR*	Se incluyó en el *Protocolo de Seguridad de la Información*
	Procedimientos para la administración de privilegios para las cuentas de usuario y administración de información.	Se incluyó en el *Protocolo de Seguridad de la Información*
	Procedimientos para la emisión del reporte y solución de incidentes de seguridad de información	Se incluyó en los *Procedimientos para la Gestión de la Seguridad de la Información*
	Procedimientos para la realización de copias de seguridad	Se incluyó en el *Protocolo de Seguridad de la Información*
	Reglamento del Comité de Tecnología	Pendiente. Se actualizará hasta el 30 de junio de 2022.
	Reglamento del Comité de Seguridad de la Información	No aplica. El Comité de Gestión Integral de Riesgos asume la función de Gestión de la Seguridad de la Información.
	Procedimientos formales para la destrucción controlada de medios de almacenamiento de respaldo	Se incluyó en el *Protocolo de Seguridad de la Información*

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

- Capacitar al personal en el estricto cumplimiento del Protocolo de Seguridad de la Información.

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, y además se imparte a todo el personal

Tema de la Capacitación	Responsable	Periodo
		nuevo desde mayo del mismo año hasta la fecha.
Seguridad de la Información	Oficial de Gestión Integral de Riesgo	Junio 2020, y además se imparte a todo el personal nuevo.
Ciberseguridad	Oficial de Gestión Integral de Riesgo	Julio 2021, y además se imparte a todo el personal nuevo.
Plan de Continuidad del Negocio	Oficial de Gestión Integral de Riesgo	Agosto 2021, y además se imparte a todo el personal nuevo.

III.h Conclusiones generales sobre la gestión de riesgos

Durante la gestión 2021 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 Gerente 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, en julio de 2021, se actualizó la 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
- Manejo de información confidencial

IV.b Principales requisitos logrados del SGSI

Durante el 2021 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	Tarea de Adecuación	Estado al 31-12-2021
II	**4**	-	-	PCR cuenta con suficientes recursos humanos, financieros y tecnológicos para realizar una efectiva gestión de la seguridad de la información. Su estructura organizacional permite delimitar las funciones de los siguientes niveles jerárquicos para liderar y dirigir el Sistema de Gestión de Seguridad de la Información de PCR: 1. Junta Directiva, 2. Gerente o Coordinador País, 3. Jefe de Administración, 4. Analista de IT, 5. Oficial de Gestión Integral de Riesgos 6. Comité de Gestión Integral de Riesgos En virtud de que el Sistema de Gestión de la Seguridad de la Información (SGSI) de PCR aún está en un nivel de madurez básico, PCR considera necesario actualizar el Manual de Organización y Funciones MOF Manual de Organización y Funciones) de los cargos citados para así fortalecer su capacidad de sinergia.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
II	**5**	a	-	PCR tiene asignados los recursos necesarios para establecer, implementar y mejorar su gestión de la seguridad de la información. Dentro de dichos recursos se contempla el presupuesto para la contratación de un Jefe de Administración, un Analista de IT, un Oficial de Gestión Integral de Riesgos y de la licencia de Office 365 Business Premium que a su vez incluye al Azure Active Directory para la configuración de políticas de seguridad a nivel corporativo. En virtud al nivel de madurez del SGSI de PCR, la entidad considera necesario actualizar el MOF (Manual de Organización y Funciones) de la Junta Directiva a fin de fortalecer sus funciones de liderazgo en la gestión de la seguridad de la información	Cumple
II	**5**	b	-	Aún no se ha definido la responsabilidad de la Junta Directiva en lo que respecta la aprobación del programa de seguridad de la información y la estructura del SGSI. Dado el giro del negocio, el tamaño y la complejidad de las operaciones de PCR, la Unidad de Gestión Integral de Riesgos funge también como Función de la Seguridad de la Información, considerando que el Oficial de Gestión Integral de Riesgos cuenta con las competencias de un profesional certificado en la ISO 31000 como Risk Manager (PECB - Professional Evaluation Certification Board), además de conocer y emplear como marco de referencia a la norma ISO 27001 y 27002 para diseñar e impulsar la implementación de un adecuado SGSI. Por este motivo, en la práctica, quedó implícita la estructura del SGSI conformada por el Oficial de Gestión Integral de Riesgos, el Comité de Gestión Integral de Riesgos, el Comité de TI y la Junta Directiva. En línea con lo mencionado: *Se establece como plan de adecuación la actualización del MOF (Manual de Organización y Funciones) de la Junta Directiva para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23. *Se dará cumplimiento a la aprobación del Programa de Seguridad de la Información en el plazo y forma establecidos según la tarea de adecuación Nro. 34 de la presente planilla.	Cumple
II	**5**	c	-	Auditoría Interna aún no ha verificado la existencia y el cumplimiento de la gestión de seguridad de la información en PCR. Para este fin, PCR considera fundamental establecer las responsabilidades de la Junta Directiva y del Auditor Interno en lo que respecta verificar la existencia y cumplimiento de un adecuado SGSI, para lo cual actualizará su MOF (Manual de Organización y Funciones), estableciendo, entre las funciones del Auditor Interno, la verificación del cumplimiento de las regulaciones que rigen al SGSI de PCR.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
II	**6**	a	-	La función de la Alta Gerencia en PCR es asumida por el Coordinador País. Dicho cargo, a su vez, es también miembro del Comité de Gestión Integral de Riesgos de PCR y forma parte activa en la implementación del SGSI. No obstante esto, se reconoce como necesario actualizar el MOF (Manual de Organización y Funciones) de la Alta Gerencia (Gerentes y Coordinadores País), a fin de afianzar su compromiso con la gestión de la seguridad de la información de PCR.	Cumple
