



## Programa de Integridad y Compliance

**TechBackup SpA, RUT 77.171.331-9**

**Dirección: Diego Portales N° 860, comuna de Puerto Montt**

**Oficial de Cumplimiento Mathias Alfonso Barria Alarcón. Rut: 19.541.153-0**



## Tabla de contenido

|                                                                     |           |
|---------------------------------------------------------------------|-----------|
| Programa de Integridad y Compliance                                 | 1         |
| <b><i>CARTA DE COMPROMISO DE LA ALTA DIRECCIÓN</i></b>              | <b>5</b>  |
| 1. Compromiso institucional                                         | 5         |
| 2. Marco normativo aplicable                                        | 5         |
| 3. Alcance y obligatoriedad                                         | 6         |
| 4. Designación del Oficial de Cumplimiento                          | 6         |
| 5. Recursos y autoridad                                             | 6         |
| 6. Tolerancia cero frente a infracciones                            | 7         |
| 7. Vigencia y revisión                                              | 7         |
| <b><i>CAPÍTULO 1</i></b>                                            | <b>8</b>  |
| <b>PRESENTACIÓN DEL PROGRAMA DE INTEGRIDAD Y CUMPLIMIENTO</b>       | <b>8</b>  |
| 1.1 Contexto general                                                | 8         |
| 1.2 Naturaleza del Programa                                         | 8         |
| 1.3 Objetivo general                                                | 9         |
| 1.4 Objetivos específicos                                           | 9         |
| 1.5 Alcance del Programa                                            | 9         |
| 1.6 Integración con la gestión de la empresa                        | 10        |
| <b><i>CAPÍTULO 2</i></b>                                            | <b>10</b> |
| <b>MARCO NORMATIVO Y ESTÁNDARES DE REFERENCIA</b>                   | <b>10</b> |
| 2.1 Principio de legalidad y cumplimiento normativo                 | 10        |
| 2.2 Ley N° 19.886 y su reglamento                                   | 11        |
| 2.3 Ley N° 20.393 - Responsabilidad penal de las personas jurídicas | 11        |
| 2.4 Ley N° 18.575 - Bases Generales de la Administración del Estado | 12        |
| 2.5 Ley N° 21.121                                                   | 12        |
| 2.6 Estrategia Nacional de Integridad Pública                       | 12        |
| 2.7 Estándares internacionales ISO                                  | 12        |
| <b><i>CAPÍTULO 3</i></b>                                            | <b>13</b> |
| <b>GOBIERNO CORPORATIVO, ROLES Y RESPONSABILIDADES</b>              | <b>13</b> |
| 3.1 Principios de gobierno del Programa de Integridad               | 13        |
| 3.2 Responsabilidad de la Alta Dirección                            | 13        |
| 3.3 Oficial de Cumplimiento Interno                                 | 14        |
| 3.4 Funciones del Oficial de Cumplimiento                           | 14        |
| 3.5 Apoyo externo MAXING                                            | 14        |
| 3.6 Deberes de trabajadores y terceros                              | 15        |
| <b><i>CAPÍTULO 4</i></b>                                            | <b>15</b> |
| <b>POLÍTICAS DE INTEGRIDAD, ÉTICA Y CONDUCTA EMPRESARIAL</b>        | <b>15</b> |
| 4.1 Principios generales de conducta                                | 15        |
| 4.2 Cumplimiento normativo obligatorio                              | 16        |

|                                        |    |
|----------------------------------------|----|
| 4.3 Prohibición de conductas indebidas | 16 |
| 4.4 Conflictos de interés              | 16 |
| 4.5 Relación con el sector público     | 17 |
| 4.6 Régimen disciplinario              | 17 |

## ***CAPÍTULO 5*** **18**

### **IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS DE INTEGRIDAD Y CUMPLIMIENTO** **18**

|                                                       |    |
|-------------------------------------------------------|----|
| 5.1 Enfoque basado en riesgos                         | 18 |
| 5.2 Objetivo del proceso de identificación de riesgos | 18 |
| 5.3 Alcance del análisis de riesgos                   | 18 |
| 5.4 Metodología de evaluación                         | 19 |
| 5.5 Responsabilidad del proceso                       | 19 |
| 5.6 Actualización de riesgos                          | 19 |

## ***CAPÍTULO 6*** **20**

### **MEDIDAS DE PREVENCIÓN, CONTROL Y MITIGACIÓN** **20**

|                                                 |    |
|-------------------------------------------------|----|
| 6.1 Principio de proporcionalidad y efectividad | 20 |
| 6.2 Tipos de controles implementados            | 20 |
| 6.3 Políticas y procedimientos formales         | 20 |
| 6.4 Controles en procesos críticos              | 21 |
| 6.5 Registro y evidencia documental             | 21 |
| 6.6 Rol del Oficial de Cumplimiento             | 21 |

