ACUERDO MARCO PARA CAPTURA DE DATOS

1. Objetivos del Acuerdo Marco

El presente Acuerdo Marco establece estándares de responsabilidad y mecanismos de captura de datos de clientes de las instituciones que adhieran a este Acuerdo Marco de manera controlada vía *web scraping*, como marco de acción mientras se establecen otros mecanismos de captura, y sin perjuicio de los cambios normativos que se aprueben en el futuro.

Para efectos de este Acuerdo Marco, *web scraping* significa el uso de los protocolos de comunicación y seguridad de la web (http y tls) para hacer captura de datos -con el previo consentimiento de los usuarios- de tal forma que los resultados sean entregados a una aplicación o sistema computacional.

El presente instrumento constituye un Acuerdo Marco al que podrán adherir las entidades bancarias y las entidades que formulan consultas a través de los mecanismos y condiciones indicados en este Acuerdo. El Acuerdo Marco debe ser complementado por contratos bilaterales que deberán acordar las instituciones participantes a que se refiere el numeral siguiente (los "**Acuerdos Bilaterales**"). En lo no establecido en dichos contratos bilaterales se entenderá que rigen las condiciones establecidas en el presente Acuerdo Marco.

2. Entidades participantes

Las entidades participantes del presente Acuerdo Marco son las empresas bancarias miembros de la Asociación de Bancos e Instituciones Financieras de Chile A.G. y Banco Estado (en adelante, los "**Bancos**"), y las empresas asociadas a la Asociación de Empresas de Innovación Financiera de Chile A.G. (en adelante, las "**Fintech**"), que hayan adherido al presente Acuerdo Marco registrando su firma en el Anexo 1.

El presente Acuerdo Marco distingue el rol de aquellas entidades signatarias – sean Bancos o Fintech- que, directa o indirectamente, realicen consultas de datos de clientes sobre portales de instituciones bancarias (individualmente "**Institución que Consulta**", o de manera colectiva "**Instituciones que Consultan**"), y el rol de los Bancos que hayan adherido al presente Acuerdo Marco, cuyas plataformas y portales son consultadas por las Entidades que Consultan, para obtener información de clientes que han dado su consentimiento (individualmente, "**Institución que Provee**", o de manera colectiva, "**Instituciones que Proveen**").

En caso de que las Instituciones que Proveen o las Instituciones que Consultan brinden su servicio encargando parte o todo el proceso objeto de este acuerdo a terceras partes, ello no las eximirá de su responsabilidad en caso de incumplimiento. A su vez, las Instituciones que

Proveen o las Instituciones que Consultan deberán exigir a estas terceras partes que adhieran a los lineamientos y mecanismos aquí indicados.

Cada parte del Acuerdo Marco deberá informar inmediatamente a la otra parte, cualquier cambio en las entidades adherentes al presente documento.

3. Estándares de las Instituciones que Consultan.

Las Instituciones que Consultan - sea directamente o a través de terceros - deberán cumplir con las siguientes obligaciones:

3.1. Estándares de Uso

3.1.1. Consentimiento del Cliente

Es responsabilidad de las Instituciones que Consultan contar con la autorización explícita de sus clientes para el acceso, uso, almacenamiento y tratamiento de la información que se obtenga a través de la captura de datos vía *web scraping*. Dicha autorización deberá señalar de manera explícita la finalidad del tratamiento de los datos, acotando el acceso, uso, almacenamiento y tratamiento sólo a aquellos datos estrictamente necesarios para cumplir el fin declarado.

Dicha autorización deberá referirse expresamente a los siguientes aspectos, que el cliente declara conocer y aceptar, de acuerdo con lo dispuesto en la Ley 19.628 y sus modificaciones:

i) los datos personales y financieros que el cliente autoriza compartir, especificando, cuando corresponda, el plazo de vigencia de dicha autorización;
ii) la finalidad o uso que la Institución que Consulta dará a dicha información; y
iii) el periodo de tiempo en que dichos datos serán almacenados por la Institución que Consulta.

Tratándose de información sujeta a secreto o reserva bancaria, la Institución que Consulta deberá proporcionar a la Institución que Provee los antecedentes donde conste que ha sido expresamente autorizada para requerir la información que corresponda.

3.1.2. Acceso a la información

Las Instituciones que Consultan deberán proporcionar a las Instituciones que Proveen, en la forma definida en los respectivos Acuerdos Bilaterales, la identificación exacta de las actividades de consulta que realizan, de manera que las Instituciones que Proveen puedan gestionar su infraestructura de ciberseguridad, y evitar bloqueos no deseados. Esta información debe contener al menos:

i) Pool de direcciones IP utilizadas (IPv4 e IPv6), ASN utilizados y países utilizados asociados al direccionamiento IP (georeferencia). En algunos casos se podrá acordar otros mecanismos, como cookies firmadas u otros en forma alternativa.

ii) URLs y/o *Path* invocados de la Institución que Provee; especificando métodos HTTP utilizados por los procesos de consulta (por ejemplo: *GET/POST*); host y/o sitios de la Institución que Provee asociados a los procesos de consulta que invoca la Institución que Consulta, con el mayor detalle que sea posible entregar para cada Institución que Provee.

iii) URLs o nombre de las aplicaciones de la Institución que Consulta utilizadas en las conexiones al portal o plataforma de la Institución que Provee.

iv) Volumetría estimada (*request*/seg) de los procesos de consulta hacia la Institución que Provee.

v) Establecer conexiones seguras hacia las Instituciones que Proveen, mediante cifrado de *request* (*payload*) y conexión bajo protocolo TLS (TLSv1.3).