II	**6**	b	-	En vista de que aún no se ha realizado la auditoría a la Gestión de la Seguridad de la Información de PCR El Salvador, tampoco se han realizado acciones que impulsen la mejora continua del SGSI de la entidad. En este sentido, se considera fundamental primero actualizar el MOF (Manual de Organización y Funciones) del puesto de los Gerentes y Coordinadores País, a fin de involucrarlos en este aspecto del SGSI.	Cumple
II	**6**	c	-	La función de la Alta Gerencia en PCR es asumida por el Coordinador País. Dicho cargo, a su vez, es también miembro del Comité de Gestión Integral de Riesgos de PCR y forma parte activa en la implementación del SGSI. No obstante esto, se reconoce como necesario actualizar el MOF (Manual de Organización y Funciones) de la Alta Gerencia (Gerentes y Coordinadores País), a fin de afianzar su compromiso con la gestión de la seguridad de la información de PCR.	Cumple
II	**7**	a	-	Aún no se ha definido la responsabilidad del Comité de Gestión Integral de Riesgos en lo que respecta la propuesta de una estructura del SGSI ante la Junta Directiva. Dado el giro del negocio, el tamaño y la complejidad de las operaciones de PCR, no obstante, la Unidad de Gestión Integral de Riesgos funge también como Función de la Seguridad de la Información, considerando que el Oficial de Gestión Integral de Riesgos cuenta con las competencias de un profesional certificado en la ISO 31000 como Risk Manager (PECB - Professional Evaluation Certification Board), además de conocer y emplear como marco de referencia a la norma ISO 27001 y 27002 para diseñar un adecuado SGSI. Por este motivo, en la práctica, quedó implícita la estructura del SGSI conformada por el Oficial de Gestión Integral de Riesgos, el Comité de Gestión Integral de Riesgos, el Comité de TI y la Junta Directiva. En línea con lo mencionado: *Se establece como plan de adecuación la actualización del MOF (Manual de Organización y Funciones) del Comité de Gestión Integral de Riesgos para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
II	**7**	b	-	PCR tiene asignados los recursos necesarios para establecer, implementar y mejorar su gestión de la seguridad de la información. Dentro de dichos recursos se contempla el presupuesto para la contratación de un Jefe de Administración, un Analista de IT, un Oficial de Gestión Integral de Riesgos y de la licencia de Office 365 Business Premium que a su vez incluye al Azure Active Directory para la configuración de políticas de seguridad a nivel corporativo. En virtud al nivel de madurez del SGSI de PCR, la entidad considera necesario actualizar el MOF (Manual de Organización y Funciones) del Comité de Gestión Integral de Riesgos a fin de fortalecer sus funciones en lo que respecta la gestión de la seguridad de la información de la entidad.	Cumple
II	**7**	c	-	Aún no se ha definido la responsabilidad del Comité de Gestión Integral de Riesgos en lo que respecta efectuar el seguimiento de la gestión de la seguridad de la información de PCR. Dado el giro del negocio, el tamaño y la complejidad de las operaciones de PCR, no obstante, la Unidad de Gestión Integral de Riesgos funge también como Función de la Seguridad de la Información, considerando que el Oficial de Gestión Integral de Riesgos cuenta con las competencias de un profesional certificado en la ISO 31000 como Risk Manager (PECB - Professional Evaluation Certification Board), además de conocer y emplear como marco de referencia a la norma ISO 27001 y 27002 para diseñar e impulsar la implementación de un adecuado SGSI. Por este motivo, en la práctica, quedó implícita la tarea de seguimiento a la gestión de la seguridad de la información por parte del Oficial de Gestión Integral de Riesgos, reportando sus resultados al Comité de Gestión Integral de Riesgos, semestralmente o cuando la situación lo amerite. En línea con lo mencionado: *Se establece como plan de adecuación la actualización del MOF (Manual de Organización y Funciones) del Comité de Gestión Integral de Riesgos para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
II	**8**	a	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta proponer la creación de Comités, áreas o cargos especializados para el cumplimiento de las responsabilidades que exige el SGSI. Dado el giro del negocio, el tamaño y la complejidad de las operaciones de PCR, no obstante, la Unidad de Gestión Integral de Riesgos ya funge como Función de la Seguridad de la Información desde el 2019, considerando que el Oficial de Gestión Integral de Riesgos cuenta con las competencias de un profesional certificado en la ISO 31000 como Risk Manager (PECB - Professional Evaluation Certification Board), además de conocer y emplear como marco de referencia a la norma ISO 27001 y 27002 para diseñar un adecuado SGSI. Por este motivo, en la práctica, no fue necesario proponer la creación de Comités, áreas o cargos adicionales para hacerse cargo de la gestión de la seguridad de la información de PCR. En línea con lo mencionado: *Se establece como plan de adecuación la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgos para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23.	Cumple
II	**8**	b	-	PCR tiene identificados y medidos sus riesgos de seguridad de la información de acuerdo a lo señalado en el documento normativo "Metodologías para la Gestión Integral de Riesgos de PCR". En tal sentido, si bien la Unidad de GIR cumple su rol en la identificación de los riesgos de seguridad de la información, es primordial que se establezcan sus responsabilidades para con el SGCN en el MOF (Manual de Organización y Funciones) del puesto de Oficial de Gestión Integral de Riesgos.	Cumple
II	**8**	-	-	Elaborar el Informe de Evaluación Técnica de la Gestión Integral de Riesgos incluyendo los resultados de la Gestión de Seguridad de la Información	Cumple
