Difusión a terceras partes interesadas de las políticas corporativas de Ciberseguridad y Seguridad de la información

Ciberresiliencia

BCC | GRUPO CAJAMAR

Índice

Control de versiones 3
Introducción 4
Ámbito de aplicación y alcance 4
Fundamento y objetivos: compromisos e iniciativas 5
Marco de gobierno 6
Principios básicos 7
- Gobierno 7
- Proveedores (Riesgo tecnológico) 7
- Seguridad de la Información 8
- Operaciones de Ciberseguridad 8
- Monitorización en Ciberseguridad 8
- Resiliencia tecnológica y no tecnológica 8
- Revisiones de seguridad de la información, ciberseguridad, evaluaciones y pruebas 8
- Formación y Concienciación en Ciberseguridad (interna y externa) 9
- Seguridad y Continuidad en Proyectos 9
- Gestión del cambio tecnológico 9
- Gestión de Crisis y comunicación 9
- Riesgo Tecnológico 9
- Indicadores y KRIs 10

Certificaciones y estándares de referencia 10

Control de versiones

Versión	Fecha	Descripción
1	31.05.2026	Primera versión resumida del marco de gobierno de Ciber Resiliencia

Introducción

El Grupo Cooperativo Cajamar (en adelante, el "Grupo") ha establecido su marco de actuación en el ámbito de la Ciber Resiliencia, entendida como la capacidad de resistir, proteger y defender los sistemas informacionales frente a atacantes y riesgos tecnológicos, mediante un modelo de gobierno constituido por una Estrategia de Resiliencia Operativa y por tres políticas corporativas: (i) Política de Ciberseguridad y Seguridad de la Información, (ii) Política para la Gestión de Riesgos Tecnológicos y (iii) Política de Resiliencia Operativa.

La información es un activo esencial para el desarrollo de la actividad del Grupo, por lo que se mantiene un enfoque orientado a garantizar la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de la información tratada y custodiada en el desarrollo de procesos de negocio y servicios.

La estrategia y el marco de actuación en materia de ciberseguridad, seguridad de la información, gestión del riesgo tecnológico y resiliencia operativa cuentan con el soporte y apoyo del Consejo de Administración y de la Alta Dirección, responsables de velar por su correcta implementación, ejecución y mantenimiento.

El Grupo articula este modelo con el objetivo de proteger sus funciones esenciales, garantizar la continuidad de sus servicios y reforzar la confianza de clientes, socios y organismos supervisores, mediante un enfoque integrado que combina la gestión del riesgo tecnológico, la protección de la información y el fortalecimiento continuo de sus capacidades de resiliencia operativa.

Ámbito de aplicación y alcance

El modelo de gobierno conformado por la Estrategia de Resiliencia Operativa y por las tres Políticas son de cumplimiento obligatorio a todos los empleados del Grupo, con independencia de su nivel jerárquico y de su ubicación funcional o territorial, e incluye igualmente a becarios, personas en prácticas, personas subcontratadas y, en general, a todas aquellas personas que trabajen o presten servicios dentro del Grupo o en empresas que presten servicios al mismo cuando utilicen información de titularidad y/o responsabilidad del Grupo.

El alcance comprende también a proveedores y terceros que acceden a sistemas, redes, servicios o información del Grupo, en los términos establecidos por la normativa interna y por los correspondientes acuerdos contractuales y de nivel de servicio.

Adicionalmente, la Política para la Gestión de Riesgos Tecnológicos aplica a todos los sistemas tecnológicos, infraestructuras digitales, procesos de negocio, proveedores de servicios tecnológicos y personal de la organización, incluyendo colaboradores externos y socios estratégicos.

Fundamento y objetivos: compromisos e iniciativas

El Grupo debe cumplir con la normativa vigente y con los requerimientos de los organismos supervisores y autoridades competentes en materia de Seguridad de la Información, Ciberseguridad, Resiliencia Operativa Digital y Protección de Datos Personales. Para ello, sus políticas toman como referencia los marcos regulatorios más relevantes, entre los que destacan DORA y sus desarrollos técnicos, RGPD y LOPDGDD, las directrices de la EBA en materia de riesgo TIC, seguridad, gobierno interno y externalización, el Esquema Nacional de Seguridad, TIBER-EU/TIBER-ES, las expectativas de ciberresiliencia del BCE y, cuando resulte aplicable, estándares internacionales como NIST, entre otros.