Adicionalmente, las Instituciones que Consultan deberán acordar con las Instituciones que Proveen, en la forma definida en los respectivos Acuerdos Bilaterales, los siguientes aspectos técnicos:

i) *User-Agent* utilizados en las conexiones.
ii) Una o más ventanas horarias de ejecución.
iii) Volumen máximo de tráfico y cantidad de conexiones concurrentes o simultáneas generadas por la Institución que Consulta.

En relación con los puntos ii) y iii) anterior, en caso de identificarse un tráfico mayor al proyectado, la Institución que Provee podrá limitar los *request* y/o peticiones hasta que se regularice el tráfico previamente acordado. Sin perjuicio de lo anterior, la Institución que Consulta deberá notificar a la Institución que Provee si el aumento de tráfico verificado se mantendrá en el tiempo, en cuyo caso las partes evaluarán la adecuación a los parámetros necesarios para este nuevo tráfico.

Los parámetros establecidos en los puntos ii) y iii) anterior, no aplican para consultas que se originen por solicitudes realizadas por el cliente en línea.

3.1.3. Uso, almacenamiento y tratamiento de la información

Las Instituciones que Consultan usarán los datos que reciban exclusivamente para los fines conocidos, aceptados y autorizados por los clientes. Los acuerdos y en general las relaciones entre clientes e Instituciones que Consultan y los derechos y obligaciones que se generen, serán de exclusiva responsabilidad y cargo de dichas partes, sin responsabilidad alguna de las Instituciones que Proveen.

Las Instituciones que Consultan deberán contar con mecanismos de validación que inhiban la suplantación de la identidad de los clientes de las Instituciones que Proveen, al momento que

dichos clientes otorguen su consentimiento para el acceso, uso, tratamiento y almacenamiento de la información.

Las Instituciones que Consultan deberán contar con procesos y mecanismos de protección de la información confidencial de los clientes, tales como credenciales, datos personales y financieros almacenados o procesados, asegurando que se cumplan con las mejores prácticas internacionales en términos de encriptación y administración segura de llaves criptográficas para datos en tránsito y reposo.

Las Instituciones que Consultan no podrán almacenar información del cliente que no estén activos conforme a los términos y condiciones acordados por el cliente con la Institución que Consulta, o si el cliente renuncia al servicio prestado.

Sin perjuicio de lo anterior, las Instituciones que Consultan no podrán almacenar las credenciales del cliente con las que ingresan a las plataformas de las Instituciones que Proveen, si el cliente renuncia al servicio prestado, no se encuentra activo en la Institución que Consulta, o por un periodo mayor al definido por la Institución que Provee en el respectivo acuerdo bilateral, lo que ocurra primero.

3.1.4. Datos a ser consultados

Las Instituciones que Consultan pueden acceder a los datos de conformidad con la legislación aplicable, respecto de los cuales el cliente haya dado su consentimiento expreso, conforme lo estipulado en el punto 3.1.1 anterior, y que corresponda a la información que se encuentre disponible en la plataforma de las Instituciones que Proveen. Será responsabilidad de las Instituciones que Consultan obtener dicho consentimiento.

El consentimiento del cliente deberá manifestarse en forma libre, informada, expresa, y específica en cuanto (i) al tipo de información financiera a la que pueden acceder las Instituciones que Consultan para que puedan proveer servicios a sus clientes basados en dicha información, (ii) la finalidad de la información y (iii) el período máximo de validez de la autorización.

El cliente podrá revocar en cualquier tiempo el consentimiento otorgado, momento a partir del cual, se prohíbe el acceso o tratamiento de la información, respecto de la cual se hubiese otorgado la autorización correspondiente.

Las Instituciones que Proveen podrán requerir a las Instituciones que Consultan los antecedentes que respalden el consentimiento del cliente donde conste (i) la autorización del cliente para acceder a los datos financieros, (ii) el tipo de información específica que puede ser capturada, (iii) la finalidad para la captura de los datos, y (iv) el período máximo de validez de la autorización.

Será responsabilidad de las Instituciones que Consultan ejecutar la captura de los datos que realicen desde las plataformas de las Instituciones que Proveen, en especial cuando se trate de datos personales, de conformidad con los siguientes principios:

1. Finalidad: la captura de los datos debe realizarse con fines específicos, explícitos y lícitos, los cuales deben ser parte integrante del consentimiento otorgado por el cliente.

