Política Corporativa de Seguridad de la Información CertiNet S.A.

2026

Versión 1.3

Código del Documento	SGSI-POL-001
Referencia Normativa	NCh-ISO 27002:2022: 5.1, 5.2, 5.3 y 5.4
Clasificación de la Información	Pública
Versión	1.3
Autor	Roberto Riveros
Revisado Por	Comité de Riesgo Operacional y Seguridad de la Información
Aprobado Por	Directorio de CertiNet

Control de Cambios

Versión	Descripción	Fecha	Creado/Modificado
0.1	Generación de documento a partir de simplificación de documento previo	Junio 2026	Roberto Riveros, Gerente General
0.2	Cambio formato CertiNet	Junio 2026	Isabel Aguilera, Gestor Documental
0.3	Actualización integral para alineación con ISO/IEC 27001:2022 y 27002:2022. Se incorpora: • Controles 5.1, 5.2, 5.3 y 5.4 (Gestión de excepciones, dueños de riesgo, segregación de funciones y canal de denuncias). • Cláusula 6.2 (Objetivos medibles mediante KPIs). • Régimen sancionatorio por incumplimiento. • Flexibilización de referencias legales y marco documental genérico. • Cambio de clasificación a información Pública.	Junio 2026	Pallavicini Consultores
0.4	Aceptación de cambios y ajuste de formato	Junio 2026	Isabel Aguilera, Gestor Documental
1.0	Referencia a certificación ISO 27001 en proceso y lo no cubierto persiste Política 2025	Julio 2026	Andrés Léniz, Gerente GRC.
1.1	Revisión coherencia Política, Procedimientos y Controles	Septiembre 2026	Roberto Riveros, Gerente General

1.2	Ajuste de gobernanza y tono normativo; separación GRC/CISO; jerarquía documental y aprobación de cambios; excepciones según riesgo; fortalecimiento de arquitectura cloud, desarrollo interno y requisitos de seguridad y resiliencia de proveedores críticos.	Sept. 2026	Gerencia General / Gerencia de GRC
1.3	Revisión formato, preparación para firmas	Sept. 2026	Gestor Documental

Tabla de Aprobación

Versión	Aprobado por	Cargo o Comité	Firma
1.3	Andrés Léniz	Gerente GRC y representante del Comité de Riesgo Operacional y Seguridad	Andrés Léniz
1.3	Roberto Riveros	Gerente General y representante del Directorio de CertiNet	Signed by:Roberto Riveros Signed at:2026-10-09 15:46:31 -03:00 Reason:Witnessing Roberto Riveros Roberto Riveros CertiNet

Contenido

1. Propósito 5
2. Alcance 5
3. Declaración de Compromiso 5
4. Principios Rectores 5
5. Objetivos de Seguridad de la Información 7
6. Gobierno de Seguridad de la Información 7
7. Gestión de Riesgos 9
8. Cumplimiento Legal y Regulatorio 9
9. Concientización y cultura de seguridad 9
10. Gestión de incidentes y continuidad 9
11. Mejora continua 10
12. Marco documental 10
13. Difusión 10
14. Incumplimiento de la Política 10
15. Vigencia y Mejora Continua 11
16. Gestión de Excepciones 11

1. Propósito

Para CertiNet, la seguridad de la información se define como la preservación de la confidencialidad, la integridad y la disponibilidad de los activos corporativos y de los servicios de confianza.

CertiNet reconoce que la información, los datos personales, los activos digitales, las infraestructuras tecnológicas, los certificados electrónicos y los servicios de confianza constituyen activos estratégicos esenciales para el cumplimiento de su misión y la generación de confianza en los negocios digitales.

La presente Política Corporativa de Seguridad de la Información establece el marco de gobierno para el Sistema de Gestión de Seguridad de la Información (SGSI), mediante el cual CertiNet protege la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y resiliencia de la información que administra, procesa, transmite o custodia, garantizando el cumplimiento de los requisitos legales, regulatorios, contractuales y normativos aplicables; para de esta forma mitigar los riesgos asociados.