## ***CAPÍTULO 7*** **22**

### **CANAL DE DENUNCIAS Y PROTECCIÓN AL DENUNCIANTE** **22**

|                                              |    |
|----------------------------------------------|----|
| 7.1 Principio general                        | 22 |
| 7.2 Alcance del Canal de Denuncias           | 22 |
| 7.3 Sujetos habilitados para denunciar       | 22 |
| 7.4 Modalidad del Canal de Denuncias         | 23 |
| 7.5 Protección al denunciante                | 23 |
| 7.6 Confidencialidad y uso de la información | 23 |
| 7.7 Registro y trazabilidad                  | 23 |

## ***CAPÍTULO 8*** **24**

### **INVESTIGACIÓN INTERNA Y GESTIÓN DE INCIDENTES** **24**

|                                          |    |
|------------------------------------------|----|
| 8.1 Principio de debida diligencia       | 24 |
| 8.2 Inicio de la investigación           | 24 |
| 8.3 Responsable de la investigación      | 25 |
| 8.4 Etapas del proceso de investigación  | 25 |
| 8.5 Medidas correctivas y disciplinarias | 25 |
| 8.6 Cierre del caso y documentación      | 26 |
| 8.7 Aprendizaje organizacional           | 26 |

## ***CAPÍTULO 9*** **27**

### **CAPACITACIÓN Y COMUNICACIÓN DEL PROGRAMA DE INTEGRIDAD** **27**

|                                      |    |
|--------------------------------------|----|
| 9.1 Principio general                | 27 |
| 9.2 Objetivos de la capacitación     | 27 |
| 9.3 Sujetos obligados a capacitación | 27 |

|                                                                |           |
|----------------------------------------------------------------|-----------|
| 9.4 Modalidades de capacitación                                | 28        |
| 9.5 Contenidos mínimos                                         | 28        |
| 9.6 Registro y evidencia                                       | 28        |
| 9.7 Comunicación del Programa                                  | 29        |
| <b>CAPÍTULO 10</b>                                             | <b>29</b> |
| <b>MONITOREO, SUPERVISIÓN Y MEJORA CONTINUA</b>                | <b>29</b> |
| 10.1 Principio de mejora continua                              | 29        |
| 10.2 Monitoreo del Programa                                    | 29        |
| 10.3 Responsable del monitoreo                                 | 30        |
| 10.4 Herramientas de supervisión                               | 30        |
| 10.5 Gestión de hallazgos                                      | 30        |
| 10.6 Actualización del Programa                                | 30        |
| 10.7 Evidencia y demostrabilidad                               | 31        |
| <b>CAPÍTULO 11</b>                                             | <b>32</b> |
| <b>RÉGIMEN DE SANCIONES Y CONSECUENCIAS DEL INCUMPLIMIENTO</b> | <b>32</b> |
| 11.1 Principio de responsabilidad                              | 32        |
| 11.2 Sujetos sujetos a sanción                                 | 32        |
| 11.3 Tipos de infracciones                                     | 33        |
| 11.4 Medidas disciplinarias internas                           | 33        |
| 11.5 Denuncia a autoridades competentes                        | 33        |
| 11.6 Registro y trazabilidad sancionatoria                     | 34        |
| <b>CAPÍTULO 12</b>                                             | <b>34</b> |
| <b>MATRIZ DE RIESGOS DE INTEGRIDAD Y CUMPLIMIENTO</b>          | <b>34</b> |
| 12.1 Rol estructural de la Matriz de Riesgos                   | 34        |
| 12.2 Objetivo de la Matriz de Riesgos                          | 34        |
| 12.3 Metodología aplicada                                      | 35        |
| 12.4 Riesgos críticos considerados                             | 35        |
| 12.5 Ejemplo estructural de matriz (referencial)               | 36        |
| 12.6 Actualización y revisión                                  | 36        |
| <b>CAPÍTULO 13</b>                                             | <b>37</b> |
| <b>VIGENCIA, APROBACIÓN, DIFUSIÓN Y COMPROMISO FINAL</b>       | <b>37</b> |
| 13.1 Aprobación formal del Programa de Integridad              | 37        |
| 13.2 Vigencia del Programa                                     | 37        |
| 13.3 Obligatoriedad y alcance final                            | 37        |
| 13.4 Difusión interna y comunicación                           | 38        |
| 13.5 Compromiso de cumplimiento                                | 38        |
| 13.6 Cierre formal del Programa                                | 39        |

**CARTA DE COMPROMISO DE LA ALTA DIRECCIÓN****PROGRAMA DE INTEGRIDAD Y CUMPLIMIENTO NORMATIVO**

Yo, **Mathias Alfonso Barria Alarcón**, cédula nacional de identidad N° **19.541.153-0**, en mi calidad de **Representante Legal** de la sociedad **TechBackup SpA**, RUT **77.171.331-9**, con domicilio en **Diego Portales N° 860**, comuna de **Puerto Montt**, declaro lo siguiente:

## 1. Compromiso institucional

TechBackup SpA declara formal y expresamente su **compromiso irrestricto con la integridad, la probidad, la ética empresarial y el cumplimiento normativo**, tanto en el desarrollo de sus actividades comerciales como en su relación con clientes, proveedores, trabajadores, organismos públicos y terceros relacionados.