2. Proporcionalidad: el acceso a los datos debe realizarse en consideración de aquellos que sean necesarios y pertinentes en relación con la finalidad del acceso a la información y por el tiempo que sea necesario para cumplir con dichas finalidades.

3. Calidad: Las Instituciones que Consultan deberán procurar que los datos capturados se mantengan vigentes y actualizados.

4. Seguridad: Las Instituciones que Consultan deberán aplicar las medidas de seguridad de la información indicadas en la sección 3.2 siguiente.

5. Transparencia: Las Instituciones que Consultan deberán mantener permanentemente accesibles sus políticas de tratamientos de datos de manera precisa, inequívoca y gratuita.

6**. Responsabilidad:** Las Instituciones que Consultan serán responsables en el acceso y tratamiento de la información de conformidad con la regulación aplicable.

7. Confidencialidad. Las partes deberán guardar secreto sobre los datos personales que tratan en conformidad con el artículo 7 de la Ley 19.628.

3.2. Estándares de seguridad

3.2.1. Gestión de seguridad

Las Instituciones que Consultan deberán implementar y gestionar una Política de Seguridad de la Información, que les permita gestionar su operación y toma de decisiones basadas en la administración de sus riesgos tecnológicos y de ciberseguridad, debiendo cumplir, al menos, con las disposiciones indicadas en el Capítulo 20-10 de la Recopilación Actualizada de Normas de la CMF. Para lo cual se establece una “línea base” de esta norma que deben cumplir todas las Instituciones así como también los controles que deberá evaluar cada Institución que Consulta de acuerdo con su “Gestión basada en Riesgo”, dependiendo del tamaño y naturaleza de la misma, todos ellos detallados en el “ANEXO 1 CONTROLES MÍNIMOS DE CIBERSEGURIDAD” de este Acuerdo Marco, que forma parte integrante del mismo.

Dicha política deberá considerar un modelo de Gestión de Incidentes de Seguridad y Ciberseguridad, como también establecer mecanismos y protocolos de intercambio de información con las Instituciones que Proveen sobre incidentes de ciberseguridad o situaciones que puedan afectar la continuidad operacional de la Institución que Provee.

Adicionalmente, las Instituciones que Consultan deberán implementar un modelo de información oportuna a las Instituciones que Proveen sobre cualquier evento anómalo (alerta o incidente), vulnerabilidades técnicas de categoría crítica o eventos de fraude identificados en la infraestructura de la Institución que Consulta, y que afecte la seguridad de la información de los clientes o de la Institución que Provee, en la forma que se establezca en los Acuerdos Bilaterales.

En los respectivos Acuerdos Bilaterales, se definirán los procedimientos que permitan a la Institución que Provee verificar el cumplimiento de la Política de Seguridad de la Información, el modelo de Gestión de Incidentes de Seguridad y Ciberseguridad y la adherencia al marco de referencia.

La verificación del cumplimiento de los estándares definidos en materia de seguridad, así como también la notificación de cualquier evento o vulnerabilidad en ningún caso significará la adopción de algún tipo de responsabilidad por parte de la Institución que Provee frente a eventos anómalos o vulnerabilidades.

Las Instituciones que Consultan y Proveen, deberán definir una persona responsable de gestionar la relación, en materias de seguridad de la información, ciberseguridad y fraudes.

3.2.2. Aspectos de Prevención de Fraudes

Este Acuerdo Marco promueve que todos los participantes proporcionen entre ellos – en la forma que se establezca en los Acuerdos Bilaterales - la información técnica asociada a eventos de fraude transaccional y/o desconocimiento de cargos por parte de los clientes.

3.2.3. Aspectos de Promoción de Seguridad y Ciberseguridad

Las Instituciones que Consultan deberán implementar mecanismos para informar a las Instituciones que Proveen – en la forma que se establezca en los Acuerdos Bilaterales - sobre cualquier evento anómalo (alerta o incidente), vulnerabilidades técnicas de categoría crítica o eventos de fraude identificados en la infraestructura de la Institución que Consulta, y afecte la seguridad de la información de los clientes o de la Institución que Provee, o su continuidad operacional.

La notificación de cualquier evento o vulnerabilidad en ningún caso significará la adopción de algún tipo de responsabilidad por parte de la Institución que Provee frente a eventos anómalos o vulnerabilidades de la Institución que Consulta, de conformidad a lo señalado en la sección 3.3.

3.2.4. Bloqueo de acceso en casos graves

Las Instituciones que Proveen podrán bloquear los accesos de las Instituciones que Consultan, en caso de que éstas presenten vulnerabilidades críticas o estén bajo un ciberataque o amenaza de éste, exista fuga de información, se incumplan los protocolos de seguridad previamente establecidos, u otro evento que pudiese afectar la seguridad de la información o la continuidad operativa de la Institución que Provee o sus clientes.

