PCR | PACIFIC CREDIT RATING

Política de Seguridad de la Información

Elaborado por:	Christian Jose Hernandez Corianga **Oficial de Gestión Integral de Riesgos**	**Revisado / Aprobado por:**	Oscar Jasaui Sabat **Presidente Ejecutivo**

ÍNDICE DE CONTENIDO

BITÁCORA DE MODIFICACIONES

Bitácora de Modificaciones				
No	**Sección y No. de página modificada**	**Descripción del cambio**	**Fecha de modificación**	**Nro. de Versión**
-	No aplica	No aplica, por ser la primera versión del documento	-	1
1	Punto I.7 Definiciones, Página 7	Eliminación del término "CSIRT (Computer Security Incident Response Team): Equipo responsable del desarrollo de medidas preventivas y de respuesta ante incidentes informáticos" en virtud a que PCR no está sujeta a regulaciones relacionadas con este ente.	21/04/2020	2
2	Punto I.4 Base Legal, Página 5	Se incorporan las Normas Técnicas para la Gestión de la Seguridad de la Información (NRP-23) entre las regulaciones que sirven de base legal de la presente Política	19/07/2021	3
3	Punto I.5 Marco Referencial Interno, Página 5	Se incorpora todos los documentos normativos internos que están relacionados con la presente Política.	19/07/2021	3
4	Punto I.6 Responsables, Página 6	Se presenta un detalle de las responsabilidades que deben cumplir distintos niveles jerárquicos de PCR para una adecuada gestión de la seguridad de la información.	19/07/2021	3
5	Punto I.7 Definiciones y Abreviaturas, Páginas 7-10	Se incorpora el significado de las sigas GIR, MOF, SGSI, además de otras definiciones relevantes para la comprensión del documento.	19/07/2021	3
6	Punto II.2 Estrategias y Recursos que componen al SGSI, Página 10	Se realiza precisiones acerca de las estrategias y recursos que utiliza PCR para gestionar la seguridad de la información.	19/07/2021	3
7	Punto II.3 Alcance del SGSI, Página 11	Se describe el alcance del Sistema de Gestión de la Seguridad de la Información en PCR	19/07/2021	3
8	Punto III.6 Responsabilidad de los colaboradores para la gestión de la seguridad de la información, Página 12	Se elimina toda la sección III.6, debido a que las responsabilidades de los colaboradores ya están incorporadas en el punto I.6 de la Política.	19/07/2021	3
9	Punto IV.3 Administración de contraseñas, Página 13	Se realizan precisiones a las políticas de manejo de contraseñas.	19/07/2021	3
10	Punto V.1 Reporte de incidentes de seguridad de la información, Página 14	Se incluye "cualquier sospecha de ciberataque" a la lista de tipos de incidentes que deben reportar los colaboradores de PCR al Analista de IT y al Oficial de Gestión Integral de Riesgo	19/07/2021	3
11	Punto VII.4 Respaldos o copias de seguridad, Página 16	Se realizan precisiones a las políticas para la realización de copias de seguridad.	19/07/2021	3
12	Punto I.6 Responsables, Páginas 7 y 8	Se realizan precisiones a las funciones que debe cumplir el Directorio/Junta Directiva, el Gerente/Coordinador País, el Jefe de Tecnología de la Información, el Oficial de Gestión Integral de Riesgos y los colaboradores de PCR en general.	28/10/2022	4

Bitácora de Modificaciones

No	Sección y No. de página modificada	Descripción del cambio	Fecha de modificación	Nro. de Versión
13	Todo el documento	Se reemplaza los cargos de Jefe de Administración y Analista de IT por el cargo de Jefe de Tecnologías de la Información y Comunicación	28/10/2022	4
14	Capítulo IV. Administración de Accesos, Página 15	Se realizan precisiones de redacción referentes a la administración de cuentas de usuarios y a la administración de privilegios	28/10/2022	4
15	Punto VII.4 Respaldos o copias de seguridad	Se realizan precisiones referentes a la responsabilidad que tienen los custodios de la información en la generación de copias de respaldo.	28/10/2022	4
16	Todo el documento	Se reemplazó el cargo de Jefe de Tecnologías de la Información y Comunicación por Jefe de Tecnología de la Información	25/10/2023	5
17	Punto III.8 Actualizaciones de Software, Página 15	Se incorpora la realización del seguimiento semestral de la debida actualización de los equipos de cómputo por parte del Jefe de Tecnología de la Información	25/10/2023	5
18	Punto III.9 Devolución de información en caso de desvinculación, Página 16	Se precisa la realización de backups de información digital de los funcionarios desvinculados de PCR por parte del Jefe de Tecnología de la Información	25/10/2023	5
19	Punto III.4 Manejo de información confidencial, Página 13	Se realizan precisiones a las políticas de manejo de información confidencial	25/10/2023	5
20	Sección 4. Base Legal, página 6	Se eliminó los detalles de la normativa peruana dado que ya no aplica a las calificadoras de riesgo	02/12/2024	6
21	Sección 6. Responsables, páginas 7-8	Se realizaron ajustes a los responsables del cumplimiento de la presente política	02/12/2024	6

1. ANTECEDENTES

Toda información puede considerarse como un activo que, al igual que cualquier otro, es fundamental para una empresa, por lo que su debido resguardo y protección es esencial para la supervivencia y continuidad de las operaciones del negocio.

La empresa Pacific Credit Rating (PCR) se dedica a la asignación de calificación de riesgos como principal actividad comercial, para lo cual, maneja información de distintas fuentes tanto externas (clientes, mercado de valores, entorno económico, etc.), como internas (metodologías, procedimientos de análisis etc.), lo que conlleva a la necesidad de contar con una Política de Seguridad de la Información.

2. OBJETIVO DE LA POLÍTICA

Establecer normas y lineamientos para el debido resguardo y protección de la información que PCR genera y administra.

