




**Política de Seguridad de la Información con
Proveedores**

Forestal Collicura Limitada

Versión 1.0	Política de Seguridad de la Información con Proveedores	
-------------	---	---

Información del documento

Versión	Fecha de Creación		Descripción
1.0	28-07-2023		Creación y primera versión del documento.

(*) La última versión sustituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los efectos.



Versión 1.0	Política de Seguridad de la Información con Proveedores	
-------------	---	---

Tabla de contenidos

1. Introducción	4
2. Objetivo	4
3. Alcance	4
4. Definiciones	5
5. Política	5
5.1 Relación con proveedores	5
5.2 Requisitos de seguridad en contratos con proveedores	6
5.3 Cadena de suministro	6
5.4 Gestión de la provisión de servicios del proveedor	7
5.5 Criterios para determinar el nivel de criticidad de la actividad externalizada	7
5.6 Requisitos que deben cumplir los proveedores críticos	8
6. Responsabilidades	8
7. Documentación de referencia	9

Versión 1.0	Política de Seguridad de la Información con Proveedores	
-------------	---	---

1. Introducción


Cómo parte del control de los aspectos relacionados con los proveedores de **FORESTAL COLLICURA LIMITADA**, es fundamental tener un registro, control y procesos de gestión sobre todos los proveedores, principalmente sobre los que puedan tener acceso a nuestra información y forman parte de nuestra cadena crítica de suministro. Este control no sólo debe realizarse desde la óptica técnica sino que también bajo todos los aspectos jurídicos necesarios que considere **FORESTAL COLLICURA LIMITADA** para asegurar la disponibilidad, integridad y confidencialidad de la data que es de su responsabilidad.

2. Objetivo

Definir los lineamientos y requisitos de Seguridad de la Información en la relación con proveedores con el fin de asegurar la protección de los activos de **FORESTAL COLLICURA LIMITADA** y mantener el nivel acordado de la provisión de servicios.

3. Alcance

Esta política es aplicable a todas las áreas que participen directa o indirectamente en procesos relacionados con proveedores, tanto en lo relacionado con los contratos, control de Riesgos de la **FORESTAL COLLICURA LIMITADA**, pagos y accesos técnicos a los diferentes repositorios.

Versión 1.0	Política de Seguridad de la Información con Proveedores	
-------------	---	---

4. Definiciones

Cadena de suministro: Conjunto de elementos que le permite a **FORESTAL COLLICURA LIMITADA** contar con la organización necesaria para llevar a cabo el desarrollo de un producto o servicio y que este cumpla el objetivo principal que es satisfacer las necesidades del cliente final.

Proveedor crítico: Es todo aquel proveedor que proporciona a **FORESTAL COLLICURA LIMITADA** un servicio crítico, el cual podría ser también efectuado internamente por la entidad, con sus propios recursos, tanto humanos como tecnológicos.


Proveedor relevante: Es todo aquel proveedor que frente a una falla en sus servicios, afecta indirectamente o de forma parcial la continuidad operacional, así mismo puede afectar la imagen, legal, normativo o seguridad de la información de **FORESTAL COLLICURA LIMITADA**.

5. Política

5.1 Relación con proveedores

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de **FORESTAL COLLICURA LIMITADA** deben acordarse con el proveedor y quedar documentados:

- Se deben identificar, documentar y clasificar según criticidad todos los proveedores de **FORESTAL COLLICURA LIMITADA**, ya sean de servicios de TI, logística, servicios financieros, componentes de infraestructura TI, etc.
- Se debe definir los tipos de acceso a la información que se permitirá a los diferentes tipos de proveedores, con su supervisión y su control del acceso.


Versión 1.0	Política de Seguridad de la Información con Proveedores	
-------------	---	---

- Se deben definir los diferentes tipos de obligaciones que sean aplicables a los proveedores para proteger la información de **FORESTAL COLLICURA LIMITADA**.
- Evaluar y comparar de forma periódica el rendimiento de proveedores vigentes y alternativos para identificar oportunidades o una necesidad apremiante de reconsideración de los contratos de los proveedores actuales.

5.2 Requisitos de seguridad en contratos con proveedores

Se deben considerar los siguientes aspectos para su inclusión en los acuerdos con el fin de satisfacer los requisitos de seguridad de la información identificados:

- Los requisitos legales y regulatorios, incluyendo la protección de datos personales, los derechos de propiedad intelectual y derechos de autor, y una descripción de cómo se garantizará que se cumplen.
- Definir los acuerdos de nivel de servicio (S.L.A)
- La obligación contractual de cada parte para implementar un conjunto acordado de controles incluyendo el control de acceso, la evaluación del desempeño, la supervisión, los informes y la auditoría.
- Requisitos y procedimientos de gestión de incidentes (en especial de notificación y colaboración durante la corrección de los incidentes).
- Los reglamentos pertinentes para la subcontratación, incluidos los controles que necesitan ser implantados.
- Acuerdos pertinentes de colaboración, incluyendo una persona de contacto de ambas partes.
- Derecho de auditar los procesos de los proveedores y los controles relacionados con el acuerdo.
- Las obligaciones de los proveedores para cumplir con los requisitos de seguridad de **FORESTAL COLLICURA LIMITADA**.