3.3. Estándares de responsabilidad

3.3.1. Actualizaciones y mantenciones de los sitios web, plataformas y apps de las Instituciones que Proveen

Las actividades realizadas por las Instituciones que Consultan no limitarán a las Instituciones que Proveen a desarrollar las mantenciones, actualizaciones, modificaciones o reemplazos que estimen necesarias en sus sitios web, plataformas y apps, sin mediar notificación.

3.3.2. Responsabilidad ante vulneraciones de datos personales

Las Instituciones que Consultan que presten servicios basados en captura de datos, serán responsables ante sus clientes por las vulneraciones a sus datos personales, en conformidad con la Ley 19.628 y sus modificaciones.

Las Instituciones que Consultan deberán proporcionar a las Instituciones que Proveen, los antecedentes que estas últimas requieran en el marco de una solicitud emanada de un organismo regulador.

3.3.3. Responsabilidad ante fraudes

3.3.3.1 Las entidades participantes del Acuerdo Marco acuerdan un procedimiento simplificado para determinar la responsabilidad de las partes por operaciones desconocidas por clientes de las Instituciones que Proveen según la Ley 20.009, conforme se indica en la presente sección.

3.3.3.2 Las Instituciones que Consultan, que estén autorizadas por sus clientes para realizar actividades de captura de datos, serán responsables y se obligan a reembolsar, conforme se determine mediante los procedimientos descritos en la sección siguiente, a las Instituciones que Provean por los montos que estas últimas hayan soportado o en que deban incurrir a favor de sus clientes en conformidad a la ley con ocasión del fraude, cuando exista una causa imputable a la Institución que Consulta, como, por ejemplo, relativa a errores en sus plataformas o vulnerabilidades en sus sistemas, que permitan el acceso no autorizado por terceros o produzcan la divulgación de credenciales o información de clientes;

Con todo, las Instituciones que Provean reembolsarán a las Instituciones que Consultan, los montos devueltos a o recuperados por las Instituciones que Provean.

Nada de lo indicado en este Acuerdo podrá entenderse como una renuncia de la Institución que Provee a ejercer las acciones legales que correspondan en contra de quienes pudieren resultar responsables directos por un fraude.

3.3.3.3 Para los efectos del numeral anterior, las entidades participantes del Acuerdo Marco deberán analizar de buena fe y realizar sus mejores esfuerzos para determinar el origen de un fraude que hayan sufrido clientes de las Instituciones que Proveen. Para estos efectos, dichas entidades dispondrán de un plazo de 12 días hábiles corridos desde la notificación por parte de la Institución que Provee a la Institución que Consulta.

3.3.3.4 En caso de no alcanzar un acuerdo dentro del plazo antes indicado, toda diferencia, dificultad, o controversia que surja entre entidades participantes del Acuerdo Marco respecto de un evento de fraude sufrido por algún cliente de la Institución que Provee y, particularmente sobre quién debe ser considerado responsable y asumir los daños ocasionados, en virtud de lo establecido en el presente numeral, será sometido a conocimiento y resolución de una comisión arbitral integrada por tres miembros, quienes resolverán en única instancia y como tribunal arbitral mixto, esto es, actuando como arbitradores en cuanto al procedimiento y conforme a derecho en cuanto a la sentencia y sus fundamentos.

Todos los miembros de la comisión arbitral deberán ser abogados. Cada entidad tendrá derecho a designar libremente a un miembro, dentro de aquellos que figuren en el listado del cuerpo arbitral del Centro de Arbitrajes y Mediación (CAM) de la Cámara de Comercio de Santiago A.G. El tercer miembro, quien presidirá la comisión arbitral, será designado por el mismo Centro de Arbitrajes de la Cámara de Comercio de Santiago A.G. a petición escrita de cualquiera de las partes, para lo cual ambas confieren poder especial e irrevocable a esta última.

Una vez instalada la Comisión Arbitral y fijadas las normas de procedimiento, dispondrá de un plazo máximo de 120 días para sustanciar el procedimiento y dictar sentencia. Dicho plazo podrá ser prorrogado por 60 días más, por voluntad de ambas partes.

3.3.3.5. Nada de lo indicado en este Acuerdo Marco podrá entenderse como una limitación a la responsabilidad de las Instituciones que Consultan. En consecuencia, las Instituciones que Proveen podrán demandar los daños o perjuicios que sufran con ocasión de hechos imputables a las Instituciones que Consultan en conformidad con la ley aplicable.

4. Vigencia del Presente Acuerdo Marco

Cualquiera de las partes del Acuerdo Marco podrá ponerle término anticipado unilateralmente y/o a cualquiera de sus anexos, en cualquier tiempo, sin que por esto quede obligado al pago

de multa, indemnización o suma por concepto alguno, no siendo necesaria declaración judicial, arbitral o de ninguna otra naturaleza, bastando para ello el envío de un aviso por carta certificada al domicilio de la otra parte indicado en este Acuerdo Marco, con al menos 30 días corridos de anticipación a la fecha que la parte correspondiente fije para su término.

En todo caso, las partes deberán tomar las medidas y adecuar el presente Acuerdo Marco a los requisitos normativos que regulen alguno de los aspectos tratados en el presente Acuerdo.