II	**9**	b	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta coordinar entre las diversas áreas relevantes de PCR para la administración del SGSI. Dado el giro del negocio, el tamaño y la complejidad de las operaciones de PCR, no obstante, la Unidad de Gestión Integral de Riesgos ya funge como Función de la Seguridad de la Información, lo que en la práctica se ve reflejado en tareas de coordinación con las demás áreas de la entidad para analizar e identificar los activos de la información que requieren mayor protección y resguardo. En línea con lo mencionado: *Se establece como plan de adecuación la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgos para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
II	**9**	c	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta velar por una gestión eficaz de la seguridad de la información. En línea con lo mencionado, se establece: *Como plan de adecuación, la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgos para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23. *El cumplimiento de los planes de adecuación en el plazo y forma definidos en los números de identificador del 25 al 38 (catorce en total), a fin de satisfacer el requisito del Art. 9, literal c de la NRP-23.	Cumple
II	**9**	d	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta proponer un manual de controles específicos de seguridad de la información al Comité de Gestión Integral de Riesgos. En línea con lo mencionado, se establece: *Como plan de adecuación, la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgos para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23. *El cumplimiento del plan de adecuación en el plazo y forma definidos con número de identificador 26.	Cumple
II	**9**	e	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta coordinar con las áreas correspondientes la implementación de los controles de seguridad de la información de PCR. En línea con lo mencionado, se establece: *Como plan de adecuación, la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgos para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23. *El cumplimiento del plan de adecuación en el plazo y forma definidos con el número de identificador 79.	Cumple
II	**9**	f	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta diseñar y proponer las métricas que permitan revisar y monitorear la seguridad de la información. En línea con lo mencionado, se establece: *Como plan de adecuación, la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgos para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
				*El cumplimiento del plan de adecuación en el plazo y forma definidos con el número de identificador 28.	
II	**9**	g	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta desarrollar actividades de concientización a todo el personal en seguridad de la información. En línea con lo mencionado, se establece: *Como plan de adecuación, la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgos para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23. *El cumplimiento del plan de adecuación en el plazo y forma definidos con el número de identificador 29, con relación al curso de entrenamiento en seguridad de la información: ciberseguridad.	Cumple
II	**9**	h	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta la elaboración del programa de seguridad de la información para propuesta al Comité de Gestión Integral de Riesgos. En línea con lo mencionado: *Se establece como plan de adecuación la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgo para así fortalecer su rol en el SGSI considerando este aspecto de la norma NRP-23. *Se dará cumplimiento, en el plazo y forma establecidos, a la tarea de adecuación Nro. 34 de la presente planilla, donde se establece proponer el Programa de Seguridad de la Información para aprobación del Comité de Gestión Integral de Riesgos y de la Junta Directiva.	Cumple
II	**9**	i	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta la evaluación de los incidentes de seguridad de la infromación y de ciberseguridad. En línea con lo mencionado: *Se establece como plan de adecuación la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgo para formalizar su compromiso con el SGSI de PCR, considerando este aspecto de la norma NRP-23. *Se dará cumplimiento al monitoreo de posibles incidentes de seguridad de la información, de acuerdo a lo establecido en las tareas de adecuación con números de identificador del 67 al 73 (diecisiete tareas), expuestos en la presente planilla.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
II	**9**	j	-	Aún no se ha definido la responsabilidad de la Unidad de Gestión Integral de Riesgos en lo que respecta informar al Comité de Gestión Integral de Riesgos sobre los aspectos relevantes del SGSI para la toma de decisiones. Asimismo, se destaca que el Comité de Gestión Integral de Riesgos tiene conocimiento de que aún existen brechas que deben ser cerradas para alcanzar el nivel de cumplimiento y madurez requeridos por la norma NRP-23 de la SSF. Esto se evidencia por su participación activa en el diseño de los planes de adecuación remitidos al regulador, y por la aprobación elevada de los mismos a la Junta Directiva. En línea con lo mencionado: *Se establece como plan de adecuación la actualización del MOF (Manual de Organización y Funciones) del Oficial de Gestión Integral de Riesgo para formalizar su compromiso con el SGSI de PCR, considerando este aspecto de la norma NRP-23. Por otra parte, a objeto de realizar una revisión periódica más detallada del SGSI, se presentará semestralmente los avances de la implementación de la Norma NRP-23 al Comité de Gestión Integral de Riesgos a partir del segundo semestre de la gestión 2021.	Cumple
III	**10**	a	i	Proponer al Comité de Gestión Integral de Riesgos y a la Junta Directiva, la actualización de la Política de Seguridad de la Información, especificando el alcance del SGSI de PCR.	Cumple