2.1 Objetivos Específicos

Preservar la *confidencialidad*, *confiabilidad*, *disponibilidad* e *integridad* de la información que genera y administra PCR, según los niveles y controles que defina para el efecto.

3. ALCANCE

La presente Política debe aplicarse a nivel corporativo en todas las Oficinas donde PCR presta servicios, abarcando todos los activos de información que genera y administra la organización, ya sea en formato impreso o digital.

4. BASE LEGAL

El presente documento se elaboró en función a lo señalado en las siguientes normas:

País	Título de la Norma	Descripción
Bolivia	Recopilación de Normas para el Mercado de Valores (ASFI)	Libro 11°, Título I, Capítulo I: Reglamento para la Gestión de Seguridad de la Información
El Salvador	NRP-23: Normas Técnicas para la Gestión Integral de la Seguridad de la Información	Todo el documento.
Resto de los países	Sin normativa específica.	En el resto de los países no se cuenta con normativa específica obligatoria sobre seguridad de la información para empresas Calificadoras de Riesgo.

5. MARCO REFERENCIAL INTERNO

Los siguientes documentos normativos internos mantienen relación directa con la Política de Seguridad de la Información de PCR:

- Política de Continuidad del Negocio
- Plan de Continuidad del Negocio
- Manual de Gestión Integral de Riesgos de PCR
- Metodologías para la Gestión Integral de Riesgos de PCR
- Procedimientos para la Gestión de la Seguridad de la Información

- Procedimientos para la Gestión Integral de Riesgos de PCR
- Protocolo de Seguridad de la Información

6. RESPONSABLES

La gestión de la seguridad de la información es un proceso que requiere del compromiso de todos los niveles jerárquicos de PCR, cuyas responsabilidades se detallan a continuación:

Instancia	Responsabilidades
Directorio o Junta Directiva	Según corresponda el país y su normativa: **a.** 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 o Comité 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 al Directorio/Junta Directiva. Si hubiese cambios en la asignación del(los) responsable(s) del SGSI, la Junta Directiva lo hará constar su nombramiento mediante Acta, la cual deberá ser remitida a la Superintendencia del Sistema Financiero de El Salvador a más tardar diez días hábiles después de dicho nombramiento. **b.** Aprobar el programa o plan de trabajo de seguridad de la información, cada año, así como cualquier cambio en la estructura del SGSI. **c.** Requerir a Auditoría Interna que verifique la existencia y el cumplimiento de la estructura del SGSI.
Comité de Tecnologías de la Información	Según corresponda el país y su normativa: **a.** Establecer los objetivos estratégicos de TI de PCR, e instruir la ejecución de las tareas que servirán para optimizar el uso de los recursos tecnológicos de PCR, tomando en cuenta siempre las directrices establecidas en esta Política, y en el Protocolo de Seguridad de la Información.
Gerente o Coordinador País	Según corresponda el país y su normativa: **a.** Apoyar y velar por el cumplimiento del programa o plan de trabajo de seguridad de la información. **b.** Promover la mejora continua del SGSI y velar por su vigencia permanente. **c.** Apoyar al responsable de la seguridad de la información en la ejecución de estrategias y tácticas de seguridad de la información requeridas. Ante un incidente de seguridad de la información o de ciberseguridad no previsto, el Gerente / Coordinador País deberá comunicarlo directamente al Directorio o la Junta Directiva.
Jefe de Tecnología de la Información	Según corresponda el país y su normativa: **a.** Ejecutar las tareas operativas de administración de usuarios y de control de la seguridad sobre el acceso lógico a los distintos recursos de información de PCR. **b.** Evaluar los incidentes de seguridad de la información y de ciberseguridad y recomendar, a las instancias correspondientes, acciones preventivas y correctivas, de acuerdo a procedimientos internos que establezca la entidad.
Oficial de Gestión Integral de Riesgos	Según corresponda el país y su normativa: **a.** Proponer al Comité de Gestión Integral de Riesgos la creación de Comités, áreas o cargos especializados para el cumplimiento de las responsabilidades relacionadas con la gestión de la seguridad de la información. **b.** Velar que la gestión de la seguridad de la información sea consistente con las políticas y metodologías aplicadas para la gestión de riesgos. **c.** Elaborar y proponer al Comité de Gestión Integral Riesgos las políticas y metodologías para la gestión de la seguridad de la información.

Instancia	Responsabilidades
	d. Coordinar entre las diversas áreas relevantes de la entidad la administración del SGSI. **e.** Velar por una gestión eficaz de la seguridad de la información. **f.** Proponer un manual de controles específicos de seguridad de la información, al Comité de Gestión Integral de Riesgos para su evaluación y validación y posteriormente someterlo a aprobación del Directorio o Junta Directiva solo si corresponde. **g.** Coordinar con las áreas correspondientes la implementación de los controles de seguridad de la información en toda la entidad y en las operaciones o procesos tercerizados, relacionados con activos de información de acuerdo a la clasificación de la información. **h.** Diseñar y proponer, al Comité de Gestión Integral de Riesgos para su evaluación y validación, las métricas que permitan revisar y monitorear la seguridad de la información solo si corresponde. **i.** Desarrollar actividades de concientización a todo el personal en seguridad de la información. **j.** Elaborar el programa o plan de trabajo de seguridad de la información y proponerlo al Comité de Gestión Integral de Riesgos, para su revisión, evaluación y aprobación solo si corresponde. **k.** Informar al Comité de Riesgos los aspectos relevantes de la gestión de la seguridad de la información para una oportuna toma de decisiones solo si corresponde. **l.** Proponer al Directorio o la Junta Directiva la estructura del SGSI solo si corresponde. **m.** Revisar, evaluar y proponer para aprobación del Directorio o 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. **n.** Efectuar el seguimiento y revisión periódica de la efectividad del SGSI.
Auditoría Interna	**a.** Verificar el cumplimiento de las políticas, procedimientos y controles implementados para el Sistema de Gestión de la Seguridad de la Información.
Todos los colaboradores de PCR	**a.** Reportar a su inmediato superior, al Jefe de Tecnología de la Información y al Oficial de Gestión Integral de Riesgos sobre cualquier incidente de seguridad de la información del que tengan conocimiento, considerando el detalle provisto en el punto “Reporte de eventos y debilidades en la seguridad de la información” del presente documento. **b.** Conocer y comprender esta política, y dar cumplimiento a lo requerido según el Protocolo de Seguridad de la Información de PCR.