En este contexto, el modelo de ciber resiliencia del Grupo establece un marco integral para prevenir, proteger, detectar, responder y recuperarse ante riesgos tecnológicos y ciberamenazas, alineando estas capacidades con los objetivos estratégicos y el apetito al riesgo de la organización.

La Estrategia de Resiliencia Operativa establece el marco general mediante el que el Grupo afronta el riesgo relacionado con las TIC y refuerza su capacidad para prevenir, responder y recuperarse ante interrupciones. Para ello, integra la definición de tolerancias, objetivos, indicadores, arquitectura tecnológica, gestión de incidentes, pruebas de resiliencia y mecanismos de comunicación.

La Política de Ciberseguridad y Seguridad de la Información define el marco corporativo para proteger los activos de información del Grupo, asegurando su confidencialidad, integridad, disponibilidad y trazabilidad. Su finalidad es garantizar una gestión eficaz de las amenazas, alineada con la estrategia del Grupo y basada en un modelo de mejora continua que refuerza la capacidad de anticipación, resistencia y recuperación ante incidentes.

La Política para la Gestión de Riesgos Tecnológicos establece el marco para identificar, evaluar, tratar, monitorizar y reportar los riesgos derivados del uso de la tecnología. Su objetivo es asegurar una gestión estructurada y homogénea de estos riesgos, alineada con el apetito al riesgo del Grupo y orientada a proteger sus procesos, sistemas y servicios.

La Política de Resiliencia Operativa define el marco de continuidad y respuesta del Grupo ante eventos disruptivos que puedan afectar a sus funciones esenciales. Su finalidad es garantizar la capacidad de mantener o restablecer la actividad dentro de niveles aceptables, mediante planes de continuidad, recuperación y gestión de crisis.

Marco de gobierno

El Grupo dispone de un modelo de gobierno que permite supervisar, coordinar y controlar de forma integral las capacidades de ciberseguridad, gestión del riesgo tecnológico y resiliencia operativa. Este modelo establece funciones y responsabilidades diferenciadas, garantizando una toma de decisiones informada, una implantación homogénea de las medidas y un seguimiento continuo del marco de control.

El marco de gobierno contempla un sistema de reporte formal y periódico a los órganos de gobierno del Grupo. En particular, el Consejo de Administración recibe, periódicamente y adicionalmente cuando las circunstancias lo requieren, información estructurada sobre la evolución del riesgo tecnológico y de ciberseguridad, el estado del entorno de control de ciberseguridad, los principales incidentes y vulnerabilidades, los resultados de auditorías y evaluaciones, el avance de los planes de acción y los indicadores y KRIs más relevantes.

A continuación, se presentan las responsabilidades y funciones clave de los órganos que participan en el modelo de gobierno de la ciber resiliencia, a considerar para aquellos órganos y áreas que tienen un rol en el marco de gobierno de la Ciberseguridad.

- El Consejo de Administración asume la responsabilidad última sobre el marco de ciberseguridad, riesgo tecnológico y resiliencia operativa del Grupo. Le corresponde aprobar las políticas y estrategias en esta materia, supervisar su aplicación y revisar periódicamente que existan recursos, capacidades y formación adecuados para su correcta implantación.
- El Comité de Tecnología y Ciberseguridad actúa como órgano de información, asesoramiento y propuesta al Consejo de Administración en materias vinculadas al riesgo tecnológico, la ciberseguridad y la estrategia tecnológica. Realiza seguimiento de las principales exposiciones, de la evolución de los planes de respuesta y recuperación y de los asuntos tecnológicos relevantes para el Grupo.
- El Comité de Riesgos ejerce una función de supervisión y contraste sobre el perfil global de riesgos del Grupo, incluyendo aquellos derivados de la tecnología. Su papel favorece que las decisiones en materia de riesgo se adopten con una visión integral, coherente con el apetito al riesgo y con los objetivos estratégicos de la organización.
- El Comité de Dirección actúa como nexo entre los órganos de gobierno y las áreas ejecutivas del Grupo, impulsando los planes de actuación y el seguimiento de las políticas aprobadas. En este ámbito, supervisa la evolución de la ciberseguridad, la resiliencia operativa y el riesgo tecnológico, y favorece la traslación de las directrices estratégicas a la gestión ordinaria.
- El Comité de Ciberseguridad y Resiliencia Operativa coordina y realiza el seguimiento de las iniciativas estratégicas asociadas a la protección de la información, la ciber resiliencia y la continuidad de negocio. Asimismo, revisa propuestas normativas, supervisa iniciativas de mejora, reportes regulatorios, planes de prueba y planes de acción derivados de auditorías o certificaciones.
- El Comité de Riesgos Tecnológicos realiza el seguimiento de los riesgos