III	**10**	a	ii	Proponer, para aprobación del Comité de Gestión Integral de Riesgos y de la Junta Directiva, la actualización de la Política de Seguridad de la Información, para su posterior difusión, concientización y puesta en marcha en toda la entidad.	Cumple
III	**10**	a	iii	Actualmente se tiene identificados los riesgos de seguridad de la información de PCR habiendo aplicado las metodologías vigentes en el documento normativo "Metodologías para la Gestión Integral de Riesgos de PCR". No obstante esto, se considera fundamental incluir en la Política de Seguridad de la Información de PCR a este lineamiento a fin de garantizar su cumplimiento y actualización periódicos.	Cumple
III	**10**	a	iv	Actualmente, se tienen establecidos controles de seguridad de la información al interior de PCR, sin embargo, estos no están aún documentados en ninguna norma interna. En tal sentido, se establece como plan de acción la inclusión de un catálogo de los controles específicos que están siendo aplicados en PCR, dentro del Protocolo de Seguridad de la Información de la entidad.	Cumple
III	**10**	b	i	Elaborar un Informe de Análisis de Riesgos de Seguridad de la Información en el cual se definan los planes y estrategias a aplicar para el tratamiento de los riesgos identificados.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**10**	b	ii	Actualmente, se tienen establecida una metodología para medir la efectividad de los controles de un proceso (herramientas de gestión del riesgo operativo). A efectos de revisar y complementar la citada metodología, se establece proponer al Comité de Gestión Integral de Riesgos y a la Junta Directiva la actualización de las "Metodologías para la Gestión Integral de Riesgos de PCR".	Cumple
III	**10**	b	iii	PCR capacita a todo su personal en materia de seguridad de la información y en el rol de los usuarios para su debido resguardo. En tal sentido, se establece como tarea de adecuación la elaboración de un curso de entrenamiento en ciberseguridad para difusión adicional al actual, sujeta a una prueba de conocimientos de todo el personal.	Cumple
III	**10**	b	iv	PCR cuenta con una Política de Seguridad de la Información y también con los respectivos controles para su resguardo y protección. A fin de dar cumplimiento a este romano de la norma técnica, se establece formalizar la actual sinergia entre las áreas que administran los recursos que componen al SGSI, es decir, el área de Administración, la Unidad de Tecnologías de la Información, el área de Gestión Integral de Riesgos y la Alta Gerencia (Coordinador País). Dicha formalización, se verá reflejada en la versión actualizada de la Política de Seguridad de la Información para la gestión 2021.	Cumple
III	**10**	b	v	Actualmente, se tienen establecidos controles para la inmediata detección y respuesta a incidentes de seguridad de la información, sin embargo, estos no están aún documentados en ninguna norma interna. En tal sentido, se establece como plan de acción la inclusión de los citados controles en un catálogo que formará parte del Protocolo de Seguridad de la Información de la entidad.	Cumple
III	**10**	c	i	El Comité de Gestión Integral de Riesgos tiene conocimiento de que aún existen brechas que deben ser cerradas para alcanzar el nivel de cumplimiento y madurez requeridos por la norma NRP-23 de la SSF. Esto se evidencia por su participación activa en el diseño de los planes de adecuación remitidos al regulador, y por la aprobación elevada de los mismos a la Junta Directiva. En línea con lo mencionado: *Proponer, para aprobación del Comité de Gestión Integral de Riesgos y de la Junta Directiva, la actualización de la Política de Seguridad de la Información incluyendo este punto de la norma NRP-23 como obligatorio para monitoreo periódico. *Asimismo, se establace que se realizará una revisión periódica más detallada de los avances de la implementación del SGSI de PCR, a presentarse semestralmente ante el Comité de Gestión Integral de Riesgos.	Cumple
III	**10**	c	ii	Evaluar los controles establecidos para la gestión de la seguridad de la información, aplicando las Metodologías para la Gestión Integral de Riesgos de PCR.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**10**	d	i	Evaluar los controles establecidos para la gestión de la seguridad de la información, aplicando las Metodologías para la Gestión Integral de Riesgos de PCR. Producto de dicha evaluación, aplicar mejoras a los controles que estén clasificados como "deficientes".	Cumple
III	**10**	d	ii	Evaluar los controles establecidos para la gestión de la seguridad de la información, aplicando las Metodologías para la Gestión Integral de Riesgos de PCR. Producto de dicha evaluación, establecer y ejecutar las acciones correctivas y preventivas que eliminen o mitiguen fallas en la seguridad de la información y ciberseguridad de PCR.	Cumple
III	**11**	a	-	Diseñar un Protocolo de Seguridad de la Información que incluya lo requerido para la gestión de la seguridad lógica, lo que permitirá cumplir con los procedimientos para la concesión, administración de derechos, perfiles y roles de cuentas privilegiadas y cuentas de usuarios finales, así como la desactivación de las mismas en los casos que sea requerido.	Cumple
III	**11**	b	-	Actualmente, PCR gestiona los accesos de los usuarios bajo el principio de menor privilegio. No obstante, se reconoce que es necesario establecer, mediante un Protocolo de Seguridad de la Información, la obligatoriedad de preservar una adecuada segregación de funciones que permita el control cruzado de la seguridad de la información.	Cumple
III	**11**	c	-	Revisar los derechos concedidos a los usuarios y el uso real de los derechos, plasmando los resultados en un reporte o informe dirigido al Comité de Gestión Integral de Riesgos	Cumple