5. Mecanismos de Resolución de Controversias

Las entidades acordarán en forma bilateral los mecanismos de resolución de conflictos que consideren apropiados, referidos a la interpretación, ejecución, cumplimiento, resolución, terminación, validez, nulidad, o cualquier otra materia que se derive directa o indirectamente de dichos Acuerdos Bilaterales.

ANEXO 1
CONTROLES MINÍMOS DE CIBERSEGURIDAD
ACUERDO MARCO FINTECHILE - ABIF

A partir de la Normativa RAN 20-10 sobre la gestión de seguridad de la informacion y ciberseguridad, se han particularizado los requisitos contenidos en la normativa y se han definido dos criterios que instruyen la gestión que deben realizar la organizaciones que se adhieran al acuerdo marco entre ABIF y FinteChile.

Criterios (columna H)

- **Línea base: Establecen los controles y requisitos minimos necesarios a cumplir, por parte de todas las Instituciones.**
- **Gestión basada en riesgo: Establece los controles y requisitos que deben ser implementados en función de la evaluación de riesgo que realice cada Institución.**

NOTAS:
En los requisitos que se indique Directorio, se debe entender como la autoridad máxima de la empresa Fintech.
Este documento debe actualizarse en función de las actualizaciones de la normativa RAN 20-10

ID	Organismo	Normativa	Dominio	Ámbito	Requisito	Gestión Controles
1	CMF	RAN-20-10	2	Elementos generales de gestión	El Directorio, o quien haga sus veces, ha definido una estructura organizacional con personal especializado y dedicado e instancias colegiadas de alto nivel jerárquico, con atribuciones y competencias necesarias para gestionar la seguridad de la información y ciberseguridad, procurando una adecuada segregación funcional entre las diferentes áreas e instancias encargadas de estas materias, con roles y responsabilidades claramente establecidos para cada una de ellas.	Gestión basada en riesgo
2	CMF	RAN-20-10	2	Elementos generales de gestión	La entidad realiza inversiones en tecnologías de procesamiento y seguridad de la información y ciberseguridad, que responden a una estrategia definida para estos efectos, que permiten mitigar los riesgos operacionales y tecnológicos y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.	Gestión basada en riesgo
3	CMF	RAN-20-10	2	Elementos generales de gestión	Dentro de la estructura organizacional definida se ha dispuesto un ROL de riesgo, independiente de las áreas generadoras de riesgos, encargada del diseño y mantención de un adecuado sistema de identificación, seguimiento, control y mitigación de los riesgos de seguridad de la información y ciberseguridad. Además, debe ser parte de esta estructura organizacional, el rol de un oficial de seguridad de la información y ciberseguridad a cargo de estas materias.	Gestión basada en riesgo
4	CMF	RAN-20-10	2	Elementos generales de gestión	El Directorio ha dispuesto una estructura de alto nivel para la administración de crisis, con atribuciones técnicas y del negocio para conocer y administrar los incidentes de seguridad y ciberseguridad de alto impacto que afecten o pudieran afectar los activos de información, propios o de sus clientes. Como parte de sus funciones, esta estructura debe definir un plan de actuación frente a este tipo de eventos y mantener canales de comunicación adecuados para informar oportunamente de estos incidentes a las autoridades y a las partes interesadas, ya sean internas o externas a la institución.	Gestión basada en riesgo
5	CMF	RAN-20-10	2	Elementos generales de gestión	El Directorio ha aprobado políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad que definan al menos, el alcance y los objetivos de la entidad respecto de estas materias; el nivel de tolerancia al riesgo en específico para cada una de ellas; una clara definición de los activos de información a resguardar; criterios para clasificar la información y la existencia de un inventario de activos de información permanentemente actualizado, consistente con el mapa de procesos de la entidad. Estas políticas deben ser ampliamente difundidas al interior de la organización, revisadas y aprobadas al menos anualmente por esta instancia.	Línea Base
6	CMF	RAN-20-10	2	Elementos generales de gestión	El Directorio como parte del nivel de tolerancia definido ha establecido los niveles de disponibilidad mínimos que espera asegurar en los servicios otorgados a través de plataformas tecnológicas, a fin de otorgar una adecuada prestación de servicios a los clientes.	Gestión basada en riesgo
7	CMF	RAN-20-10	2	Elementos generales de gestión	El Directorio se asegura de informarse periódica y adecuadamente respecto de los riesgos a que está expuesta la entidad en términos de seguridad de la información y ciberseguridad, así como del cumplimiento de sus políticas e incidentes de seguridad de la información y ciberseguridad pronunciándose sobre ellos al menos semestralmente, con el fin de mejorar su gestión y prevención	Gestión basada en riesgo
8	CMF	RAN-20-10	2	Elementos generales de gestión	El Directorio ha aprobado políticas de conducta interna, de manera que todos los empleados y/o personas externas que presten servicios a la entidad utilicen de manera responsable las tecnologías de la información y comunicación puestas a su disposición.	Gestión basada en riesgo