tecnológicos más relevantes del Grupo y evalúa las propuestas de tratamiento y remediación asociadas. También analiza alertas, indicadores, riesgos en proveedores tecnológicos y la adecuación de las medidas adoptadas respecto al nivel de riesgo definido por la organización.

- La Dirección de Ciber Resiliencia, liderada por la función CISO, define y mantiene el marco de protección de la información, ciberseguridad, riesgo tecnológico y resiliencia operativa del Grupo. Entre sus responsabilidades se incluyen el asesoramiento a los órganos de gobierno, la definición de controles y metodologías, la gestión de incidentes, el seguimiento de amenazas y el impulso de la formación y concienciación.
- La Dirección de Tecnología y Procesos impulsa la implantación práctica de las medidas técnicas y organizativas necesarias para cumplir el cuerpo normativo aplicable en materia de ciberseguridad, seguridad de la información y resiliencia operativa. Su función resulta clave para trasladar los requisitos de control al diseño, operación y evolución de los servicios tecnológicos.
- La Dirección General de Auditoría Interna realiza una revisión independiente de los sistemas de gestión y control vinculados a la ciberseguridad, el riesgo tecnológico, la resiliencia operativa, la continuidad de negocio y la gestión de crisis. Su función contribuye a verificar la eficacia del marco implantado y a promover su mejora continua.

Principios básicos

Los principios básicos del modelo de ciber resiliencia del Grupo se estructuran en los siguientes ámbitos, que abarcan el gobierno, la protección, la operación y la resiliencia de las capacidades tecnológicas y de negocio:

Gobierno

El ámbito de gobierno establece cómo se organizan la supervisión, la toma de decisiones y la asignación de responsabilidades en materia de ciberseguridad, riesgo tecnológico y resiliencia operativa. Su finalidad es asegurar que existan roles claros, seguimiento por los órganos competentes y una dirección alineada con la estrategia y el marco de control del Grupo.

Proveedores (Riesgo tecnológico)

Este ámbito se centra en asegurar que los servicios prestados por terceros se gestionan con niveles adecuados de seguridad, continuidad y control. Para ello, se contemplan requisitos en los acuerdos con proveedores, así como mecanismos de seguimiento, evaluación o verificación del cumplimiento de estos requisitos, de acuerdo con el enfoque de riesgo aplicable y con las condiciones previstas en cada relación contractual.

Seguridad de la Información

La seguridad de la información tiene como objetivo proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información del Grupo. Este ámbito recoge los principios y medidas necesarias para garantizar un uso adecuado de los activos de información y prevenir accesos, alteraciones o divulgaciones no autorizadas.

Operaciones de Ciberseguridad

Las operaciones de ciberseguridad agrupan las medidas orientadas a prevenir, detectar, contener y responder ante amenazas o incidentes que afecten a los sistemas y servicios tecnológicos. Incluyen, entre otros aspectos, la gestión de vulnerabilidades, la protección de activos, la configuración segura y la implantación de controles técnicos de seguridad.

Monitorización en Ciberseguridad

Este ámbito se orienta a la vigilancia continua de la actividad tecnológica para identificar comportamientos anómalos, amenazas, incidentes o posibles vulnerabilidades. Su finalidad es facilitar una detección temprana y una respuesta oportuna, fortaleciendo la capacidad preventiva y reactiva de la organización.

Resiliencia tecnológica y no tecnológica

La resiliencia tecnológica y no tecnológica abarca la capacidad del Grupo para mantener o restablecer sus funciones esenciales ante interrupciones, tanto si tienen origen en sistemas TIC como en personas, procesos, instalaciones o proveedores. Su objetivo es asegurar la continuidad del negocio mediante planes, recursos y medidas de respuesta y recuperación adecuados.