III	**11**	e	-	PCR, a través del Azure Active Directory, permite controlar permanentemente el tráfico de información al interior de la entidad y fuera de ella, sin embargo, se reconoce que aún no se ha formalizado este lineamiento en el marco normativo interno de la Clasificadora. En línea con lo mencionado, se actualizará la Política de Seguridad de la Información de PCR para aprobación del Comité de Gestión Integral de Riesgos y de la Junta Directiva, incluyendo este aspecto como mandatorio para el SGSI.	Cumple
III	**11**	f	-	PCR, a través del Azure Active Directory, permite realizar el mantenimiento, monitoreo y análisis de los registros de auditoría para diversas actividades de los usuarios, sin embargo, se reconoce que aún no se ha formalizado este lineamiento en el marco normativo interno de la Clasificadora. En línea con lo mencionado, se actualizará la Política de Seguridad de la Información de PCR para aprobación del Comité de Gestión Integral de Riesgos y de la Junta Directiva, incluyendo este aspecto como mandatorio para el SGSI.	Cumple
III	**11**	g	-	PCR, a través del Azure Active Directory, permite detectar actividades no autorizadas para los usuarios de Office 365, sin embargo, se reconoce que a la fecha no se ha formalizado la tarea propia de seguimiento de las pistas de auditoría respectivas dentro del marco normativo interno de la Clasificadora. En línea con lo mencionado, se actualizará la Política de Seguridad de la Información de PCR para aprobación del Comité de Gestión Integral de Riesgos y de la Junta Directiva, incluyendo este aspecto como mandatorio para el SGSI.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**12**	b	-	Difundir periódicamente comunicados o boletines que describan brevemente los distintos tipos de ciberataques que podrían afectar la seguridad de la información de PCR.	Cumple
III	**12**	c	-	Proponer capacitaciones que deben recibir regularmente los miembros de la Junta Directiva, Comité de Riesgos, Alta Gerencia y otros que designe la Junta Directiva de la entidad en temas relacionados con ciberseguridad y mantenerlos actualizados sobre las nuevas ciberamenazas.	Cumple
III	**12**	d	-	PCR cuenta con un proveedor de servicios de IT que presenta reportes mensuales relacionados con el cumplimiento de las políticas de seguridad de la información configuradas en el Azure Active Directory. En este sentido, corresponde al Oficial de Gestión Integral de Riesgos identificar posibles desvíos en dichos reportes y, cuando amerite, presentarlos ante el Comité de Gestión Integral de Riesgos y ante la Junta Directiva. Dicha tarea de comunicación a los órganos de control se realizará trimestralmente desde la sesión 04/2021 programada para el mes de octubre del año el curso.	Cumple
III	**12**	-	-	Elaborar un Protocolo de Seguridad de la Información que establezca la tarea de los usuarios estándar, en lo que respecta reportar eventos e incidentes de seguridad de la información, así como cualquier debilidad o falla que identifiquen en sus equipos de cómputo a la Unidad de Tecnologías de la Información y al Oficial de Gestión Integral de Riesgos.	Cumple
III	**13**	a	-	Elaborar un Protocolo de Seguridad de la Información que establezca la tarea de la Unidad de Tecnologías de la Información y del Oficial de Gestión Integral de Riesgos en lo que respecta reportar a la Alta Gerencia y a la Superintendencia sobre los incidentes de seguridad de la información y de ciberseguridad que se susciten en PCR, registrando para ello los campos requeridos por la SSF, en una bitácora de eventos.	Cumple
III	**13**	b	-	Elaborar un Protocolo de Seguridad de la Información que establezca la información que PCR reportará, de acuerdo a sus políticas internas a sus clientes y usuarios de productos y servicios financieros afectados, sobre incidentes de ciberseguridad que hubiesen afectado la confidencialidad o integridad de su información, así como las medidas adoptadas para mitigar el incidente.	Cumple
III	**14**	-	-	Evaluar la elaboración de un modelo de Contrato o Adenda que PCR requiera suscribir, donde se incluya los requisitos mínimos de seguridad para servicios críticos terciarizados.	Cumple
III	**16**	a	i	Si bien PCR administra efectivamente el control de accesos a su información, no se tienen formalizados dichos controles a nivel operativo. En línea con lo mencionado, se establece como plan de adecuación la elaboración de un Protocolo de Seguridad de la Información que incluya la aplicación de los controles citados para la etapa de "prevención".	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**16**	a	ii	Actualmente, se tienen establecidos controles de seguridad de la información al interior de PCR, sin embargo, estos no están aún documentados en ninguna norma interna. En tal sentido, se establece como plan de acción la inclusión de un catálogo de los controles específicos que están siendo aplicados en PCR, dentro del Protocolo de Seguridad de la Información de la entidad.	Cumple
III	**16**	a	iii	Elaborar un Protocolo de Seguridad de la Información que establezca la tarea de los usuarios estándar, en lo que respecta reportar eventos e incidentes de seguridad de la información, así como cualquier debilidad o falla que identifiquen en sus equipos de cómputo a la Unidad de Tecnologías de la Información y al Oficial de Gestión Integral de Riesgos.	Cumple
III	**16**	a	iv	Elaborar un Protocolo de Seguridad de la Información que establezca la tarea de la Unidad de Tecnologías de la Información y del Oficial de Gestión Integral de Riesgos en lo que respecta reportar a la Alta Gerencia y a la Superintendencia sobre los incidentes de seguridad de la información y de ciberseguridad que se susciten en PCR, registrando para ello los campos requeridos por la SSF, en una bitácora de eventos.	Cumple
III	**16**	a	v	Monitorear las diferentes fuentes de información (sitios web, blogs, redes sociales, proveedores y comunidades de interés), que divulguen vulnerabilidades o amenazas de ciberseguridad que apliquen a Office 365. Comunicar los principales hallazgos de este monitoreo al Comité de Gestión Integral de Riesgos y Junta Directiva.	Cumple