Este compromiso se materializa mediante la **implementación, mantención y mejora continua** del presente **Programa de Integridad y Cumplimiento**, el cual se adopta como **instrumento oficial, obligatorio y vinculante** para toda la organización.

## 2. Marco normativo aplicable

El Programa de Integridad de TechBackup SpA se diseña, implementa y ejecuta en estricto apego a la normativa vigente, incluyendo, a lo menos:

- **Ley N° 19.886** sobre Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y su reglamento vigente.
- **Ley N° 20.393**, sobre responsabilidad penal de las personas jurídicas, integrada de forma expresa y operativa al programa.
- **Ley N° 18.575**, Orgánica Constitucional de Bases Generales de la Administración del Estado.
- **Ley N° 21.121**, que modifica el Código Penal y otros cuerpos legales en materia de probidad.
- **Estrategia Nacional de Integridad Pública.**
- Enfoque y principios de los estándares internacionales **ISO 37301:2021** (Sistemas de Gestión de Compliance) e **ISO 37001:2016** (Sistemas de Gestión Antisoborno).

### 3. Alcance y obligatoriedad

El presente Programa de Integridad es **obligatorio** para:

- La alta dirección y representación legal.
- El Oficial de Cumplimiento interno.
- Todos los trabajadores, colaboradores, contratistas y terceros que actúen en nombre o representación de TechBackup SpA.

El desconocimiento del programa **no exime de responsabilidad**, y su cumplimiento constituye una **condición esencial** de permanencia y vinculación con la empresa.

### 4. Designación del Oficial de Cumplimiento

TechBackup SpA designa como **Oficial de Cumplimiento Interno** a:

**Nombre:** Mathias Alfonso Barria Alarcón  
**RUT:** 19.541.153-0

El Oficial de Cumplimiento contará con el **apoyo técnico, metodológico y documental externo de MAXING**, en calidad de asesor especializado, asegurando independencia funcional, respaldo técnico y alineación permanente con el estándar PI-ESTANDAR-V1.

### 5. Recursos y autoridad

La empresa se compromete a proporcionar al Oficial de Cumplimiento los **recursos, acceso a información, autonomía funcional y respaldo jerárquico** necesarios para el ejercicio efectivo de sus funciones, incluyendo la facultad de:

- Supervisar el cumplimiento del programa.
- Gestionar el canal de denuncias.
- Proponer mejoras y medidas correctivas.
- Reportar directamente a la alta dirección cuando corresponda.

## 6. Tolerancia cero frente a infracciones

TechBackup SpA adopta un **principio de tolerancia cero** frente a conductas que vulneren la ley, la ética, la probidad administrativa o las disposiciones del presente Programa de Integridad, aplicando las medidas disciplinarias, contractuales y legales que correspondan.

## 7. Vigencia y revisión

El presente compromiso entra en vigencia desde su firma y se mantendrá plenamente vigente mientras TechBackup SpA desarrolle sus actividades comerciales, siendo objeto de **revisión periódica**, conforme a la matriz de riesgos y a los mecanismos de mejora continua establecidos en el Programa.

Firma Representante Legal  
**Mathias Alfonso Barria Alarcón**  
Representante Legal - TechBackup SpA  
RUT: 19.541.153-0

## CAPÍTULO 1

# PRESENTACIÓN DEL PROGRAMA DE INTEGRIDAD Y CUMPLIMIENTO

## 1.1 Contexto general

El presente **Programa de Integridad y Cumplimiento Normativo** ha sido desarrollado para **TechBackup SpA**, empresa dedicada a la **compra y venta de productos y servicios de informática**, con el propósito de establecer un **marco estructurado, formal y verificable** de prevención, detección y respuesta frente a riesgos legales, éticos y de integridad asociados a su actividad comercial, especialmente en su interacción con terceros y, cuando corresponda, con el Estado.

Este programa constituye un **instrumento institucional oficial**, adoptado por decisión expresa de la alta dirección, y se integra plenamente a la gestión de la empresa como un **sistema permanente**, no circunstancial, orientado al cumplimiento normativo y a la conducta empresarial responsable.

## 1.2 Naturaleza del Programa

El Programa de Integridad de TechBackup SpA:

- Es **obligatorio, vinculante y transversal** a toda la organización.
- Tiene carácter **preventivo, correctivo y sancionatorio**.
- Se encuentra **alineado con la legislación chilena vigente** y con estándares internacionales reconocidos en materia de compliance.
- Está diseñado bajo un **enfoque basado en riesgos**, donde cada política, procedimiento y control responde directamente a riesgos identificados y evaluados.

