Política de Relación con Proveedores

Versión 01

Tabla de Contenido

1. OBJETIVO

Establecer los principios y lineamientos para la gestión segura, controlada y basada en riesgo de las relaciones con proveedores, contratistas y terceros que suministren bienes o servicios a CELUWEB y que puedan tener acceso a información, sistemas, infraestructura o procesos críticos, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y mitigar riesgos asociados a la cadena de suministro.

2. ALCANCE

La presente política aplica a:

- Todos los proveedores y terceros que suministren bienes o servicios a CELUWEB.
- Proveedores que tengan acceso lógico o físico a instalaciones, activos de información o datos personales.
- Proveedores críticos para la operación, continuidad del negocio o seguridad de la información.
- Contratistas, subcontratistas y aliados estratégicos.

3. DEFINICIONES

Seguridad de la Información: Protección de la información para preservar su confidencialidad, integridad y disponibilidad. (Referencia: ISO/IEC 27000:2018).

SGSI: Sistema de Gestión de Seguridad de la Información, conjunto de políticas, procesos, procedimientos y controles para gestionar los riesgos de seguridad de la información. (Referencia: ISO/IEC 27000:2018).

Activo de Información: Información o elemento asociado que tiene valor para la organización. (Referencia: ISO/IEC 27000:2018).

Confidencialidad: Propiedad que asegura que la información solo sea accesible a personas autorizadas. (Referencia: ISO/IEC 27000:2018).

Integridad: Propiedad que salvaguarda la exactitud y completitud de la información. (Referencia: ISO/IEC 27000:2018).

Disponibilidad: Propiedad que garantiza que la información esté accesible y utilizable cuando se requiera. (Referencia: ISO/IEC 27000:2018).

Proveedor: Persona natural o jurídica que suministra bienes o servicios a la organización bajo un acuerdo contractual. (Referencia: ISO/IEC 27002:2022).

Tercero: Entidad externa que interactúa con la organización y que puede tener acceso a información, activos o servicios. (Referencia: ISO/IEC 27002:2022).

Relación con Proveedores: Acuerdo formal mediante el cual un proveedor suministra productos o servicios y puede estar sujeto a requisitos de seguridad de la información. (Referencia: ISO/IEC 27002:2022).

Riesgo de Terceros: Riesgo derivado del acceso o dependencia de proveedores que puede impactar la seguridad, disponibilidad o cumplimiento regulatorio de la organización. (Referencia: NIST SP 800-53).

Proveedor Crítico: Proveedor cuyo producto o servicio es esencial para la operación, continuidad o seguridad de la organización. (Referencia: ISO 22301 / ISO 27001 enfoque basado en riesgo).

Acuerdo de Nivel de Servicio (SLA): Documento que establece niveles de desempeño, disponibilidad y responsabilidades entre la organización y el proveedor. (Referencia: Buenas prácticas de gestión de servicios – alineado con ISO/IEC 20000).

Acuerdo de Confidencialidad (NDA): Compromiso contractual que obliga a las partes a proteger la información confidencial compartida. (Referencia: ISO/IEC 27002:2022).

Cadena de Suministro: Conjunto de organizaciones, personas, procesos y recursos involucrados en la provisión de bienes o servicios. (Referencia: ISO 28000).

4. ROLES Y RESPONSABILIDADES

4.1. Alta Dirección

- Asegurar recursos para su implementación.
- Aceptar riesgos residuales asociados a proveedores críticos cuando aplique.

4.2. CISO

- Definir los requisitos mínimos de seguridad que deben cumplir los proveedores.
- Participar en la evaluación de riesgos de terceros.
- Validar cláusulas de seguridad en contratos.
- Monitorear cumplimiento de requisitos de seguridad.
- Autorizar excepciones justificadas.

4.3. Administrativa y Financiera

- Garantizar que todo proveedor pase por proceso de evaluación antes de contratación.
- Incluir cláusulas contractuales obligatorias de seguridad.
- Mantener inventario actualizado de proveedores.

4.4. Dueño del Servicio

- Justificar la necesidad del proveedor.
- Clasificar la criticidad del servicio contratado.
- Supervisar cumplimiento operativo del proveedor.

4.5. Infraestructura / Tecnología

- Validar controles técnicos cuando el proveedor tenga acceso a sistemas.
- Supervisar accesos otorgados a proveedores.
- Revocar accesos al finalizar la relación contractual.

4.6. Proveedores y Terceros

- Cumplir con los requisitos de seguridad establecidos por CELUWEB.
- Proteger la información recibida.
- Notificar incidentes de seguridad.
- Cumplir con la presente política y obligaciones contractuales y regulatorias aplicables.