III	**16**	a	vi	Publicar recomendaciones para adoptar una adecuada gestión de la ciberseguridad en la página web de PCR.	Cumple
III	**16**	a	vii	Actualizar el Inventario de Activos de la Información, identificando aquellos que se encuentran en formato digital.	Cumple
III	**16**	b	i	PCR contrató el servicio de ethical hacking en la gestión 2020 para la identificación de sus vulnerabilidades técnicas, no habiéndose evidenciado ninguna que represente un riesgo alto o moderado para la entidad. Esta práctica, aún no está definida en los documentos normativos internos de la entidad, por lo tanto, se incluirá como parte de la etapa de "protección y detección" dentro del Protocolo de Seguridad de la Información de PCR.	Cumple
III	**16**	b	ii	PCR contrató el servicio de ethical hacking en la gestión 2020 para la identificación de sus vulnerabilidades técnicas, no habiéndose evidenciado ninguna que represente un riesgo alto o moderado para la entidad. Esta práctica, aún no está definida en los documentos normativos internos de la entidad, por lo tanto, se incluirá como parte de la etapa de "protección y detección" dentro del Protocolo de Seguridad de la Información de PCR.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**16**	b	iii	Office 365, a través del Azure Active Directory, realiza el monitoreo continuo de la infraestructura tecnológica de PCR, e identifica así como mitiga potenciales ataques externos que puedan poner en riesgo la seguridad de la información de la entidad. Se reconoce, no obstante, que esta herramienta integral, debe estar formalizada en el Protocolo de Seguridad de la Información, para su gestión desde el área de Administración y Unidad de TI.	Cumple
III	**16**	c	i	Las áreas de Administración y de Gestión Integral de Riesgos coordinan frecuentemente para realizar una efectiva gestión de la seguridad de la información al interior de PCR, lo cual implica una fluida comunicación a través de diversos canales de la Clasificadora (correo electrónico, mensajería instantánea, teléfono), en caso de requerir atender algún incidente de seguridad de la información de manera inmediata. No obstante lo señalado, se reconoce que es necesario elaborar un Protocolo de Seguridad de la Información que establezca las tareas necesarias para mitigar incidentes relacionados con la ciberseguridad de PCR.	Cumple
III	**16**	c	ii	Diseñar un Protocolo de Seguridad de la Información que establezca la tarea de la Unidad de Tecnologías de la Información y del Oficial de Gestión Integral de Riesgos en lo que respecta coordinar para evaluar los elementos de la red que pudieran ser afectados por un ciberataque.	Cumple
III	**16**	c	iii	Diseñar un Protocolo de Seguridad de la Información que establezca los mecanismos que deberían ser empleados para que PCR pueda recuperarse de un ataque cibernético.	Cumple
III	**16**	c	iv	Verificar que se cuente con la generación de reportes de pistas de auditoría periódicos a fin de poder emplearlos como evidencia digital en caso de suscitarse un ciberataque.	Cumple
III	**16**	d	i	Incluir, en el punto III.g "Plan de Recuperación de Desastres" del Plan de Continuidad del Negocio de PCR, las medidas a implementar en caso de suscitarse un ciberataque, a fin de para ajustar/modificar las políticas configuradas en el Azure Active Directory. Presentar dicho documento ante el Comité de Gestión Integral de Riesgos y ante la Junta Directiva para su aprobación.	Cumple
III	**16**	d	ii	Incluir, en el punto III.f "Plan de emergencias para la gestión de incidentes" del Plan de Continuidad del Negocio de PCR, las medidas a implementar para la recuperación y reanudación de las operaciones de la entidad. Presentar dicho documento ante el Comité de Gestión Integral de Riesgos y ante la Junta Directiva para su aprobación.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**16**	d	iii	Incluir, en el punto III.j "Mantenimiento y ejercicios del BCP" del Plan de Continuidad del Negocio de PCR, la obligatoriedad de realizar al menos una prueba simulada de ciberataque para entrenar al personal involucrado en el SGSI y el SGCN de la entidad. Presentar dicho documento ante el Comité de Gestión Integral de Riesgos y ante la Junta Directiva para su aprobación. Por otra parte, cabe mencionar que la realización de las mencionadas pruebas se tiene definida entre las tareas de adecuación definidas para la norma NRP-24.	Cumple
III	**17**	b	-	Proponer al Comité de Gestión Integral de Riesgos y a la Junta Directiva, la actualización del apartado III.7 "Proceso Disciplinario" contenido en la Política de Seguridad de la Información de la entidad, a fin de que esté debidamente alineado a cualquier actualización efectuada al Reglamento Interno de Trabajo de la Clasificadora.	Cumple
III	**17**	c	-	PCR tiene definidas políticas para la protección de la información ante el cese de alguno de sus colaboradores, sin embargo, no se tiene definida la operativa para dichas políticas. En línea con lo mencionado, se elaborará un Protocolo de Seguridad de la Información que incluirá los procedimientos para la baja de usuarios y devolución de activos en caso de cese del personal.	Cumple
III	**18**	a	-	Elaborar un Protocolo de Seguridad de la Información que establezca los controles de seguridad física y ambiental que debe aplicarse a los activos de información, de acuerdo a su nivel de criticidad.	Cumple
III	**18**	b	-	Actualmente, se tienen establecidas medidas de prevención para la preservación de la confidencialidad, disponibilidad e integridad de la información de PCR dentro del Plan de Continuidad del Negocio. En tal sentido, se debe incluir en el Protocolo de Seguridad de la Información a los controles citados en la norma NRP-23, artículo 18, literal b, según lo requerido por la SSF.	Cumple
III	**19**	a	-	PCR cuenta con un Inventario de Activos de la Información elaborado en abril de 2020. Se debe revisar y, si es pertinente actualizar el mismo en la gestión 2021, identificando al propietario, custodio y usuario de cada tipo de activo.	Cumple