6.1 Responsable de Revisión y Periodicidad de Actualización

El Oficial de Gestión Integral de Riesgos es el responsable de revisar y consecuentemente actualizar o proponer la ratificación de la presente Política al menos una vez al año, o cuando las condiciones del negocio y del entorno lo ameriten.

7. DEFINICIONES Y ABREVIATURAS

a) **GIR:** Gestión Integral de Riesgos

b) **MOF:** Manual de Organización y Funciones

c) **SGSI:** Sistema de Gestión de Seguridad de la Información de PCR

d) Activo de Información: En seguridad de la información, corresponde a aquellos datos, información, sistemas y elementos relacionados con la tecnología de la información, que tienen valor para PCR.

e) Acuerdo de Nivel de Servicio (SLA: Service Level Agreement): Contrato en el que se estipulan las condiciones de un servicio en función a parámetros objetivos, establecidos de mutuo acuerdo entre un proveedor de servicio y PCR.

f) Análisis y evaluación de riesgos en seguridad de la información: Proceso por el cual se identifican los activos de información, las amenazas y vulnerabilidades a las que se encuentran expuestos, con el fin de generar controles que minimicen los efectos de los posibles incidentes de seguridad de la información.

g) Cambio Significativo: Todo aquel cambio en el ambiente operativo, informático o de negocios que tenga una influencia significativa en el perfil de riesgo de una Entidad.

h) Centro de Procesamiento de Datos (CPD): Ambiente físico clasificado como área de exclusión, donde están ubicados los recursos utilizados para el procesamiento de información.

i) Centro de Procesamiento de Datos Alterno: Lugar alternativo provisto de equipos computacionales, equipos de comunicación, estaciones de trabajo, enlaces de comunicaciones, fuentes de energía y accesos seguros que se encuentran instalados en una ubicación geográfica distinta al Centro de Procesamiento de Datos.

j) Ciberamenaza o amenaza cibernética: Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

k) Ciberataque o ataque cibernético: Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

l) Ciberespacio: Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

m) Ciberseguridad: Condición de estar protegido en contra de consecuencias físicas, sociales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en el Ciberespacio que se pueda considerar no deseable.

n) Cifrar: Proceso mediante el cual la información o archivos es alterada, en forma lógica, incluyendo claves en el origen y en el destino, con el objetivo de evitar que personas no autorizadas puedan interpretarla al verla, copiarla o utilizarla para actividades no permitidas;

o) Contraseña o clave de acceso (Password): Conjunto de caracteres que una persona debe registrar para ser reconocida como usuario autorizado, para acceder a los recursos de un equipo computacional o red.

p) Cortafuegos (Firewall): Dispositivo o conjunto de dispositivos (software y/o hardware) configurados para permitir, limitar, cifrar, descifrar el tráfico entre los diferentes ámbitos de un sistema, red o redes, sobre la base de un conjunto de normas y otros

criterios, de manera que sólo el tráfico autorizado, definido por la política local de seguridad, sea permitido.

q) **Criterios mínimos de la información:** Son la confidencialidad, integridad y disponibilidad de la información.

- ✓ **Confidencialidad**: La información debe mantenerse en reserva, pudiendo ser accesible únicamente a aquellos usuarios que se encuentren debidamente autorizados, capacitados y supervisados.
- ✓ **Disponibilidad:** La información debe ser accesible a los usuarios autorizados cuando sea requerida.
- ✓ **Integridad:** La información debe ser completa, veraz y exacta.

r) **Gestión de la seguridad de la información:** Procesos mediante los cuales se previene, detecta y se responde a la seguridad de la información, independientemente al formato de ésta, incluyendo documentos en papel, propiedad digital e intelectual, y las comunicaciones verbales o visuales.

s) **Factor de autenticación:** Información utilizada para verificar la identidad de un servicio o una persona.

t) **Gobierno de la seguridad de la información:** Conjunto de responsabilidades y prácticas que tienen la finalidad de brindar dirección estratégica y garantizar que se logren los objetivos corporativos relacionados con la seguridad de la información, gestionándolo conforme a estándares internacionales, de acuerdo con la naturaleza, tamaño, perfil de riesgo de las entidades y volumen de sus operaciones y verificando que los recursos de la empresa se empleen con responsabilidad para estos fines.

u) **Hardware:** Conjunto de todos los componentes físicos y tangibles de un computador o equipo electrónico.

v) **ISAE (Información de Seguridad para la Administración de Eventos) o SIEM por sus siglas en inglés**: Sistema de información que proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones, dispositivos de seguridad y los elementos de red, como por ejemplo sistemas de centralización de registros de eventos del sistema operativo;

w) **Incidente de seguridad de la información:** Suceso o serie de sucesos inesperados, que tienen una probabilidad significativa de comprometer las operaciones de PCR, amenazar la seguridad de su información y/o de sus recursos tecnológicos.

x) **Internet:** Red de redes de alcance mundial que opera bajo estándares y protocolos internacionales;

y) **Intranet:** Red interna de computadoras que haciendo uso de tecnología de Internet, permite compartir información o programas;

z) **Infraestructura de tecnología de la información:** Es el conjunto de hardware, software, redes de comunicación, multimedia y otros, así como el sitio y ambiente que los soporta, que es establecido para el procesamiento de las aplicaciones;

aa) Medios de acceso a la información: Son equipos servidores, computadores personales, teléfonos inteligentes, terminales tipo cajero automático, las redes de comunicación, Intranet, Internet y telefonía;

bb) Plan de Continuidad del Negocio (*BCP: Business Continuity Plan*): Documento que contempla la logística que debe seguir la entidad supervisada a objeto de restaurar los servicios y aplicaciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado, después de una interrupción o desastre.