No constituye una declaración genérica de principios, sino un **sistema estructurado de normas, roles, procedimientos, controles y registros**, diseñado para ser **auditable, demostrable y exigible**.



### 1.3 Objetivo general

El objetivo general del presente Programa de Integridad es **prevenir la comisión de infracciones legales, faltas éticas y conductas contrarias a la probidad**, protegiendo a TechBackup SpA frente a riesgos penales, administrativos, contractuales y reputacionales, y asegurando un actuar empresarial conforme a la ley y a estándares de integridad.

### 1.4 Objetivos específicos

Son objetivos específicos del Programa:

- a) **Dar cumplimiento efectivo** a las obligaciones establecidas en la normativa chilena aplicable.
- b) **Prevenir delitos y conductas indebidas**, en especial aquellas contempladas en la Ley N° 20.393.
- c) **Establecer reglas claras de conducta** para trabajadores, directivos y terceros.
- d) **Identificar, evaluar y gestionar riesgos** asociados a la actividad de la empresa.
- e) **Proveer mecanismos formales de denuncia**, investigación y sanción.
- f) **Asegurar trazabilidad documental** frente a fiscalizaciones, auditorías o procesos judiciales.
- g) **Fortalecer la cultura organizacional de integridad** mediante capacitación y comunicación permanente.

### 1.5 Alcance del Programa

El Programa de Integridad se aplica a:

- El Representante Legal.
- El Oficial de Cumplimiento interno.
- Todos los trabajadores, cualquiera sea su modalidad contractual.
- Proveedores, contratistas y terceros cuando actúen en representación, beneficio o interés de TechBackup SpA.

Su cumplimiento es exigible **sin excepción**, y su desconocimiento no constituye excusa válida para eximir responsabilidades.

## 1.6 Integración con la gestión de la empresa

El Programa se integra a la operación diaria de TechBackup SpA mediante:

- Políticas internas obligatorias.
- Procedimientos operativos documentados.
- Registros y formularios verificables.
- Canales de comunicación y denuncia formales.
- Mecanismos de control, seguimiento y mejora continua.

## CAPÍTULO 2

### MARCO NORMATIVO Y ESTÁNDARES DE REFERENCIA

#### 2.1 Principio de legalidad y cumplimiento normativo

TechBackup SpA adopta como principio rector el **cumplimiento estricto de la ley**, entendiendo que toda actividad empresarial debe desarrollarse dentro del marco normativo vigente, sin recurrir a prácticas elusivas, abusivas o contrarias a la probidad.

El presente Programa de Integridad se estructura sobre la base de normas legales obligatorias y estándares técnicos reconocidos, los cuales se integran de forma **operativa y no meramente declarativa**.

## 2.2 Ley N° 19.886 y su reglamento

La **Ley N° 19.886**, sobre Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios, y su reglamento vigente, establecen principios de **probidad, transparencia, igualdad de los oferentes y libre concurrencia** en la contratación pública.

El Programa incorpora medidas orientadas a:

- Prevenir conflictos de interés en procesos de contratación pública.
- Asegurar relaciones lícitas y transparentes con organismos del Estado.
- Evitar prácticas que puedan derivar en inhabilidades, sanciones o exclusiones del sistema de compras públicas.

## 2.3 Ley N° 20.393 - Responsabilidad penal de las personas jurídicas

El Programa integra expresamente la **Ley N° 20.393**, estableciendo mecanismos destinados a prevenir los delitos por los cuales una persona jurídica puede ser penalmente responsable, incluyendo, entre otros:

- Cohecho.
- Lavado de activos.
- Financiamiento del terrorismo.
- Receptación y delitos incorporados por modificaciones posteriores.

El diseño del Programa cumple con los elementos exigidos por la ley, incluyendo:

- Designación de un Oficial de Cumplimiento.
- Identificación de actividades o procesos de riesgo.
- Protocolos y procedimientos específicos.
- Sistemas de supervisión y control.
- Régimen disciplinario y de sanciones.

## 2.4 Ley N° 18.575 - Bases Generales de la Administración del Estado

Esta normativa establece los principios de **probidad administrativa, legalidad, eficiencia y responsabilidad**, los cuales son asumidos por TechBackup SpA como criterios de conducta en toda relación directa o indirecta con órganos del Estado y sus funcionarios.

## 2.5 Ley N° 21.121

La Ley N° 21.121 refuerza el marco sancionatorio en materia de probidad y delitos funcionarios, ampliando tipos penales y endureciendo sanciones. El Programa considera esta normativa como un **riesgo crítico**, integrando controles específicos para prevenir conductas que puedan configurar infracciones penales graves.

## 2.6 Estrategia Nacional de Integridad Pública

El Programa se alinea con los principios de la **Estrategia Nacional de Integridad Pública**, promoviendo una gestión empresarial responsable, transparente y coherente con los estándares exigidos por el Estado y la ciudadanía.