III	**19**	b	-	PCR cuenta con un Inventario de Activos de la Información elaborado en abril de 2020. Se debe actualizar el mismo en la gestión 2021 clasificando cada tipo de activo por nivel de criticidad.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**20**	a	-	PCR cuenta con un Comité de Tecnología que monitorea si es necesario implementar cambios en la infraestructura tecnológica de la entidad a fin de evitar el riesgo de obsolescencia de la misma. No obstante esto, se elaborará un Informe de Evaluación de la Infraestructura Tecnológica mínimamente anual, proponiendo los cambios o mejoras que se podría implementar para la operación de los sistemas informáticos.	Cumple
III	**20**	b	-	PCR no tiene planificado realizar cambios en su infraestructura tecnológica, al menos hasta finalizar el 2022, cuando deberá evaluar si es necesario actualizar su Plan Estratégico de IT. No obstante esto, en caso de surgir la necesidad de realizar dichos cambios de manera no prevista, se debe establecer la operativa y controles mínimos a ser aplicados en el Protocolo de Seguridad de la Información de la entidad.	Cumple
III	**20**	c	-	PCR no tiene planificado realizar cambios en su infraestructura tecnológica, al menos hasta finalizar el 2022, cuando deberá evaluar si es necesario actualizar su Plan Estratégico de IT. No obstante esto, en caso de surgir la necesidad de realizar dichos cambios de manera no prevista, se debe establecer la operativa y controles mínimos a ser aplicados en el Protocolo de Seguridad de la Información de la entidad.	Cumple
III	**20**	d	-	PCR no tiene planificado realizar cambios en su infraestructura tecnológica, al menos hasta finalizar el 2022, cuando deberá evaluar si es necesario actualizar su Plan Estratégico de IT. No obstante esto, en caso de surgir la necesidad de realizar dichos cambios de manera no prevista, se debe establecer la operativa y controles mínimos a ser aplicados en el Protocolo de Seguridad de la Información de la entidad.	Cumple
III	**20**	e	-	PCR cuenta con un Comité de Tecnología que monitorea si es necesario implementar cambios en la infraestructura tecnológica de la entidad a fin de garantizar su capacidad de procesamiento, almacenamiento y transmisión de información. No obstante esto, en caso de surgir la necesidad aplicar mejoras en dichas capacidades, se debe establecer la operativa pertinente a través de un Protocolo de Seguridad de la Información.	Cumple
III	**20**	f	-	PCR cuenta con controles preventivos y de detección sobre el uso de programas informáticos de procedencia dudosa, virus, malware, denegación de servicios, phishing y otros similares. Dichos controles se aplican a través del antivirus BitDefender y mediante el Azure Active Directory a nivel corporativo. No obstante esto, se reconoce que es necesario incluir a estos controles en el catálogo que formará parte del Protocolo de Seguridad de la Información de la entidad.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**20**	g	-	PCR tiene definidas y configuradas políticas que restringen el uso de cuentas de correo electrónico personales para el desarrollo de las funciones de su personal. Sin embargo, se reconoce que es necesario incluir este y otros controles según lo citado en el Artículo 20, literal g dentro del Protocolo de Seguridad de la Información de la entidad.	Cumple
III	**20**	h	-	El Azure Active Directory de Office 365 ofrece la opción de generar reportes con pistas de auditoría para diversas actividades que realizan los usuarios de PCR. Dichos reportes, son generados por el Analista de IT de la entidad cuando es requerido por el Oficial de Gestión Integral de Riesgos. En tal sentido, a fin de efectivizar el uso de este control, se propondrá el mismo dentro del catálogo de controles que fomará parte del Protocolo de Seguridad de la Información de PCR.	Cumple
III	**20**	i	-	PCR contrató el servicio de ethical hacking en la gestión 2020 para la identificación de sus vulnerabilidades técnicas, no habiéndose evidenciado ninguna que represente un riesgo alto o moderado para la entidad. Esta práctica, se realizará una vez más en la gestión 2021 durante el cuarto trimestre.	Cumple
III	**21**	a	-	PCR no tiene planificada la adquisición, desarrollo ni mantenimiento de algún sistema informático hasta finalizar el 2022, cuando deberá evaluar si es necesario actualizar su Plan Estratégico de IT. No obstante esto, en caso de surgir la necesidad de realizar dichos cambios de manera imprevista, se debe establecer la operativa y controles mínimos a ser aplicados en el Protocolo de Seguridad de la Información de la entidad.	Cumple
III	**21**	b	-	PCR tiene definido en el punto VII.1 de su Política de Seguridad de la Información, que tomará en cuenta la opción de cifrado de la misma con base en un análisis y evaluación de riesgos. Adicional a esto, se solicitará al área de Administración pueda instruir realizar el cifrado de la información de los equipos de cómputo (discos duros) de todo el personal de PCR para prevenir el mal uso de la información por parte de terceros, ante algúnn evento de robo del(los) equipo(s).	Cumple
III	**21**	c	-	PCR tiene definido en el punto VII.2 de su Política de Seguridad de la Información a los principios bàsicos a aplicar en caso de someter sus sistemas de información a un proceso de migración. Sin embargo, a la fecha PCR no tiene planificada la adquisición, desarrollo ni mantenimiento de algún sistema informático hasta finalizar el 2022, cuando deberá evaluar si es necesario actualizar su Plan Estratégico de IT. En este sentido, en caso de surgir la necesidad de realizar dichos cambios de manera imprevista, se debe establecer la operativa y controles mínimos a ser aplicados en un Protocolo de Seguridad de la Información de la entidad.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**21**	d	-	PCR no tiene planificada la adquisición, desarrollo ni mantenimiento de algún sistema informático hasta finalizar el 2022, cuando deberá evaluar si es necesario actualizar su Plan Estratégico de IT. No obstante esto, en caso de surgir la necesidad de realizar dichos cambios de manera imprevista, se debe establecer la operativa y controles necesarios para tener acceso al código fuente de los sistemas informáticos que serán propiedad de la entidad, dentro de su Protocolo de Seguridad de la Información.	Cumple