cc) Principio de menor privilegio: Establece que cada programa y cada usuario del sistema de información debe operar utilizando los privilegios estrictamente necesarios para completar el trabajo.

dd) Proceso crítico: Proceso o sistema de información que al dejar de funcionar, afecta la continuidad operativa de PCR.

ee) Procesamiento de datos o ejecución de sistemas en lugar externo: Procesos informáticos que soportan las operaciones administrativas y de negocio de PCR, que incluyen: el procesamiento de tarjetas electrónicas, servicios de pago móvil, custodia electrónica de valores desmaterializados en Entidades de Depósito de Valores, alojamiento de sitios web o de correo electrónico institucional en servidores administrados externamente, el hospedaje físico de servidores utilizados por la entidad en ambientes ajenos y otros procesos similares.

ff) Programa de Seguridad de la Información: Conjunto de planes implementados para preservar y mejorar continuamente la seguridad de la información, sobre la base de los requerimientos del negocio y el análisis de riesgos.

gg) Propietario de la información: Es el responsable formalmente designado para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

hh) Pruebas de intrusión: Son pruebas controladas que permiten identificar posibles debilidades de los recursos tecnológicos de PCR, que un intruso podría llegar a explotar para obtener el control de sus sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores y/o dispositivos de red. Las pruebas de intrusión pueden ser realizadas a través de la red interna, desde Internet, accesos remotos o cualquier otro medio.

ii) Resiliencia: es la capacidad de un mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que pudo estar sometido.

jj) Respaldo o copias de seguridad (backup): Copia de información almacenada en un medio digital, que se genera en forma periódica, con el propósito de utilizar dicha información, en casos de emergencia o contingencia.

kk) Seguridad de la Información (SI): Conjunto de medidas y recursos destinados a resguardar y proteger la información, buscando mantener la confidencialidad, confiabilidad, disponibilidad e integridad de la misma.

ll) Seguridad física: aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los activos de información e información de la entidad.

mm) **Seguridad lógica**: aplicación de barreras y procedimientos que resguarden el acceso a la información y solo se permita acceder a ellos a las personas o servicios autorizadas para hacerlo, quedando evidencia de ello;

nn) **Sistema de información:** Conjunto organizado e interrelacionado de procedimientos de recopilación, procesamiento, transmisión y difusión de información que interactúan entre sí para lograr un objetivo.

oo) **Sitio externo de resguardo:** Ambiente externo al Centro de Procesamiento de Datos, donde se almacenan todos los medios de respaldo, documentación y otros recursos de tecnología de información catalogados como críticos, necesarios para soportar los planes de continuidad del negocio y contingencias tecnológicas.

pp) **Software**: Equipamiento o soporte lógico de un sistema de información que comprende el conjunto de los componentes lógicos que hacen posible la realización de tareas específicas. El software incluye: software de sistema, software de programación y software de aplicación.

qq) **Transferencia electrónica de información**: Forma de enviar y/o recibir en forma electrónica, datos, información, archivos y mensajes, entre otros.

rr) **Tecnología de la Información (TI)**: Conjunto de procesos y productos derivados de herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión de la información.

ss) **Tercerización de actividades, operaciones o procesos de tecnologías de la información**: Se produce cuando PCR encarga la realización de actividades, operaciones o procesos de tecnologías de la información, relacionados a servicios o productos financieros de la entidad, a un tercero, es decir, a una persona natural o jurídica distinta a la entidad.

tt) **Unidad de Ciberseguridad (UCIB)**: Unidad encargada de monitorear, evaluar y defender los sistemas de información de la entidad como por ejemplo sitios web, aplicaciones, bases de datos, centros de datos principales o alternos, servidores, redes, escritorios, dispositivos, entre otros.

uu) **Usuario del sistema de información**: Persona identificada, autenticada y autorizada para utilizar un sistema de información. Ésta puede ser funcionario de PCR (Usuario Interno del sistema de información) o cliente (Usuario Externo del sistema de información).

vv) **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado o utilizado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.

8. PLAN ESTRATÉGICO DE TI

Se debe desarrollar un Plan Estratégico de Tecnologías de la Información (TI) que esté alineado con la estrategia institucional, y que considere la naturaleza, tamaño y complejidad de las operaciones de PCR, sus procesos, estructura y análisis y evaluación de riesgos de SI.

9. ESTRATEGIAS Y RECURSOS QUE COMPONEN AL SGSI

PCR utiliza las siguientes estrategias y recursos para gestionar la seguridad de la información:

1era. Línea de Defensa

- **Usuarios**

Todo el personal firma un Contrato de Trabajo y Acuerdo de Confidencialidad que señala su obligación de proteger y no divulgar la información que genera y administra 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.

- **Jefe de Tecnología de la Información**

Es la instancia responsable de asignar los usuarios y contraseñas al personal nuevo y dar de baja al personal desvinculado, en el marco de los niveles de acceso autorizados para cada perfil de usuario.

2da. Línea de Defensa

- **Oficial de Gestión Integral de Riesgos**

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.

- **Proveedor del servicio de Ethical Hacking**

Instancia cuyo servicio es contratado para realizar las pruebas de intrusión internas y externas a las plataformas que maneja PCR, permitiendo identificar las vulnerabilidades técnicas de la compañía.

- **Comité de Gestión Integral de Riesgos**

Instancia responsable de monitorear y evaluar periódicamente el cumplimiento de la presente Política.

3ra. Línea de Defensa

- **Auditoría Interna**

Instancia que debe verificar la efectividad de las acciones adoptadas por la primera y segunda línea de defensa para el logro de los objetivos del SGSI.