## 2.7 Estándares internacionales ISO

El diseño y estructura del Programa consideran los principios y lineamientos de:

- **ISO 37301:2021** - Sistemas de Gestión de Compliance.
- **ISO 37001:2016** - Sistemas de Gestión Antisoborno.

Estos estándares se incorporan como **marco metodológico**, fortaleciendo la lógica de mejora continua, enfoque basado en riesgos y liderazgo organizacional.

## CAPÍTULO 3

# GOBIERNO CORPORATIVO, ROLES Y RESPONSABILIDADES

## 3.1 Principios de gobierno del Programa de Integridad

TechBackup SpA adopta un modelo de gobierno del Programa de Integridad basado en los principios de:

- Responsabilidad de la alta dirección.
- Separación funcional de roles.
- Autonomía operativa del Oficial de Cumplimiento.
- Trazabilidad documental y rendición de cuentas.
- Mejora continua y supervisión permanente.

El gobierno del Programa tiene por finalidad asegurar que las políticas y procedimientos no solo existan formalmente, sino que sean **efectivamente aplicados, supervisados y corregidos** cuando corresponda.

## 3.2 Responsabilidad de la Alta Dirección

La alta dirección de TechBackup SpA es la **máxima responsable del Programa de Integridad**, asumiendo, entre otras, las siguientes obligaciones:

- a) Aprobar formalmente el Programa y sus actualizaciones.
- b) Promover una cultura organizacional basada en la integridad y el cumplimiento.
- c) Respalda explícitamente la autoridad del Oficial de Cumplimiento.
- d) Proveer los recursos necesarios para la implementación y funcionamiento del Programa.
- e) Conocer y resolver, cuando corresponda, los reportes elevados por el Oficial de Cumplimiento.

La responsabilidad de la alta dirección es **indelegable**, sin perjuicio de la existencia de roles operativos específicos.

### 3.3 Oficial de Cumplimiento Interno

TechBackup SpA designa como **Oficial de Cumplimiento Interno** a:

**Nombre:** Mathias Alfonso Barria Alarcón

**RUT:** 19.541.153-0

El Oficial de Cumplimiento actúa con **autonomía funcional**, sin perjuicio de su rol ejecutivo, y cuenta con **apoyo técnico externo especializado de MAXING**, conforme al modelo PI-OC-APOYO=MAXING.

### 3.4 Funciones del Oficial de Cumplimiento

Son funciones mínimas del Oficial de Cumplimiento:

- a) Supervisar la correcta implementación del Programa de Integridad.
- b) Identificar, evaluar y actualizar riesgos de cumplimiento.
- c) Velar por la aplicación efectiva de políticas y procedimientos.
- d) Administrar el canal de denuncias y coordinar investigaciones internas.
- e) Mantener registros y evidencia documental del funcionamiento del Programa.
- f) Proponer medidas correctivas y de mejora.
- g) Informar a la alta dirección sobre incumplimientos relevantes o riesgos críticos.

### 3.5 Apoyo externo MAXING

MAXING actúa como **asesor externo especializado**, prestando apoyo metodológico, técnico y documental al Oficial de Cumplimiento, sin asumir funciones ejecutivas ni decisorias.

El apoyo externo tiene por objeto:

- Fortalecer la independencia del sistema.
- Asegurar alineación permanente con PI-ESTANDAR-V1.
- Apoyar procesos de actualización, auditoría interna y mejora continua.
- Respalda técnicamente la trazabilidad y demostrabilidad del Programa.

### 3.6 Deberes de trabajadores y terceros

Todos los trabajadores y terceros vinculados a TechBackup SpA tienen el deber de:

- Conocer y cumplir el Programa de Integridad.
- Actuar conforme a la ley y a las políticas internas.
- Reportar oportunamente situaciones irregulares.
- Colaborar en investigaciones internas cuando corresponda.

El incumplimiento de estos deberes da lugar a las medidas disciplinarias y contractuales pertinentes.

## CAPÍTULO 4

### POLÍTICAS DE INTEGRIDAD, ÉTICA Y CONDUCTA EMPRESARIAL

#### 4.1 Principios generales de conducta

TechBackup SpA establece como principios rectores de conducta empresarial:

- **Legalidad**
- **Probidad**
- **Transparencia**
- **Buena fe**
- **Responsabilidad empresarial**

Estos principios son obligatorios y orientan todas las decisiones y actuaciones de la empresa, cualquiera sea el nivel jerárquico o función desempeñada.

## 4.2 Cumplimiento normativo obligatorio

Toda actuación de la empresa y de quienes actúan en su nombre debe ajustarse estrictamente a la legislación vigente, quedando prohibida cualquier conducta destinada a:

- Obtener ventajas indebidas.
- Eludir controles legales o administrativos.
- Influir indebidamente en decisiones de terceros.
- Distorcionar procesos de contratación o evaluación.