III	**21**	e	-	PCR no tiene planificada la adquisición, desarrollo ni mantenimiento de algún sistema informático hasta finalizar el 2022, cuando deberá evaluar si es necesario actualizar su Plan Estratégico de IT. No obstante esto, en caso de surgir la necesidad de realizar dichos cambios de manera imprevista, se debe establecer la operativa y controles necesarios para mantener un estricto y formal control de cambios y versiones de los sistemas informáticos, dentro del Protocolo de Seguridad de la Información.	Cumple
III	**21**	f	-	PCR no tiene planificada la adquisición, desarrollo ni mantenimiento de algún sistema informático hasta finalizar el 2022, cuando deberá evaluar si es necesario actualizar su Plan Estratégico de IT. No obstante esto, en caso de surgir la necesidad de realizar dichos cambios de manera imprevista, se debe establecer los mecanismos de desarrollo seguro que permitan analizar y corregir las vulnerabilidades de seguridad existentes en las aplicaciones informáticas de la entidad, dentro de su Protocolo de Seguridad de la Información.	Cumple
III	**21**	g	-	El área de Gestión Integral de Riesgos promueve, a través de sus boletines de seguridad de la información y TI, que los usuarios sean quienes actualicen el software de sus equipos continuamente a fin de prevenir vulnerabilidades y eventos de mal funcionamiento en general. No obstante esto, se reconoce la necesidad de establecer esta actividad como un control necesario en la primera línea de defensa de PCR: los usuarios estándar.	Cumple
III	**22**	-	-	Elaborar un Informe de Evaluación de Riesgos para la adquisición de sistemas informáticos y presentar sus recomendaciones al Comité de Gestión Integral de Riesgos y a la Junta Directiva.	Cumple
III	**23**	-	-	Los colaboradores de PCR almacenan su información en la nube, dentro de sus cuentas de OneDrive corporativas. Así también, la entidad cuenta con Microsoft Teams y con la Intranet (SharePoint) para efectos de compartir información que debe ser trabajada y/o socializada entre varias personas. Al efecto, se tiene definidos puntos de restauración de la información en caso de desastres cibernéticos, sin embargo, el uso de estos no se encuentra definido en ningún documento normativo de la entidad. En este sentido, se establece la inclusión de este tipo de control en el catálogo de controles que formará parte del Protocolo de Seguridad de la Información de PCR.	Cumple

Capítulo	Artículo	Literal	Romano	Tarea de Adecuación	Estado al 31-12-2021
III	**24**	a	-	Elaborar un Protocolo de Seguridad de la Información que establezca la tarea de los usuarios estándar, en lo que respecta reportar eventos e incidentes de seguridad de la información, así como cualquier debilidad o falla que identifiquen en sus equipos de cómputo a la Unidad de Tecnologías de la Información y al Oficial de Gestión Integral de Riesgos.	Cumple
III	**24**	b	-	Elaborar un Protocolo de Seguridad de la Información que establezca la tarea de la Unidad de Tecnologías de la Información y del Oficial de Gestión Integral de Riesgos en lo que respecta reportar a la Alta Gerencia y a la Superintendencia sobre los incidentes de seguridad de la información y de ciberseguridad que se susciten en PCR, registrando para ello los campos requeridos por la SSF, en una bitácora de eventos.	Cumple
IV	**27**	-	-	No aplica para PCR, ya que no es parte de un conglomerdado financiero	No aplica para PCR, ya que no es parte de un conglomerdado financiero
IV	**28**	-	-	PCR cumple con el estricto resguardo de la información de todos sus clientes, según lo establecido en el marco legal aplicable. Se reconoce, no obstante, la necesidad de incluir este lineamiento dentro de la Política de Seguridad de la Información de la entidad para puesta en consideración del Comité de Gestión Integral de Riesgos y de la Junta Directiva.	Cumple
IV	**29**	a	-	Elaborar el Informe de Evaluación Técnica de la Gestión Integral de Riesgos incluyendo los resultados de la Gestión de Seguridad de la Información	Cumple
IV	**29**	b	-	Elaborar el Informe de Evaluación Técnica de la Gestión Integral de Riesgos incluyendo los resultados de la Gestión de Seguridad de la Información	Cumple
IV	**29**	c	-	Elaborar el Informe de Evaluación Técnica de la Gestión Integral de Riesgos incluyendo los resultados de la Gestión de Seguridad de la Información	Cumple
IV	**30**	-	-	Incluir la evaluación del cumplimiento de la NRP-23 en el Plan Anual de la Unidad de Auditoría Interna	Cumple
IV	**31**	-	-	No aplica	No aplica
V	**32**	-	-	No aplica	No aplica
V	**33**	-	-	No aplica	No aplica
V	**34**	-	-	PCR no tiene planificada la adquisición, desarrollo ni mantenimiento de algún sistema informático hasta finalizar el 2022, cuando deberá evaluar si es necesario actualizar su Plan Estratégico de IT. No obstante esto, en caso de surgir la necesidad de realizar contrataciones de manera imprevista, se debe establecer lo dispuesto en el artículo 22, literal c) de la NRP-23, dentro del Protocolo de Seguridad de la Información de la entidad.	No aplica
V	**36**	-	-	No aplica	No aplica
V	**37**	-	-	No aplica	No aplica

IV.c Programa de Seguridad de la Información

El Programa de Seguridad de la Información de PCR para el 2022 se basa primordialmente en la implementación de los planes de acción aprobados por la Junta Directiva y remitidos al Sistema de Control de Envíos de la SSF en diciembre de 2020 y complementados en agosto de 2021 a requerimiento del regulador, cuyos plazos están plasmados en dicho reporte.

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

Daniela Urquizo Rojas
OFICIAL DE GESTION INTEGRAL DE RESGOS