9	CMF	RAN-20-10	2	Elementos generales de gestión	La entidad promueve una cultura de riesgos en materia de seguridad de la información y ciberseguridad. Esto a través de planes formales de difusión, capacitación y concientización a todos los empleados y personal externo que preste servicios a la entidad, los que deben estar en concordancia con las funciones desempeñadas, considerando una periodicidad establecida y oportuna.	Gestión basada en riesgo
10	CMF	RAN-20-10	2	Elementos generales de gestión	Los activos de información de la entidad cuentan con un adecuado resguardo en términos de la seguridad física y ambiental, como, por ejemplo: la protección de las áreas sensibles de negocios, operativas y dependencias técnicas dentro de las que se encuentran los centros de datos, fuentes de energía alterna (UPS por su sigla en inglés) y respaldos de datos y aplicativos.	Gestión basada en riesgo
11	CMF	RAN-20-10	2	Elementos generales de gestión	La entidad como parte de la gestión de sus servicios externalizados, ha implantado un proceso de verificación permanente de la aplicación y cumplimiento de sus políticas de seguridad de la información y ciberseguridad, de manera de garantizar la adecuada protección de los activos de información que son utilizados o administrados por proveedores externos. Asimismo, monitorea permanentemente la infraestructura conectada con proveedores externos, y analiza e implementa medidas para detectar y mitigar potenciales amenazas a la ciberseguridad de la entidad.	Gestión basada en riesgo
12	CMF	RAN-20-10	2	Elementos generales de gestión	La entidad se asegura de evaluar oportunamente los riesgos asociados a la seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades y/o definir nuevos procesos.	Línea Base
13	CMF	RAN-20-10	2	Elementos generales de gestión	La entidad gestiona sus incidentes de seguridad de la información y ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación de impacto de estos eventos, y resguardar la confidencialidad, disponibilidad e integridad de sus activos de información.	Línea Base
14	CMF	RAN-20-10	2	Elementos generales de gestión	El proceso de gestión de la seguridad de la información y ciberseguridad implementado por la entidad asegura el cumplimiento de las leyes y normativas vigentes, entre las que se encuentran, por ejemplo, la protección de los datos de carácter personal y los derechos de propiedad intelectual.	Gestión basada en riesgo
15	CMF	RAN-20-10	2	Elementos generales de gestión	La entidad realiza auditorías al proceso de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias.	Gestión basada en riesgo
16	CMF	RAN-20-10	3	Proceso de gestión de riesgos de seguridad de la información y ciberseguridad	Identificación de sus activos de información de acuerdo con la definición y alcance contenido en la política de seguridad de la información y ciberseguridad. El nivel de detalle utilizado en la identificación del activo de información debe ser suficiente para la adecuada evaluación del riesgo, considerando, por ejemplo, su ubicación física y función, entre otros aspectos.	Gestión basada en riesgo
17	CMF	RAN-20-10	3	Proceso de gestión de riesgos de seguridad de la información y ciberseguridad	Identificación de las amenazas que puedan dañar los activos de información, así como de sus vulnerabilidades con relación a las amenazas conocidas y los controles existentes. La identificación de amenazas y vulnerabilidades se refuerza con información obtenida de diferentes fuentes, tanto internas como externas.	Línea Base
18	CMF	RAN-20-10	3	Proceso de gestión de riesgos de seguridad de la información y ciberseguridad	Evaluación de los controles existentes de manera de conocer su efectividad y suficiencia.	Gestión basada en riesgo
19	CMF	RAN-20-10	3	Proceso de gestión de riesgos de seguridad de la información y ciberseguridad	Identificación de las consecuencias que puedan tener en los activos de información las pérdidas de confidencialidad, integridad y disponibilidad.	Gestión basada en riesgo
20	CMF	RAN-20-10	3	Proceso de gestión de riesgos de seguridad de la información y ciberseguridad	La entidad realiza un proceso de análisis de riesgo, que considera elementos como la evaluación de la probabilidad de ocurrencia de incidentes y su consecuencia o impacto en los activos de información, en base al grado de daño o costos causados por un evento de seguridad de la información y de ciberseguridad, determinando así su nivel de riesgo.	Gestión basada en riesgo
21	CMF	RAN-20-10	3	Proceso de gestión de riesgos de seguridad de la información y ciberseguridad	La entidad efectúa un proceso de valoración del riesgo, entendido como una actividad donde se compara el nivel de riesgo determinado previamente contra los criterios de valoración y de tolerancia, previamente definidos.	Gestión basada en riesgo
22	CMF	RAN-20-10	3	Proceso de gestión de riesgos de seguridad de la información y ciberseguridad	La entidad elabora un plan de tratamiento del riesgo, entendido como una actividad donde los riesgos priorizados en la etapa de valoración, permiten establecer los controles para reducir, aceptar, evitar o transferir los riesgos.	Gestión basada en riesgo
23	CMF	RAN-20-10	3	Proceso de gestión de riesgos de seguridad de la información y ciberseguridad	La entidad lleva a cabo un proceso formal tendiente a asegurar que los riesgos resultantes sean concordantes con la tolerancia a los riesgos definida.	Gestión basada en riesgo
24	CMF	RAN-20-10	3	Proceso de gestión de riesgos de seguridad de la información y ciberseguridad	La entidad monitorea y revisa regularmente su proceso de gestión de riesgos de seguridad de la información y ciberseguridad, de manera de identificar oportunamente la necesidad de efectuar ajustes en las metodologías y/o herramientas utilizadas.	Gestión basada en riesgo