5. CONDICIONES GENERALES

La relación con proveedores constituye un componente estratégico del Sistema de Gestión de Seguridad de la Información (SGSI) y deberá gestionarse bajo un enfoque integral de riesgos.

Todo proveedor será considerado una extensión del entorno de riesgo de CELUWEB cuando tenga acceso a información, sistemas, infraestructura, procesos críticos o datos personales.

La gestión de proveedores deberá abarcar el ciclo completo de la relación contractual, desde la evaluación inicial hasta su terminación o renovación.

La clasificación de proveedores deberá realizarse considerando la criticidad del servicio, el nivel de acceso a información y el impacto potencial en la operación.

CELUWEB mantendrá un inventario actualizado de proveedores que identifique su nivel de criticidad y riesgos asociados.

Las relaciones con proveedores deberán formalizarse mediante acuerdos contractuales que incluyan obligaciones en materia de seguridad de la información.

La subcontratación por parte de los proveedores no podrá generar pérdida de control sobre los requisitos de seguridad definidos por CELUWEB.

La terminación de la relación con proveedores deberá contemplar controles que aseguren la devolución o eliminación segura de información.

La seguridad en la relación con proveedores deberá alinearse con las obligaciones legales, regulatorias, contractuales y de protección de datos aplicables.

5.1. Clasificación de proveedores

Proveedores de servicio estandarizado por adhesión: (Cloud hyperscalers, SaaS globales, multinacionales con términos unilaterales) Ejemplo: AWS, Microsoft 365, Google.

Proveedores contractuales directos: Con contrato negociado y relación directa Ejemplo: contratistas, proveedor local de software.

5.2. Revisión y actualización

Esta política será revisada anualmente y actualizada cuando existan cambios significativos en el negocio, el entorno tecnológico o los requisitos aplicables.

5.3. Marco sancionatorio

El incumplimiento de la presente política y de las demás políticas, procedimientos y controles del Sistema de Gestión de Seguridad de la Información (SGSI) será considerado una falta al marco de seguridad de la información de CELUWEB y podrá dar lugar a la aplicación de medidas disciplinarias, contractuales o legales, según la gravedad del caso, sin perjuicio de las acciones civiles o penales a que haya lugar, conforme a la normativa interna y la legislación vigente.

6. LINEAMIENTOS

6.1. Declaración de la Política

Todo proveedor deberá ser evaluado antes de su contratación mediante un proceso formal de debida diligencia.

Los proveedores que traten información confidencial o datos personales deberán demostrar cumplimiento de normativas aplicables.

La criticidad del proveedor deberá clasificarse como ALTA, MEDIA o BAJA según impacto en confidencialidad, integridad y disponibilidad.

Los proveedores que brinden sus servicios a la compañía deberán contar con certificaciones vigentes relativas a la seguridad de la información, o bien, implementar buenas prácticas basadas en la norma ISO 27001, aplicadas a los servicios y/o productos contratados por CELUWEB.

6.1.1. Requisitos Contractuales de Seguridad

los proveedores, contratistas y terceros que tenga cualquier tipo de acceso a información de CELUWEB deberán firmar acuerdos de confidencialidad.

los proveedores, contratistas y terceros deberán notificar inmediatamente los incidentes de seguridad que afecten la información de CELUWEB, al correo gestionsi@celuweb.com .

El proveedor deberá facilitar la información necesaria para investigaciones relacionadas con incidentes de seguridad.

6.1.2. Control de Accesos de Proveedores

El acceso a sistemas por parte de proveedores deberá otorgarse bajo el principio de mínimo privilegio, y no podrá compartir, transferir ni delegar credenciales de acceso.

Los accesos privilegiados para proveedores deberán estar justificados y aprobados formalmente.

Los accesos que CELUWEB le otorgue a proveedores, contratistas y terceros deberá utilizarse exclusivamente para la ejecución del servicio contratado.

Toda visita a las instalaciones de CELUWEB deberá ser notificada previamente y contar con autorización formal del responsable del servicio contratado.

El proveedor deberá cumplir estrictamente los protocolos de seguridad física establecidos por CELUWEB.

Se prohíbe tomar fotografías, grabaciones o capturar información dentro de las instalaciones de CELUWEB, sin autorización expresa.

Los equipos de computo o medio de almacenamiento que se pretenda ingresar a las instalaciones de CELUWEB por parte de proveedores, terceros o contratistas; deberá ser reportado previamente.

Al finalizar la visita, el proveedor deberá registrar su salida conforme a los controles establecidos.

Los accesos deberán revocarse inmediatamente al finalizar la relación contractual con el proveedor.

6.1.3. Monitoreo y Supervisión

Todos los proveedores, contratistas y terceros deberán permitir auditorías o verificaciones de seguridad de la información, cuando contractualmente se haya establecido dicho derecho.