Versión 1.0	Política de Seguridad de la Información con Proveedores	
-------------	---	---


5.3 Cadena de suministro

- Para los servicios y productos de infraestructura tecnológica se requiere que los proveedores reproduzcan los requisitos de seguridad a lo largo de su cadena de suministro, si los proveedores subcontratan parte de los servicios o productos a otros proveedores.
- Se deben identificar los productos críticos ofrecidos por los proveedores, con el fin de mantener un stock que permita asegurar la continuidad del servicio y operaciones.
- El origen de los componentes o productos críticos se debe poder trazar a lo largo de la cadena de suministro.
- Deben existir procedimientos y se deben considerar los riesgos de seguridad de la información, y principalmente de problemas de disponibilidad en la entrega de productos o servicios por un proveedor crítico, cualquiera que sea el motivo.

5.4 Gestión de la provisión de servicios del proveedor

Se debe incluir un proceso de gestión del servicio entre **FORESTAL COLLICURA LIMITADA** y el proveedor para:

- Supervisar los niveles de rendimiento del servicio para verificar el cumplimiento de los acuerdos.
- Revisar los informes del servicio producidos por el proveedor y organizar reuniones periódicas de progreso según sea requerido en los acuerdos.
- Asegurar que el proveedor mantenga la capacidad de servicio suficiente, junto con planes viables destinados a garantizar que los niveles de continuidad de servicio acordados se mantengan después de fallos mayores de los servicios o de desastre.

Versión 1.0	Política de Seguridad de la Información con Proveedores	
-------------	---	---


5.5 Criterios para determinar el nivel de criticidad de la actividad externalizada

- Grado de impacto de una falla del proveedor en la provisión o ejecución del servicio en las siguientes variables:
 - Financiera.
 - Reputacional.
 - Legal.
 - Continuidad del Negocio.
 - Seguridad de la Información.
 - Cumplimiento Normativo.

5.6 Requisitos que deben cumplir los proveedores críticos

- Grado de dificultad y tiempo necesario para seleccionar un proveedor alternativo de servicios o de llevar la actividad empresarial internamente, en caso que el proveedor no preste un servicio adecuado.
- Verificar si la actividad externalizada debe necesariamente procesar información en instalaciones y equipos propios del proveedor.
- Contar con un plan de continuidad del negocio, que incluya un plan de recuperación de desastres y efectuar pruebas periódicas.
- Contar con una adecuada capacidad financiera.
- Contar con la capacidad técnica necesaria para desempeñar satisfactoriamente las actividades externalizadas.
- Contar con las certificaciones que correspondan a los procesos donde ellos intervienen (Ejemplo PCI, ISO 27001)

6. Responsabilidades

Versión 1.0	Política de Seguridad de la Información con Proveedores	
-------------	---	---

Cargo responsable por el proveedor:

- Es el cargo más alto relacionado con los Servicios de Información de **FORESTAL COLLICURA LIMITADA**, a cargo de evaluar antes de la contratación y también en forma periódica, el grado de adecuación o capacidad del proveedor para la entrega de su servicio, solicitando las evidencias necesarias para certificar cada uno de los aspectos evaluados.
- Monitorear el adecuado cumplimiento de los acuerdos de niveles de servicio definidos por contrato con el proveedor.
- Definir planes de acción para aquellos proveedores que presenten debilidades de carácter no crítico al momento de la contratación o en las evaluaciones futuras que se realicen al proveedor.
- Comunicar oportunamente la necesidad de externalizar un servicio, entregando información que sirva de análisis al área de Ciberseguridad.

Área de ciberseguridad:

- Encargada de definir los lineamientos de seguridad de la información y de actualizar y velar por el cumplimiento de esta política.
- Apoyar en la evaluación del grado de criticidad del servicio, así como también, de la capacidad del proveedor para la entrega del servicio.
- Monitorear el cumplimiento de los planes de acción definidos para los proveedores críticos que presentan debilidades al momento de la contratación o durante el periodo de vigencia del contrato.

7. Documentación de referencia

- Código de prácticas para los controles de seguridad de la información (ISO/IEC 27002:2013)
- Marco de Referencia COBIT 2019: Objetivos de gobierno y gestión.