25	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La institución cuenta con un inventario de activos ciberseguridad críticos clasificados desde una perspectiva de confidencialidad, integridad y disponibilidad, considerando sus diferentes estados de su ciclo de vida como son el almacenamiento, la transmisión y procesamiento.	Línea Base
26	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad cuenta con un proceso de gestión del cambio que permite que las modificaciones realizadas a la infraestructura de tecnologías de la información (TI) sean efectuadas de manera segura y controlada, y que los cambios realizados son controlados y monitoreados.	Línea Base
27	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad cuenta con un apropiado proceso de gestión de capacidades, que le permite asegurar que la infraestructura TI cubre las necesidades presentes y futuras, considerando el volumen y complejidad de las operaciones de la entidad.	Gestión basada en riesgo
28	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad cuenta con un proceso de gestión de la obsolescencia tecnológica que le permite mantener una infraestructura TI con estándares de seguridad adecuados.	Línea Base
29	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad cuenta con un proceso de gestión de configuraciones que permite asegurar adecuados controles a los elementos configurables de la infraestructura TI; y su acceso es controlado y monitoreado.	Línea Base
30	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad ha implementado un programa de gestión de parches para asegurar que éstos sean aplicados tanto al software como al firmware de manera oportuna.	Línea Base
31	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	Las redes informáticas se encuentran adecuadamente protegidas de ataques provenientes de Internet o de otras redes externas, a través de la implementación de herramientas que se complementan, tales como: firewalls, firewalls de aplicaciones web (WAF), sistemas de prevención de intrusos (IPS), sistemas de prevención de pérdida de datos (DLP), sistemas anti denegación de servicios, filtrado de mail, antivirus y anti-malware.	Línea Base
32	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	Las redes informáticas se encuentran segmentadas de manera de implementar controles diferenciados, considerando aspectos como grupos de usuarios, tráfico de datos encriptado, tipo de servicios y sistemas de información, a fin de proteger las comunicaciones y los activos críticos de ciberseguridad, así como aislar la propagación de los efectos adversos que podrían derivarse de ciberataques a la infraestructura tecnológica.	Línea Base
33	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La segmentación de redes alcanza los diferentes ambientes dispuestos por la entidad, entre los que se encuentran aquellos de desarrollo, de pruebas y de producción.	Línea Base
34	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	Los controles establecidos permiten proteger y detectar en forma proactiva ataques a la infraestructura TI realizados a través del uso de códigos maliciosos.	Línea Base
35	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	Los controles establecidos permiten mitigar los riesgos derivados del uso de dispositivos móviles y del trabajo a distancia realizado por personal interno o externo.	Línea Base
36	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	Los controles establecidos mitigan los riesgos derivados de la adquisición o desarrollo de aplicativos y sistemas, así como su puesta en producción.	Línea Base
37	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La gestión de identidades y de acceso físico y lógico contempla adecuados controles para resguardar las áreas de acceso restringido, los privilegios otorgados a los usuarios de los sistemas, los derechos de accesos a los servicios de red, a los sistemas operativos, a las bases de datos y a las aplicaciones de negocios, entre otros aspectos.	Línea Base
38	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad cuenta con adecuadas herramientas para controlar, registrar y monitorear las actividades realizadas por los usuarios en general, así como de aquellos con privilegios especiales.	Línea Base