## 4.3 Prohibición de conductas indebidas

Se prohíbe expresamente:

- a) El ofrecimiento, promesa, entrega o aceptación de sobornos, dádivas o beneficios indebidos.
- b) La participación en actos de corrupción, cohecho o tráfico de influencias.
- c) La falsificación, alteración u ocultamiento de información o registros.
- d) El uso indebido de recursos, activos o información de la empresa.
- e) Cualquier conducta que pueda comprometer la responsabilidad penal de la empresa.

## 4.4 Conflictos de interés

Los trabajadores y directivos deben evitar situaciones en las que intereses personales, familiares o económicos puedan interferir con los intereses de TechBackup SpA.

Toda situación de potencial o actual conflicto de interés debe ser **informada oportunamente** al Oficial de Cumplimiento, conforme a los procedimientos establecidos en los anexos del Programa.



#### 4.5 Relación con el sector público

En toda relación con organismos del Estado, funcionarios públicos o empresas vinculadas al sector público, TechBackup SpA se obliga a actuar con:

- Estricto apego a la Ley N° 19.886 y su reglamento.
- Transparencia y trazabilidad documental.
- Respeto irrestricto a los principios de probidad administrativa.

#### 4.6 Régimen disciplinario

El incumplimiento de las políticas de integridad y conducta dará lugar a la aplicación de medidas disciplinarias proporcionales a la gravedad de la falta, sin perjuicio de las acciones legales que correspondan.

## CAPÍTULO 5

# IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS DE INTEGRIDAD Y CUMPLIMIENTO

### 5.1 Enfoque basado en riesgos

TechBackup SpA adopta un **enfoque basado en riesgos** como eje estructural de su Programa de Integridad, conforme a la Ley N° 20.393 y a los principios de los estándares ISO 37301 e ISO 37001.

Este enfoque implica que todas las políticas, procedimientos, controles y medidas del Programa se diseñan y aplican en función de **riesgos reales, identificables y evaluables**, propios de la actividad, tamaño, estructura y contexto operativo de la empresa.

### 5.2 Objetivo del proceso de identificación de riesgos

El proceso de identificación y evaluación de riesgos tiene por objeto:

- Identificar procesos, actividades y relaciones expuestas a riesgos de integridad.
- Evaluar la probabilidad e impacto de dichos riesgos.
- Priorizar riesgos relevantes y críticos.
- Definir controles y medidas de mitigación proporcionales.
- Generar trazabilidad entre riesgos, controles y acciones correctivas.

### 5.3 Alcance del análisis de riesgos

El análisis de riesgos de TechBackup SpA considera, a lo menos:

- Actividades comerciales habituales.
- Relación con clientes privados y públicos.
- Interacción con proveedores y terceros.
- Procesos de compras, ventas y contratación de servicios.
- Manejo de información, activos y recursos financieros.
- Participación en procesos de contratación pública, cuando corresponda.

## 5.4 Metodología de evaluación

La evaluación de riesgos se realiza mediante una metodología estructurada que considera:

- Identificación del riesgo.
- Descripción del evento de riesgo.
- Causa potencial.
- Probabilidad de ocurrencia.
- Impacto legal, económico y reputacional.
- Nivel de riesgo inherente.
- Controles existentes o propuestos.
- Nivel de riesgo residual.

Esta metodología se documenta formalmente en la **Matriz de Riesgos**, desarrollada íntegramente en el **Capítulo 12** del presente Programa.

## 5.5 Responsabilidad del proceso

El proceso de identificación y evaluación de riesgos es liderado por el **Oficial de Cumplimiento**, con apoyo técnico de MAXING, y con la colaboración de las áreas y personas que correspondan.

La alta dirección debe **conocer, validar y respaldar** los resultados del análisis de riesgos y las medidas de mitigación propuestas.

## 5.6 Actualización de riesgos

La identificación y evaluación de riesgos se revisará:

- Periódicamente, al menos una vez al año.
- Cuando existan cambios relevantes en la actividad de la empresa.
- Frente a modificaciones normativas significativas.
- Ante la ocurrencia de incidentes, denuncias o incumplimientos relevantes.

## CAPÍTULO 6

# MEDIDAS DE PREVENCIÓN, CONTROL Y MITIGACIÓN

## 6.1 Principio de proporcionalidad y efectividad

Las medidas de prevención y control adoptadas por TechBackup SpA se diseñan bajo los principios de:

- **Proporcionalidad**, en función del nivel de riesgo identificado.
- **Efectividad**, orientadas a prevenir, detectar y corregir conductas indebidas.
- **Formalización**, mediante procedimientos escritos y registros verificables.
- **Trazabilidad**, permitiendo demostrar su aplicación ante terceros.