10. ALCANCE DEL SGSI

PCR debe establecer los controles necesarios para el resguardo **de toda la información que genera y administra**, acorde con los niveles de criticidad de cada activo clasificado en el **Inventario de Activos de la Información**. Entre los controles citados se debe considerar como mínimo, a aquellos implementados en aplicaciones informáticas para la gestión de accesos, así como a aquellos que permitan monitorear actividades sospechosas o no autorizadas por la presente Política, contando para esto, adecuados registros/pistas de auditoría.

11. ANÁLISIS Y EVALUACIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

El Oficial de Gestión Integral de Riesgos debe realizar un análisis y evaluación de riesgos en seguridad de la información, acorde a la naturaleza, tamaño y complejidad de operaciones de PCR, debiendo aplicar las metodologías aprobadas por el Directorio o Junta Directiva para el efecto.

El resultado obtenido del análisis efectuado debe estar contenido en un informe dirigido al Comité de Gestión Integral de Riesgos, constituyéndose esto en un proceso continuo, por lo cual debe realizarse al menos una (1) vez al año.

12. ACUERDOS DE CONFIDENCIALIDAD

Como parte de las obligaciones contractuales de los Directores, Ejecutivos, demás funcionarios, consultores y personal eventual, éstos deben aceptar y firmar los términos y condiciones del contrato de empleo en el cual se establecerán sus obligaciones en cuanto a la seguridad de la información, entre las que se debe incluir el mantenimiento de la confidencialidad de la información a la que tengan acceso, inclusive después de la finalización de la relación contractual.

13. INVENTARIO DE ACTIVOS DE INFORMACIÓN

PCR debe contar con un inventario actualizado de sus activos de información, clasificados de acuerdo a su nivel de criticidad (alto, medio o bajo) y sensibilidad (confidencial, de uso interno, público) a fin de permitir una adecuada asignación de derechos de acceso, propietarios de la información y de responsabilidades para su protección.

Adicionalmente, se debe actualizar hasta el 31 de marzo de cada año el detalle del software que utiliza PCR con corte al cierre de la gestión anterior, de acuerdo al formato contenido en el **Anexo 1: Inventario de Software**.

14. MANEJO DE INFORMACIÓN CONFIDENCIAL

- PCR debe clasificar debidamente sus activos de la información a fin de definir los controles que aplicará para proteger la documentación (física o digital) que sea catalogada como *confidencial*.
- Todos los colaboradores firman un acuerdo de confidencialidad al momento de su ingreso. Dicho acuerdo demuestra las obligaciones pactadas y las penalidades por incumplimiento referente al tratamiento de la información confidencial.
- Todos los colaboradores son responsables de reportar cualquier incidente de seguridad de la información tan pronto como sea posible, al área de Tecnología de la Información y al Director de Cumplimiento (Gestión Integral de Riesgos).
- Todo propietario de algún activo de la información *confidencial,* es responsable de solicitar al Área de IT la implementación de los controles que, a su criterio, sean necesarios para proteger y resguardar la misma de personas no autorizadas, pudiendo aplicar desde la asignación/restricción de accesos a sitios, bibliotecas o documentos específicos de la Intranet, hasta el establecimiento de contraseñas en archivos o el cifrado de los mismos, cuando lo considere necesario.

- El personal de Análisis de PCR sólo puede tener acceso a la información de los clientes que pertenecen a su cartera asignada. A fin de que esto se cumpla, el Director de Análisis debe gestionar o solicitar la correcta asignación de los accesos de todo el personal de su área bajo el *principio de menor privilegio*.
- La información que genera y administra PCR se debe almacenar en los equipos de cómputo dentro de las cuentas individuales de OneDrive Pacific Credit Rating, de manera que tengan su réplica respectiva en la nube, lo que se constituye en las copias de respaldo de la información, actualizadas y sincronizadas en tiempo real.
- **Escritorios Limpios:** Los Empleados de PCR no deben dejar a la vista de personas no autorizadas ningún documento o papel de trabajo de tipo confidencial.
- El personal de PCR que NO pertenezca al área de Análisis no debe, bajo ninguna circunstancia, acceder a información de clientes de la entidad, salvo autorización expresa del Director de Análisis o la Alta Dirección y con la debida justificación y solicitud por escrito.
- Las metodologías, plantillas y otras herramientas que conforman el *know-how* de PCR debe ser debidamente custodiada y resguardada por el Coordinador de Metodologías, según las directrices establecidas por el Director de Análisis.
- Todo el personal de PCR tiene prohibido enviar o recibir información confidencial a través de canales que NO estén autorizados por Presidencia. En tal sentido, el acceso a dichos canales debe ser restringido por la Unidad de IT para prevenir su uso en los computadores de todo el personal del Grupo.
- **Está terminantemente prohibido que cualquier empleado de PCR divulgue información privilegiada de algún cliente o de la misma Calificadora/Clasificadora, ya sea de manera verbal, escrita o mediante algún medio audiovisual, antes de que dicha información se haga pública por los medios legales y normativos.**
- **Asimismo, ningún empleado de PCR tiene permitido revelar datos ni información confidencial de los clientes de la entidad a personas no autorizadas (externas o no al Grupo PCR), ya sea de forma verbal, escrita o mediante algún medio audiovisual.**
- Los Empleados de PCR no deben involucrarse en la compra o venta de valores de ninguno de los clientes de la Clasificadora, por el riesgo de conflicto de interés y de fuga de información que esto podría representar para la entidad.
    - El personal de la calificadora debe evitar utilizar la información confidencial para participar o influir de otro modo en la determinación de una calificación crediticia si tiene una relación inmediata (es decir, un cónyuge, pareja, padre, hijo o hermano) que actualmente trabaja para la entidad calificada.
- PCR no debe participar en el proceso de alguna calificación crediticia, si cualquier persona de la calificadora, un miembro cercano a su familia o una empresa a la que esté vinculada directa o indirectamente cumple con alguna de las siguientes condiciones:
    - Mantiene u opera un instrumento de negociación emitido por la entidad o deudor calificado.