2. Alcance

Esta política es de cumplimiento obligatorio y aplica a:

- Todo el personal de CertiNet (Directores, ejecutivos y colaboradores).
- Contratistas y terceros que presten servicios a CertiNet.
- Proveedores con acceso a información o activos tecnológicos.
- Sistemas, plataformas, redes, aplicaciones e infraestructura tecnológica.
- Servicios de certificación digital, firma electrónica, identidad digital y confianza.
- Información física y electrónica administrada por CertiNet.

3. Declaración de Compromiso

La Alta Dirección de CertiNet se compromete a proporcionar liderazgo, recursos y apoyo permanente para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) basado en las normas NCh-ISO 27001:2022 e NCh-ISO 27002:2022, así como en la legislación vigente relacionada con firma electrónica, protección de datos personales, protección al consumidor, ciberseguridad y servicios de confianza.

La seguridad de la información es responsabilidad de todos los que participan en los procesos de CertiNet.

4. Principios Rectores

Confianza Digital:
CertiNet desarrollará sus actividades bajo el principio de generación y preservación de confianza digital para clientes, usuarios, organismos reguladores y partes interesadas.

Confidencialidad: La información sólo podrá ser accedida por personas, sistemas o procesos expresamente autorizados.

Integridad: La información deberá mantenerse exacta, completa y protegida contra modificaciones no autorizadas.

Disponibilidad: Los activos de información y servicios críticos deberán encontrarse disponibles cuando sean requeridos por usuarios autorizados.

Autenticidad: Toda información, transacción o identidad digital deberá contar con mecanismos que permitan verificar su origen y legitimidad.

Arquitectura tecnológica y soluciones de seguridad de clase mundial: CertiNet adoptará, como decisión estratégica de diseño y de prestación de sus servicios, una arquitectura tecnológica basada en infraestructura y servicios de Data Center en la nube, sin mantener servidores en Data Center propios.

Las aplicaciones e integraciones que forman parte de los servicios de CertiNet serán desarrolladas o integradas por especialistas de CertiNet, sin contratación de desarrollo externo.

Los proveedores de plataformas y componentes críticos, incluyendo aquellos que soportan la PKI y los servicios de confianza, deberán acreditar niveles de seguridad, resiliencia y cumplimiento reconocidos internacionalmente, considerando, según corresponda, ISO/IEC 27001, NIST, Cyber Resilience Act (CRA), DORA y otros requisitos regulatorios, contractuales o de seguridad aplicables.

Esta definición constituye un principio de arquitectura y abastecimiento tecnológico orientado a sostener la resiliencia, seguridad, trazabilidad y confianza requeridas por los servicios B2B de CertiNet, incluidos aquellos prestados a entidades financieras y otras organizaciones reguladas.

Cumplimiento: CertiNet cumplirá con las leyes, regulaciones, contratos y estándares aplicables a sus actividades.

Gestión Basada en Riesgos: Las decisiones de seguridad deberán fundamentarse en la identificación, evaluación y tratamiento de riesgos.

Mejora Continua: Los controles de seguridad de la información serán evaluados y mejorados de forma permanente para responder a los cambios tecnológicos, regulatorios y de amenazas.

Segregación de Funciones: Se establecerá una estricta separación de funciones y áreas de responsabilidad para todos los procesos críticos de CertiNet. Esto obliga a segregar entornos (ej. desarrollo, pruebas y producción), procesos y autorizaciones conflictivas, con el objetivo de prevenir modificaciones no autorizadas, fraudes o el uso indebido de la información y los activos corporativos.

5. Objetivos de Seguridad de la Información

CertiNet establece los siguientes objetivos corporativos, los cuales serán evaluados, monitoreados y actualizados periódicamente a través de Indicadores Clave de Desempeño (KPIs) definidos formalmente por el Comité de Riesgo Operacional y Seguridad:

- Proteger la información contra accesos no autorizados.
- Mantener la continuidad de los servicios críticos.
- Proteger los datos personales tratados por la organización.
- Preservar la confianza en los servicios de certificación e identidad digital.
- Reducir la exposición a amenazas y vulnerabilidades operativas.
- Cumplir estrictamente con los requisitos legales y regulatorios aplicables.
- Fortalecer la resiliencia operacional y tecnológica.
- Promover una cultura organizacional continua de Seguridad de la Información y Ciberseguridad.