## 6.2 Tipos de controles implementados

El Programa de Integridad contempla, entre otros, los siguientes tipos de controles:

- a) **Controles preventivos**, destinados a evitar la ocurrencia de conductas indebidas.
- b) **Controles detectivos**, orientados a identificar oportunamente desviaciones o incumplimientos.
- c) **Controles correctivos**, destinados a mitigar efectos y evitar recurrencias.

## 6.3 Políticas y procedimientos formales

TechBackup SpA implementa políticas y procedimientos formales, desarrollados en los anexos del Programa, que incluyen, a lo menos:

- Código de Ética.
- Política Anticorrupción y Antisoborno.
- Política de Conflictos de Interés.
- Política de Regalos, Beneficios e Incentivos.
- Política de Canal de Denuncias.
- Política de Proveedores y Terceros.
- Política de Comunicación de Integridad.

Estas políticas son obligatorias y su cumplimiento es exigible a todo el personal y terceros relacionados.

## 6.4 Controles en procesos críticos

Se establecen controles específicos en procesos considerados críticos, tales como:

- Selección y contratación de proveedores.
- Relación con clientes y terceros estratégicos.
- Participación en procesos de contratación pública.
- Gestión de pagos, cobros y documentación comercial.
- Acceso y uso de información sensible o confidencial.

## 6.5 Registro y evidencia documental

Todas las medidas de prevención y control deben quedar respaldadas mediante:

- Registros formales.
- Formularios estandarizados.
- Actas, reportes y respaldos documentales.

La ausencia de registro se considera una **debilidad del control**, aun cuando la medida haya sido aplicada de hecho.

## 6.6 Rol del Oficial de Cumplimiento

El Oficial de Cumplimiento es responsable de:

- Supervisar la correcta aplicación de los controles.
- Verificar la existencia de evidencia documental.
- Proponer ajustes o mejoras a las medidas de mitigación.
- Reportar desviaciones relevantes a la alta dirección.

## CAPÍTULO 7

# CANAL DE DENUNCIAS Y PROTECCIÓN AL DENUNCIANTE

## 7.1 Principio general

TechBackup SpA establece un **Canal de Denuncias formal, accesible y seguro**, destinado a permitir la comunicación de hechos, conductas o situaciones que puedan constituir infracciones legales, incumplimientos normativos o vulneraciones al Programa de Integridad.

El Canal de Denuncias es un **mecanismo obligatorio del Programa**, diseñado para cumplir funciones preventivas, detectivas y correctivas, conforme a la Ley N° 20.393 y a los estándares ISO 37301 e ISO 37001.

## 7.2 Alcance del Canal de Denuncias

El Canal de Denuncias permite reportar, entre otros, los siguientes hechos:

- Posibles delitos contemplados en la Ley N° 20.393.
- Infracciones a la Ley N° 19.886 y su reglamento.
- Conductas contrarias a la probidad y ética empresarial.
- Conflictos de interés no declarados.
- Ofrecimiento, solicitud o aceptación de beneficios indebidos.
- Uso indebido de recursos, información o activos de la empresa.
- Incumplimientos a las políticas internas del Programa.

## 7.3 Sujetos habilitados para denunciar

Pueden utilizar el Canal de Denuncias:

- Trabajadores de TechBackup SpA.
- Directivos y representantes.
- Proveedores, contratistas y terceros relacionados.
- Cualquier persona que tenga conocimiento fundado de una situación irregular vinculada a la empresa.

## 7.4 Modalidad del Canal de Denuncias

El Canal de Denuncias se implementa mediante mecanismos formales definidos en los anexos del Programa, los cuales garantizan:

- Accesibilidad razonable.
- Confidencialidad de la información.
- Registro y trazabilidad del ingreso de denuncias.
- Custodia segura de los antecedentes.

El canal puede admitir denuncias **identificadas o anónimas**, según se establezca en los procedimientos internos.

## 7.5 Protección al denunciante

TechBackup SpA garantiza la **protección del denunciante de buena fe**, prohibiendo expresamente cualquier forma de:

- Represalia.
- Amenaza.
- Discriminación.
- Perjuicio laboral, contractual o comercial.

Cualquier represalia será considerada una **infracción grave al Programa de Integridad** y dará lugar a las medidas disciplinarias correspondientes.

## 7.6 Confidencialidad y uso de la información

La información recibida a través del Canal de Denuncias será tratada con estricta confidencialidad y utilizada exclusivamente para los fines del Programa de Integridad y el cumplimiento normativo.

El acceso a los antecedentes quedará restringido al **Oficial de Cumplimiento** y a quienes deban intervenir conforme a los procedimientos establecidos.

## 7.7 Registro y trazabilidad

Toda denuncia recibida deberá quedar registrada, incluyendo:

- Fecha de recepción.
- Medio de ingreso.
- Tipo de denuncia.
- Estado de tramitación.
- Medidas adoptadas.

Estos registros constituyen **evidencia documental obligatoria** del funcionamiento del Programa.