- Mantiene u opera un instrumento de negociación, que no sea de un fondo de inversión, que contenga un interés en la entidad o deudor calificado, o sea un derivado basado en un instrumento de negociación emitido por esta misma entidad.
- Mantiene u opera un instrumento de negociación emitido por un afiliado de la entidad, deudor calificado o estructurador de la obligación calificada cuya propiedad pueda causar un conflicto de interés.
- Posee información confidencial o material no abierto al público sobre un instrumento de negociación, en cuyo caso debe evitar participar en una operación en el instrumento de negociación o de usar la información confidencial para aconsejar o darle ventaja a una persona involucrada en la transacción de dicho instrumento.

- Los Analistas son responsables de custodiar y resguardar la información recibida de los clientes de PCR (archivos, correos electrónicos, documentos, etc.), así como los documentos producidos internamente (metodologías, plantillas, informes, comunicaciones, etc.).
- En PCR los colaboradores deben recibir entrenamiento formal y continuo al menos una (1) vez al año sobre el cumplimiento de esta Política. Los temas cubiertos en la capacitación deben ser pertinente a las responsabilidades del colaborador y cubrir, mientras sea aplicable, las metodologías de calificación crediticia, las leyes que gobiernan las actividades de dicha calificación; las políticas aplicadas al mantenimiento y operación de instrumentos de negociación y las políticas y procedimientos destinados al manejo de información confidencial o material.
- Los controles que asegurarán el adecuado manejo de la información confidencial deben detallarse en un ***Protocolo de Seguridad de la Información*** para conocimiento de todo el personal de PCR y su consiguiente cumplimiento obligatorio.
- El Auditor Interno y el Director de Cumplimiento, deben verificar el cumplimiento de las políticas aplicadas al mantenimiento y a la operación de instrumentos de negociación, así como de las políticas establecidas en esta sección para el manejo de la información confidencial.

15. ANÁLISIS DE VULNERABILIDADES TÉCNICAS

La evaluación de vulnerabilidades técnicas debe efectuarse por lo menos una (1) vez por año y/o ante un cambio significativo en la infraestructura tecnológica.

La ejecución de pruebas de seguridad debe considerar la realización de pruebas de intrusión controladas internas y externas.

PCR debe exigir a las empresas y/o personas que le presten servicios de evaluación de seguridad de la información, la respectiva documentación que acredite la experiencia necesaria para realizar este tipo de trabajos. Adicionalmente, se debe garantizar que el personal que realice las pruebas de intrusión controladas sea certificado y firme un acuerdo de confidencialidad conforme se establece en la presente Política.

15.1 Mecanismos de Control y Mitigación

- Las vulnerabilidades técnicas identificadas deben contar con plazos oportunos para su tratamiento, de acuerdo al nivel de riesgo que representen, priorizando aquellas que impliquen un alto nivel de exposición.
- En ese sentido, cuando una vulnerabilidad represente un alto nivel de riesgo para PCR, el plan de acción propuesto debe tener un plazo máximo de 90 días para su implementación.
- En los casos que amerite, se debe considerar el establecimiento de parches de seguridad en los sistemas de información de PCR, evaluando el riesgo de instalar el parche versus el riesgo que representa la vulnerabilidad.
- Adicionalmente, se puede considerar los siguientes controles:
    - Desconectar o deshabilitar los servicios o capacidades relacionados con la vulnerabilidad
    - Adaptar o agregar controles de acceso, disminuir privilegios
    - Aumentar la frecuencia del monitoreo para detectar o evitar ataques reales.

16. DESTRUCCIÓN CONTROLADA DE MEDIOS DE RESPALDO

Para realizar la destrucción de medios de almacenamiento de respaldo, se debe contar con autorización expresa de Presidencia, debiendo participar como mínimo, en el acto de eliminación de las copias, el Gerente/Coordinador País, el Auditor Interno y el Jefe de Tecnología de la Información.

17. PROCESO DISCIPLINARIO

Todo Director, Ejecutivo, colaborador, consultor y/o personal eventual de PCR que cometa un incumplimiento a la presente Política, estará sujeto al siguiente proceso disciplinario:

- Verificación de la ocurrencia del incumplimiento, por parte del Auditor Interno (recolección de evidencia).
- Revisión por parte del Asesor Legal, para estimar la gravedad del incumplimiento.
- Revisión de los hallazgos del Auditor Interno y del Asesor Legal en el **Comité de Gestión Integral de Riesgos**, contemplando los siguientes tipos de sanción disciplinaria según establece el ***Reglamento Interno de Trabajo***, para faltas leves o graves, sujeto a un análisis del caso y de los antecedentes del funcionario:

  Para Directores, Ejecutivos, colaboradores y personal eventual:

    - Amonestación escrita con copia al legajo personal.
    - Despido o rescisión de contrato, de acuerdo con las normas legales.

  Para Consultores:

    - Sanción monetaria proporcional al impacto ocasionado por el incumplimiento, y según contrato.
    - En casos serios de dolo, se analizará el inicio de acciones judiciales.

18. ACTUALIZACIONES DE SOFTWARE

Todo Director, Ejecutivo, colaborador y personal eventual que haga uso de los equipos de cómputo de PCR debe velar por la debida ejecución de los procesos de actualización de sus sistemas operativos y aplicaciones. El Jefe de Tecnología de la Información se encargará de hacer seguimiento semestral a los equipos de cómputo verificando que se encuentren actualizados según corresponda y elevará un reporte comunicando el cumplimiento o no de las actualizaciones al Oficial de Gestión Integral de Riesgos.

19. DEVOLUCIÓN DE INFORMACIÓN EN CASO DE DESVINCULACIÓN

Todo colaborador que termine su relación laboral con PCR (ya sea por renuncia voluntaria o por despido), tiene la obligación de devolver en su integridad, toda la información que tuvo bajo su custodia durante el desarrollo de sus funciones, acompañada de un Inventario según formato del **Anexo 2: Devolución de Información en Custodia**.