6. Gobierno de Seguridad de la Información

Directorio

- Aprobar la presente política.
- Supervisar el desempeño del SGSI.
- Revisar periódicamente los riesgos estratégicos de seguridad.

Gerencia General

- Asegurar la implementación de esta política.
- Proveer recursos para el SGSI. Promover una cultura de seguridad y cumplimiento.
- Proveer y garantizar el funcionamiento de un canal confidencial y anónimo de denuncias para el reporte seguro de violaciones de seguridad, incidentes, o malas prácticas, protegiendo a los denunciantes de cualquier represalia.

Comité de Riesgo Operacional y Seguridad

- Supervisar la gestión de riesgos de seguridad.
- Revisar incidentes relevantes.
- Proponer mejoras al marco de control.
- Revisar la presente Política.

Gerencia de GRC

- Gobernar y mantener el marco del SGSI, coordinando su planificación, seguimiento y mejora continua.

- Coordinar el proceso corporativo de gestión de riesgos de seguridad de la información, en conjunto con los dueños de riesgo y las áreas responsables.
- Verificar el cumplimiento del marco normativo del SGSI y coordinar auditorías, revisiones, indicadores y planes de mejora.
- Consolidar y reportar al Comité de Riesgo Operacional y Seguridad de la Información el estado de riesgos, cumplimiento, excepciones y acciones de mejora.
- Coordinar la preparación de la información de desempeño del SGSI que corresponda elevar a la Alta Dirección y al Directorio.

Oficial de Seguridad de la Información (CISO)

- Definir los requisitos y criterios especializados de seguridad de la información y ciberseguridad aplicables a los activos, servicios y tecnologías de CertiNet.
- Supervisar la implementación y efectividad de los controles de seguridad, manteniendo independencia respecto de su ejecución operativa cuando corresponda.
- Evaluar riesgos, vulnerabilidades, incidentes y excepciones desde la perspectiva técnica y de seguridad, proponiendo medidas de tratamiento y escalamiento.
- Coordinar la respuesta especializada de seguridad y ciberseguridad conforme a las políticas y procedimientos aplicables.
- Informar oportunamente a la Gerencia de GRC y al Comité sobre riesgos, incidentes y materias de seguridad que requieran decisión, seguimiento o aceptación de riesgo.

Propietarios o Dueños del Riesgo

- Asumir la responsabilidad formal por los riesgos identificados en sus respectivas áreas de competencia. Aprobar los planes de tratamiento de riesgos y aceptar formalmente los riesgos operativos residuales de sus procesos.

Colaboradores y Terceros

- Cumplir con las políticas y procedimientos de Seguridad de la Información establecidos, suscribiendo obligatoriamente un acuse de recibo formal y/o una toma de conocimiento de la presente Política y sus futuras actualizaciones.
- Proteger la información bajo su responsabilidad.
- Reportar incidentes, vulnerabilidades o incumplimientos (utilizando el canal de denuncias anónimo dispuesto por la Alta Dirección, cuando corresponda).

Delegación y Competencia de Roles

Todo individuo con responsabilidades de seguridad de la información asignadas podrá delegar tareas específicas cuando sea necesario, pero retendrá en todo momento la

responsabilidad final y deberá validar la correcta ejecución de las labores delegadas. Asimismo, la organización garantizará que las personas que asumen roles específicos en materia de seguridad cuenten con la competencia técnica requerida y reciban el apoyo continuo necesario para mantener actualizados sus conocimientos y habilidades frente al entorno de amenazas.

7. Gestión de Riesgos

CertiNet implementará un proceso permanente de identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos que puedan afectar los activos de información, los servicios de confianza digital y la continuidad operacional.

Los controles de seguridad de la información se definirán de acuerdo con el nivel de riesgo identificado y el apetito de riesgo aprobado por la organización.

8. Cumplimiento Legal y Regulatorio

CertiNet cuidará del estricto cumplimiento de la legislación y normativa vigentes en materia de Seguridad de la Información, Ciberseguridad, Protección de Datos Personales, firma electrónica y servicios de confianza digital, así como de los estándares internacionales adoptados por la organización (tales como la familia ISO/IEC 27000 y la continuidad del negocio) y de los demás requisitos legales, contractuales y regulatorios aplicables.