Se deberán evaluar periódicamente los niveles de servicio y cumplimiento de acuerdos (SLA).

6.1.4. Subcontratación

El proveedor no podrá subcontratar servicios relacionados con información confidencial o datos personales sin autorización formal de CELUWEB.

En caso de subcontratación autorizada, el proveedor deberá garantizar que el subcontratista cumpla exactamente los mismos requisitos de seguridad aquí definidos.

6.1.5. Protección de Datos Personales

Los proveedores que traten datos personales por cuenta de CELUWEB, deberá cumplir la normativa de protección de datos aplicable.

No se permitirá transferencia internacional de datos sin validación previa por parte de CELUWEB.

6.1.6. Continuidad del Negocio

Los proveedores críticos deberán contar con planes de continuidad documentados.

Cuando aplique, deberán presentar evidencia de pruebas de continuidad.

Los proveedores deberán notificar interrupciones que puedan afectar la disponibilidad del servicio contratado.

6.1.7. Gestión de vulnerabilidades

CELUWEB solicitará a los proveedores de plataformas o servicios tecnológicos, un certificado de ejecución de análisis de vulnerabilidades, como mínimo una vez al

año, así como un plan de trabajo en caso de presentarse hallazgos de nivel alto o crítico.

6.1.8. Seguridad en Servicios Cloud

Los proveedores de servicios en la nube deberán proporcionar garantías de cumplimiento en materia de seguridad.

Se deberá validar ubicación de datos y modelo de responsabilidad compartida.

6.1.9. Transferencia de Información

No se permitirá el intercambio de información fuera del alcance del contrato o sin justificación del servicio contratado.

La información deberá transferirse únicamente a través de canales seguros autorizados por CELUWEB.

Cuando la información sea confidencial o se trate de datos personales, deberá utilizarse cifrado u otros mecanismos de protección adecuados durante la transmisión.

Se prohíbe el envío de información sensible mediante canales no autorizados o inseguros.

El proveedor deberá limitar el acceso a la información recibida únicamente a personal autorizado y que participe directamente en la ejecución del servicio.

El proveedor no podrá usar la información transferida para fines distintos a los autorizados contractualmente.

El proveedor no podrá compartir, vender, divulgar o reutilizar la información transferida sin autorización previa y escrita de CELUWEB.

6.1.10. Gestión de Cambios para proveedores de servicio estandarizado por adhesión

Cuando el proveedor opere bajo modelo de adhesión y no permita autorización previa de cambios por parte de CELUWEB, este deberá garantizar la notificación oportuna de cambios relevantes que puedan impactar la seguridad, disponibilidad o integridad del servicio.

CELUWEB deberá monitorear los canales oficiales de comunicación del proveedor para mantenerse informada sobre:

- Cambios en arquitectura del servicio.

- Actualizaciones relevantes.
- Modificaciones en condiciones de seguridad.
- Incidentes que puedan afectar la prestación del servicio.

6.1.11. Gestión de Cambios para proveedores contractuales directos

Todo cambio significativo que pueda impactar la seguridad, disponibilidad, arquitectura, configuración o tratamiento de información deberá ser notificado previamente a CELUWEB.

Los cambios críticos requerirán validación formal antes de su implementación cuando así se haya establecido contractualmente.

El proveedor deberá informar posterior a la ejecución:

- Resultado del cambio.
- Incidentes asociados.
- Confirmación de estabilidad del servicio.

Los cambios deberán contar con análisis de impacto y plan de reversión.

CELUWEB podrá solicitar evidencia técnica del proceso de cambio cuando el nivel de riesgo lo requiera.

6.1.12. Terminación de la Relación

A la finalización del contrato, el proveedor deberá devolver o eliminar la información de manera segura, certificando por escrito la ejecución de dicha actividad, cuando así se solicite.

Una vez finalizada la relación contractual con el proveedor, contratista o tercero, se deberán revocar accesos tanto físicos como lógicos.

6.1.13. Aceptación de Riesgo y Cumplimiento

Cualquier desviación a estos requisitos deberá contar con aprobación formal y documentada de CELUWEB.

El incumplimiento de estos lineamientos podrá dar lugar a las acciones contractuales, civiles o legales que correspondan.

7. ANEXOS

N/A

8. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Responsable
V01	24/03/2026	Creación del documento	CISO

9. APROBACIÓN

Elaboró	Revisó	Aprobó
Angie Melissa Correa CISO	Mónica Martínez Patiño Gerente Administrativa y Financiera Paola Andrea Ossa Coordinadora de Talento Humano y SST	Mónica Martínez Patiño Gerente Administrativa y Financiera