39	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	Los canales electrónicos dispuestos por la entidad, con los que interactúan los clientes y usuarios, cuentan con apropiados mecanismos de control de accesos, de manera de mitigar, entre otros, los riesgos de suplantación o uso indebido por parte de terceros, de los productos y servicios puestos a su disposición.	Línea Base
40	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad ha dispuesto normas y procedimientos que establecen el tipo de información que requiere ser protegida a través de técnicas de cifrado, así como los algoritmos criptográficos permitidos o autorizados, controles que se utilizan tanto para la transmisión como para el almacenamiento de la información, en orden de proteger su confidencialidad e integridad.	Línea Base
41	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad ha implementado adecuados resguardos para la conservación, transmisión y eliminación de la información, en conformidad con lo establecido en las políticas internas y la legislación vigente.	Línea Base
42	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad ha dispuesto herramientas de monitoreo permanente que le permitan en forma proactiva identificar, recolectar y analizar información interna y externa respecto de nuevas amenazas y vulnerabilidades que puedan afectar sus activos de ciberseguridad.	Gestión basada en riesgo
43	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad cuenta con un proceso de administración de respaldos que le permite asegurar la integridad y la disponibilidad de su información y de sus medios de procesamiento, ante la ocurrencia de un incidente o desastre. A su vez, la entidad realiza al menos anualmente pruebas de restauración de sus respaldos, con el fin de verificar que la información crítica puede ser recuperada en caso que los datos originales se pierdan o se dañen.	Gestión basada en riesgo
44	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad evalúa mecanismos de cobertura destinados a cubrir los costos asociados a eventuales ataques cibernéticos.	Gestión basada en riesgo
45	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad cuenta con un Security Operación Center (SOC), propio o a través de un servicio externo, que opera las 24 horas del día, con instalaciones, herramientas tecnológicas y personal dedicado, a fin de prevenir, detectar, evaluar y responder a amenazas e incidentes de ciberseguridad.	Gestión basada en riesgo
46	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad identifica y evalúa regularmente los vectores de ataque a los cuales pudiera estar expuesta, como por ejemplo la manipulación o interceptación de las comunicaciones; phishing; malware; elevación de privilegios; inyección de código; denegación de servicios; ingeniería social; etc., distinguiendo claramente entre aquellos que pueden afectar la infraestructura física; la infraestructura lógica; o los equipos finales (endpoint).	Línea Base
47	CMF	RAN-20-10	4.1	Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades	La entidad realiza en forma regular, con el suficiente alcance y profundidad, pruebas a la infraestructura crítica de ciberseguridad para detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información en el ciberespacio, tales como pentesting y/o ethical hacking. Sus resultados son gestionados por las áreas de tecnología y seguridad de la información, monitoreados y controlados por el oficial de seguridad, y comunicados al Directorio, al menos semestralmente, quedando evidencia en las actas de los análisis y acuerdos adoptados.	Línea Base
48	CMF	RAN-20-10	4.2	Respuesta y recuperación de las actividades ante incidentes	La entidad prueba, al menos anualmente, los planes necesarios para enfrentar adecuadamente los escenarios que puedan afectar la ciberseguridad, así como los equipos para dar respuesta a los ciberincidentes que se pudieran materializar, conforme a los escenarios que amenacen la ciberseguridad, definidos de acuerdo al Capítulo 20-9 de la RAN. Estos planes son actualizados cada vez que se registran cambios relevantes, o se materialicen eventos que amenacen la ciberseguridad.	Línea Base
49	CMF	RAN-20-10	4.2	Respuesta y recuperación de las actividades ante incidentes	La entidad cuenta con un plan definido de actuación, que dependiendo de la severidad de un incidente de ciberseguridad permite escalar la situación a la alta administración para la toma de decisiones.	Línea Base
50	CMF	RAN-20-10	4.2	Respuesta y recuperación de las actividades ante incidentes	La entidad cuenta con un plan de comunicaciones, liderado por la alta administración, que opera ante incidentes de ciberseguridad de alto impacto, el cual alcanza a todas las partes interesadas, ya sea internas o externas, a fin de mantenerlas adecuadamente informadas.	Línea Base
51	CMF	RAN-20-10	4.2	Respuesta y recuperación de las actividades ante incidentes	La entidad efectúa un proceso de análisis forense para los ciberincidentes relevantes, que incluya al menos las etapas de investigación y recolección de evidencias, junto con la generación de documentación con el análisis y las conclusiones del trabajo realizado; además de los requerimientos necesarios para custodiar adecuadamente las evidencias generadas.	Gestión basada en riesgo
52	CMF	RAN-20-10	4.2	Respuesta y recuperación de las actividades ante incidentes	La entidad cuenta con una base comprensiva de incidentes de ciberseguridad que ponen en riesgo la seguridad de los activos de información presentes en el ciberespacio, identificados de manera individual.	Gestión basada en riesgo

53	CMF	RAN-20-10	4.2	Respuesta y recuperación de las actividades ante incidentes	La entidad considera la base de incidentes como un insumo para la realización de pruebas que permitan detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información y ciberseguridad.	Gestión basada en riesgo
54	CMF	RAN-20-10	4.2	Respuesta y recuperación de las actividades ante incidentes	La entidad cuenta con una base de conocimientos y lecciones aprendidas, con el objeto de disminuir los tiempos de respuesta cuando se repita un incidente igual o similar; identificar posibles mejoras en los procesos; facilitar el intercambio de conocimientos; y disponer de información que permita apoyar la toma de decisiones en caso de materializarse nuevos incidentes.	Gestión basada en riesgo
55	CMF	RAN-20-10	4.2	Respuesta y recuperación de las actividades ante incidentes	La entidad realiza autoevaluaciones en esta materia, al menos anualmente, para determinar el grado de cumplimiento con las políticas internas, normativa regulatoria y la adherencia a las mejores prácticas en ciberseguridad, de manera de determinar las vulnerabilidades de su infraestructura y tomar las acciones para su mitigación, así como para prever la adopción oportuna de medidas ante escenarios de amenazas de ciberseguridad.	Gestión basada en riesgo