Revisiones de seguridad de la información, ciberseguridad, evaluaciones y pruebas

Este ámbito comprende la realización de revisiones y pruebas periódicas orientadas a verificar la solidez del marco de seguridad de la información y ciberseguridad, así como su capacidad real de respuesta ante escenarios de crisis, incluyendo auditorías internas y externas, análisis de brechas y revisiones técnicas que permiten identificar debilidades y validar los controles existentes; adicionalmente, se ejecutan pruebas específicas de resiliencia operativa, tanto tecnológicas como no tecnológicas, tales como pruebas de recuperación, ejercicios avanzados tipo TLPT conforme a TIBER-EU/TIBER-ES y pruebas de penetración, con el objetivo de evaluar de forma práctica la eficacia de las medidas implantadas en todas las fases de prevención, respuesta y recuperación, e identificar oportunidades de mejora continua.

Formación y Concienciación en Ciberseguridad (interna y externa)

La formación y concienciación buscan reforzar el conocimiento y la cultura de seguridad en todas las personas que participan en la actividad del Grupo. Este ámbito promueve formación obligatoria y periódica para reducir errores, fomentar comportamientos seguros y asegurar que empleados y colectivos relevantes conocen sus responsabilidades. Asimismo, el Grupo establece e implementa programas periódicos de concienciación sobre seguridad que incluyan tanto al personal como a los miembros del Consejo de Administración, con el fin de garantizar una adecuada comprensión de los riesgos relacionados con la seguridad de la información y su correcta gestión.

Seguridad y Continuidad en Proyectos

Este ámbito persigue que los proyectos tecnológicos incorporen, desde sus fases iniciales, requisitos de seguridad y continuidad acordes con la criticidad de los servicios afectados. De este modo, se favorece que nuevas iniciativas, cambios o desarrollos se implanten de forma segura, controlada y alineada con las necesidades de resiliencia del Grupo.

Gestión del cambio tecnológico

La gestión del cambio tecnológico regula cómo deben evaluarse, aprobarse, probarse, documentarse e implantarse los cambios en los sistemas y servicios tecnológicos. Su finalidad es minimizar riesgos, evitar impactos no deseados y garantizar que la evolución tecnológica se produce de forma controlada.

Gestión de Crisis y comunicación

Este ámbito recoge los mecanismos necesarios para activar una respuesta organizada ante situaciones graves que puedan alterar el funcionamiento normal del Grupo. Incluye la coordinación de actuaciones, la definición de roles y la comunicación interna y externa con las partes interesadas y, cuando proceda, con las autoridades competentes. Estos mecanismos permiten que las personas destinatarias comuniquen de forma inmediata cualquier incidente, vulnerabilidad o comportamiento anómalo detectado, asegurando su evaluación, tratamiento, seguimiento y, cuando proceda, la activación de medidas de contención, recuperación, comunicación interna o externa y elevación a los órganos competentes.

Riesgo Tecnológico

El riesgo tecnológico se refiere al conjunto de amenazas derivadas del uso, gestión o dependencia de la tecnología que pueden afectar a los procesos, servicios o

activos del Grupo. Este ámbito establece el marco para identificar, evaluar, tratar, monitorizar y reportar dichos riesgos de forma estructurada y alineada con el apetito al riesgo de la organización.

Indicadores y KRIs

Los indicadores y KRIs permiten medir el grado de eficacia del marco de control y monitorizar la exposición al riesgo en materia de ciberseguridad, tecnología y resiliencia operativa. Su función es facilitar el seguimiento periódico, apoyar la toma de decisiones y detectar de manera anticipada desviaciones o señales de deterioro.

Certificaciones y estándares de referencia

El Grupo refuerza su marco de ciber resiliencia mediante la adopción de estándares y esquemas de referencia reconocidos internacionalmente para fortalecer su marco de seguridad y resiliencia. Entre ellos se incluyen certificaciones y acreditaciones como ISO 27001, ENS Alto, PCI DSS y PCI PIN, que contribuyen a consolidar un enfoque de control, mejora continua y alineamiento con buenas prácticas del sector.

Este modelo permite al Grupo ofrecer servicios fiables, seguros y resilientes, incluso en entornos adversos o ante incidentes tecnológicos, contribuyendo a la protección de sus clientes, la continuidad del negocio y el cumplimiento de los requerimientos regulatorios.