Dicho Inventario debe contar con la firma de entrega por parte del colaborador y con la firma de recepción por parte del funcionario designado para recibir dicha documentación.

Así mismo, el Jefe de Tecnología de la Información realizará copias de seguridad (backup) de toda la información del equipo de cómputo y el OneDrive en un tiempo no mayor a 48 horas del ex funcionario de PCR.

20. ADMINISTRACIÓN DE CUENTAS DE USUARIOS

- Se debe desarrollar perfiles de acceso para los usuarios que accederán a los sistemas de información y redes de datos de PCR.
- Se debe llevar un control y monitoreo de la correcta asignación de perfiles de acceso a los usuarios.
- La creación, modificación o eliminación de cuentas de usuarios de los sistemas de información, debe contar con la autorización de la instancia correspondiente.
- La gestión de perfiles de acceso se debe realizar de acuerdo con el principio de menor privilegio.

21. ADMINISTRACIÓN DE PRIVILEGIOS

- Se debe restringir y controlar el uso y asignación de privilegios para las cuentas de usuario y de administración de los sistemas de información, aplicaciones, sistemas operativos, bases de datos, Intranet e Internet.
- Cuando un usuario cambie de cargo/puesto dentro de la organización, se debe reasignar sus niveles de acceso y privilegios de acuerdo con el perfil asignado para ese fin.
- Se debe remover de manera inmediata los derechos de acceso de aquellos usuarios que ya no trabajen en la compañía.

22. ADMINISTRACIÓN DE CONTRASEÑAS

- Es responsabilidad de cada colaborador mantener sus contraseñas confidenciales, lo que implica **no compartirlas con ningún otro empleado de PCR, y mucho menos con un externo a la entidad.**

- Los computadores de los usuarios deben estar apagados o protegidos mediante bloqueo de teclado controlado por una contraseña, cuando no estén siendo utilizados.

23. REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Se debe capacitar al personal para que realice un adecuado reporte de los incidentes de seguridad de la información que puedan suscitarse en PCR. A continuación, se expone, con carácter enunciativo mas no limitativo, una lista de tipos de incidentes que los colaboradores de PCR deben reportar al área de TI y al área de Gestión Integral de Riesgos, en caso de su materialización:

- Pérdida de servicio;
- Pérdida de equipo o instalaciones;
- Sobrecargo o malfuncionamiento del sistema;
- Errores humanos;
- Incumplimiento de políticas o procedimientos;
- Deficiencias de controles de seguridad física;
- Cambios incontrolables en el sistema;
- Mal funcionamiento del software;
- Mal funcionamiento del hardware;
- Violación de accesos;
- Código malicioso;
- Negación de servicio;
- Errores resultantes de datos incompletos o no actualizados;
- Violaciones en la confidencialidad e integridad de la información;
- Mal uso de los sistemas de información;
- Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos;
- Intentos recurrentes y no recurrentes de acceso no autorizado.
- **Cualquier sospecha de ciberataque.**

Todo colaborador, proveedor o consultor externo debe conocer el procedimiento para reportar los incidentes que podrían causar algún impacto negativo en la seguridad de los activos de información de PCR.

24. EVALUACIÓN Y SELECCIÓN DE PROVEEDORES DE SERVICIOS RELACIONADOS CON TI

Se debe analizar y determinar el nivel de riesgo que representa un proveedor de servicios para PCR previo a su contratación, y, en función a los resultados de dicho análisis, se debe establecer los controles/mitigantes necesarios que se aplicará desde el inicio hasta la finalización del contrato.

Todo contrato a suscribir con los proveedores de PCR (*Acuerdo de Nivel de Servicio – SLA*), debe contemplar mínimamente las cláusulas sobre el tipo de servicio que se otorgará, sobre el soporte y

asistencia que el proveedor pondrá a disposición de PCR, sobre la seguridad de los datos a los que se compromete el proveedor, las garantías y tiempos de respuesta del servicio del mismo (planes de contingencia / continuidad), la disponibilidad del servicio, y las multas que se aplicará en caso de incumplimiento.

Cada Gerente/Coordinador País debe velar por que se mantenga un registro actualizado de información sobre todas las subcontrataciones realizadas, considerando como mínimo:

a) El nombre del proveedor

b) La descripción del servicio prestado a PCR

c) Fecha de inicio y de finalización de la relación contractual con PCR

d) Seguimiento y descripción de las modificaciones o adendas realizadas al contrato suscrito con el proveedor

25. CONTROLES CRIPTOGRÁFICOS

- La información catalogada como crítica y confidencial de PCR debe contar con los controles necesarios para su protección, tomando en cuenta la opción de cifrado de la información cuando sea pertinente, y a criterio del Propietario de la Información.
- Deberá utilizarse la opción de firma electrónica para la información de carácter legal, cuando sea imprescindible garantizar la autenticidad y el no repudio de dicha información.
- Se debe garantizar la seguridad de la información en sitios web propios de PCR que almacenen o transmitan información confidencial, a través del uso de certificados para la navegación web, cuando corresponda.

25.1 Cifrado de datos confidenciales cuando se contrata servicios externos

- Si se requiere contratar servicios externos en los que sea necesario el tratamiento de datos confidenciales, se verificará que las transferencias de datos sean seguras, ya sea cifrando los datos antes de transferirlos o bien utilizando canales seguros.

25.2 Cifrado de datos confidenciales cuando se solicita el desarrollo de aplicaciones

- Si se requiere contratar el desarrollo de un aplicativo web o una app para dispositivos móviles que ofrezca acceso a información clasificada como confidencial, la información debe almacenarse cifrada; asimismo todos los desarrolladores que contemplen el tratamiento de datos personales o protegidos por ley deben contemplar criterios de privacidad por defecto y por diseño.
- Se debe cifrar las credenciales de acceso y la información confidencial cuando se soliciten desarrollos web o apps que impliquen almacenamiento, envío o recepción de información confidencial.