9. Concientización y cultura de seguridad

CertiNet promoverá una cultura de seguridad de la información mediante programas permanentes de capacitación, difusión y sensibilización orientados a fortalecer el comportamiento seguro de colaboradores, contratistas y terceros.

10. Gestión de incidentes y continuidad

Todo incidente de seguridad deberá ser reportado, gestionado y documentado conforme a los procedimientos internos establecidos. Adicionalmente, en consideración a la naturaleza crítica de los servicios de CertiNet como Prestador de Servicios de Certificación acreditado por el MMEE y a su rol como Operador de Importancia Vital (OIV) o figura equivalente bajo la legislación de ciberseguridad vigente, la organización garantizará el reporte oportuno y obligatorio de los incidentes que correspondan ante la Agencia Nacional de Ciberseguridad (o la autoridad sectorial competente) dentro de los plazos normativos estipulados.

CertiNet mantendrá planes de continuidad del negocio y de recuperación ante desastres que aseguren la resiliencia de sus servicios críticos y la protección de los activos de información frente a interrupciones de mayor magnitud.

11. Mejora continua

El SGSI será revisado periódicamente mediante auditorías, revisiones de la dirección, análisis de riesgos, indicadores de desempeño y procesos de mejora continua.

12. Marco documental

La presente Política Corporativa constituye el nivel superior del marco documental de seguridad de la información de CertiNet. Sus principios y obligaciones se despliegan mediante políticas específicas, procedimientos y planes, instructivos y estándares técnicos, y los registros y evidencias que acreditan su ejecución.

La jerarquía documental será, en consecuencia: Política Corporativa de Seguridad de la Información; políticas específicas del SGSI; procedimientos y planes; instructivos y estándares técnicos; y registros y evidencias.

Los documentos subordinados deberán mantener coherencia con esta Política y no podrán modificar ni reducir sus principios, obligaciones o responsabilidades.

La Gerencia de GRC coordinará la consistencia y actualización del marco documental, con participación del CISO y de las áreas responsables según la materia.

Las políticas específicas serán aprobadas conforme al esquema de gobierno documental vigente; los procedimientos, planes, instructivos y estándares serán aprobados por la autoridad competente definida para cada tipo documental.

13. Difusión

El presente documento estará disponible para todo el personal y partes interesadas pertinentes de forma accesible y comprensible. Las áreas emisoras, en coordinación con el Oficial de Seguridad de la Información (CISO), gestionarán su difusión a través de los canales institucionales. Será obligatorio el registro formal del acuse de recibo por parte de los colaboradores, terceros y cualquier parte interesada relevante, quienes deberán confirmar expresamente que comprenden las directrices de la política y asumen el compromiso de cumplirlas.

14. Incumplimiento de la Política

El incumplimiento de esta Política resultará en la aplicación de medidas disciplinarias, conforme a lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad de CertiNet y los contratos vigentes. Lo anterior es sin perjuicio de las responsabilidades civiles, patrimoniales o penales conforme a las leyes aplicables.

15. Vigencia y Mejora Continua

La presente Política Corporativa de Seguridad de la Información y sus modificaciones materiales deberán ser aprobadas por el Directorio de CertiNet. La Política será revisada al menos una vez al año, o antes cuando se produzcan cambios significativos en el negocio, la tecnología, la regulación, los servicios o el contexto de riesgos. El Comité de Riesgo Operacional y Seguridad de la Información de la Información revisará la propuesta de actualización y formulará las recomendaciones que correspondan antes de su elevación al Directorio. La Gerencia de GRC coordinará el proceso de revisión y mantendrá la trazabilidad de los cambios aprobados.

16. Gestión de Excepciones

Toda desviación o excepción temporal a esta Política o al SGSI deberá solicitarse formalmente, con justificación, evaluación de riesgo, controles compensatorios cuando correspondan, responsable y vigencia. GRC mantendrá su registro y seguimiento; el CISO emitirá la evaluación especializada de seguridad cuando corresponda. La aprobación se realizará según el riesgo y las atribuciones vigentes. Las excepciones de riesgo alto, que afecten servicios críticos o impliquen una desviación material deberán elevarse al Comité y, cuando corresponda, al Directorio. Ninguna excepción podrá eludir obligaciones legales o regulatorias.