25.3 Uso de protocolos seguros de comunicación

- Se debe implementar protocolos seguros para acceder a los servicios de PCR, tanto si éstos están en instalaciones propias, como si están en algún proveedor externo (nube).

26. MIGRACIÓN DE SISTEMAS DE INFORMACIÓN

Los siguientes principios deben aplicarse en caso de que PCR se someta a la migración de sus sistemas de información:

- Se debe establecer planes de acción para el proceso de migración, y procedimientos específicos que garanticen la disponibilidad, integridad y confidencialidad de la información.
- El Gerente / Coordinador País es responsable de designar a la instancia que realizará el control de calidad durante el proceso de migración, el cual debe estar debidamente documentado y a disposición de los entes reguladores.
- El Auditor Interno de PCR debe evaluar y registrar los resultados obtenidos del proceso de migración, respaldado mediante Informe.

27. ADMINISTRACIÓN DE BASES DE DATOS

Se debe cumplir con los siguientes principios mínimos para la administración de las bases de datos de PCR:

- Arquitectura definida, para organizar y aprovechar de la mejor forma los sistemas de información
- Establecimiento de controles de acceso (contraseñas), cuando se trate de bases de datos confidenciales.
- Respaldo de las actividades de administración (cambios, modificaciones, depuraciones), de las bases de datos, sujetas a autorización por los propietarios de la información, según inventario de activos de la información.
- Realización de revisiones sobre la capacidad y desempeño de las bases de datos, que permitan determinar las necesidades de expansión de capacidades y/o la afinación en forma oportuna.

28. RESPALDOS O COPIAS DE SEGURIDAD

El Jefe de Tecnología de la Información debe monitorear que todos los colaboradores tengan cargada su información en la nube para la debida realización de copias de seguridad (backup) cuando sea requerido, cumpliendo con los siguientes principios mínimamente:

- La información respaldada debe poseer un nivel adecuado de protección lógica, física y ambiental, en función a su nivel de criticidad.
- Se debe realizar revisiones periódicas, a fin de garantizar la confiabilidad de las copias de seguridad con relación a su eventual uso en casos de emergencia. Dichas pruebas deben ser documentadas y efectuadas en los periodos definidos por el Oficial de Gestión Integral de Riesgos.
- El sitio externo de respaldo donde se almacenan las copias de seguridad debe mantener al menos diez (10) años la información crítica de la empresa.
- El ambiente físico destinado al resguardo de la información crítica debe contar con condiciones físicas y ambientales suficientes para garantizar mínimamente la protección contra daños, deterioro y hurto.

- Los custodios de la información deben mantener, a disposición del Oficial de Gestión Integral de Riesgos, un repositorio de las copias de respaldo que la información altamente crítica, donde se pueda identificar el nombre del usuario y fecha de la última copia de respaldo, y la cantidad de información respaldada, en especial cuando se trate de información de usuarios que sean ex empleados de la entidad.

29. CONFIGURACIÓN DE SOFTWARE Y HARDWARE

Se debe contar con un registro formal que contenga toda la información referente a los elementos de configuración del hardware, software, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas de información, por perfil de usuario, considerando lo siguiente:

- Procedimientos para identificar, registrar y actualizar los elementos de configuración existentes en el repositorio de configuraciones.
- Se debe revisar mínimamente una (1) vez al año, la existencia de cualquier software de uso personal o no autorizado, que no se encuentre incluido en los acuerdos de licenciamiento vigentes de PCR.

30. CAPACITACIÓNES

30.1 Capacitaciones sobre Riesgos y Amenazas de Seguridad de la Información

Todos los Directores, Ejecutivos, funcionarios, consultores y personal eventual deben ser capacitados al menos una vez al año sobre la gestión de riesgos de seguridad de la información, y sobre el debido reporte de incidentes de seguridad que se susciten en el desarrollo de sus funciones.

30.2 Capacitación sobre la presente Política

Todos los Directores, Ejecutivos, funcionarios y personal eventual deben ser capacitados al menos una vez al año para aplicar y cumplir con los lineamientos expuestos en la presente Política en el desarrollo normal de su trabajo.

ANEXO 1. INVENTARIO DE SOFTWARE

Nombre:
Fecha de Corte: 31/12/AAAA

Nombre[1]	Objeto[2]	Versión	Tipo de Procesamiento o Ejecución[3]	Fecha de Puesta en Producción	Fecha de la Última Actualización	Empresa Proveedora*		Soporte Vigente[4]
						Nombre	Regulada por ASFI [4]	

[1] Se debe incluir el detalle de todo el software que utiliza la entidad.
[2] Explicación resumida de la finalidad del software
[3] Interno, Externo o No Aplica
[4] Sí o No
[*] Si el tipo de procesamiento o ejecución es externo

Responsable del Área de TI

Gerente General

ANEXO 2: DEVOLUCIÓN DE INFORMACIÓN EN CUSTODIA

Acta de Devolución de Información en Custodia

Yo **xxxxxxx** con número de identificación DNI **XXXXX** declaro que en fecha **21/10/2024** he realizado la devolución de la siguiente información que estuvo bajo mi custodia durante el desarrollo de mis funciones como **xxxxxx**;

Activo de Información	Título / Marca / Versión	Formato	Ubicación Electrónica o Física (ingresar dirección URL o detallar la ubicación física del activo)
Información de PCR PA, durante la gestión 2024: - ABC - XYZ - ... etc.	(Varios documentos)	Digital-Word	Carpeta(s) ubicadas en: (Ingresar link)
Laptop de 15 pulgadas	DELL Vostro 14 3000, Modelo XXXXXX, con Número de Serie 184793284928	Hardware	
Documentación de los clientes: - ABC - XYZ - ... etc.	**(Varios documentos)**	Físico	
Documentación de los clientes: - ABC - XYZ - ... etc.	**(Varios documentos)**	Digital – archivos PDF, Word, Excel.	

Entregué conforme
Nombre Funcionario
Cargo Funcionario

Recibí Conforme
Nombre Funcionario
Cargo Funcionario