## CAPÍTULO 8

# INVESTIGACIÓN INTERNA Y GESTIÓN DE INCIDENTES

## 8.1 Principio de debida diligencia

TechBackup SpA se obliga a **investigar de manera oportuna, objetiva y documentada** toda denuncia, indicio o antecedente que sugiera la existencia de un incumplimiento normativo o vulneración al Programa de Integridad.

La investigación interna constituye un elemento esencial del sistema de prevención y control.

## 8.2 Inicio de la investigación

La investigación interna puede iniciarse por:

- Denuncia ingresada a través del Canal de Denuncias.
- Detección interna de irregularidades.
- Observaciones derivadas de auditorías o revisiones internas.
- Requerimientos de autoridades competentes.



### 8.3 Responsable de la investigación

La investigación será dirigida por el **Oficial de Cumplimiento**, quien podrá contar con el **apoyo técnico externo de MAXING**, cuando la complejidad, naturaleza o sensibilidad del caso lo justifique.

El Oficial de Cumplimiento actuará con **imparcialidad, confidencialidad y diligencia**, resguardando los derechos de las personas involucradas.

### 8.4 Etapas del proceso de investigación

El proceso de investigación interna considera, a lo menos, las siguientes etapas:

- a) Análisis preliminar de admisibilidad.
- b) Recopilación y revisión de antecedentes.
- c) Entrevistas, cuando corresponda.
- d) Evaluación de hechos y determinación de incumplimientos.
- e) Elaboración de informe de investigación.
- f) Propuesta de medidas correctivas o sancionatorias.

### 8.5 Medidas correctivas y disciplinarias

En caso de confirmarse incumplimientos, TechBackup SpA adoptará las medidas que correspondan, las cuales podrán incluir:

- Medidas disciplinarias internas.
- Ajustes a procedimientos o controles.
- Capacitación adicional.
- Término de relaciones contractuales.
- Denuncia ante autoridades competentes, cuando proceda.

## 8.6 Cierre del caso y documentación

Toda investigación deberá concluir con un **cierre formal**, debidamente documentado, dejando constancia de:

- Hechos investigados.
- Conclusiones alcanzadas.
- Medidas adoptadas.
- Fecha de cierre.

La documentación asociada a investigaciones constituye **evidencia crítica** del Programa de Integridad y deberá ser conservada conforme a las políticas internas.

## 8.7 Aprendizaje organizacional

Los resultados de las investigaciones internas deberán ser considerados para:

- Actualizar la matriz de riesgos.
- Fortalecer controles existentes.
- Prevenir recurrencias.
- Mejorar la efectividad del Programa.

## CAPÍTULO 9

# CAPACITACIÓN Y COMUNICACIÓN DEL PROGRAMA DE INTEGRIDAD

## 9.1 Principio general

TechBackup SpA reconoce que la efectividad del Programa de Integridad depende de que sus disposiciones sean **conocidas, comprendidas y aplicadas** por todas las personas obligadas a su cumplimiento. En consecuencia, la empresa implementa un **sistema formal de capacitación y comunicación**, obligatorio y permanente.

## 9.2 Objetivos de la capacitación

La capacitación en materia de integridad y cumplimiento tiene por objeto:

- Informar sobre el contenido y alcance del Programa de Integridad.
- Explicar obligaciones legales y normativas relevantes.
- Prevenir conductas indebidas mediante sensibilización temprana.
- Fortalecer la cultura organizacional de integridad.
- Asegurar trazabilidad y evidencia del cumplimiento formativo.

## 9.3 Sujetos obligados a capacitación

Deben participar obligatoriamente en los procesos de capacitación:

- Representante Legal.
- Oficial de Cumplimiento.
- Todos los trabajadores, cualquiera sea su función o modalidad contractual.
- Terceros relevantes, cuando así se determine contractualmente.

## 9.4 Modalidades de capacitación

La capacitación podrá impartirse mediante una o más de las siguientes modalidades, conforme a las necesidades de la empresa:

- Capacitación presencial.
- Capacitación en modalidad digital o remota.
- Inducción obligatoria para nuevo personal.
- Refuerzos periódicos o capacitaciones específicas por riesgo.

Las modalidades, contenidos y frecuencia serán definidas y supervisadas por el **Oficial de Cumplimiento**, con apoyo técnico de MAXING.

## 9.5 Contenidos mínimos

Las actividades de capacitación deberán abordar, al menos:

- Principios del Programa de Integridad.
- Marco normativo aplicable.
- Prohibición de conductas indebidas.
- Conflictos de interés.
- Canal de Denuncias y protección al denunciante.
- Consecuencias del incumplimiento.

## 9.6 Registro y evidencia

Toda capacitación deberá quedar debidamente respaldada mediante:

- Listas de asistencia o registros digitales.
- Materiales utilizados.
- Evaluaciones o confirmaciones de participación, cuando corresponda.

La falta de registro se considerará **incumplimiento formal** del Programa.

## 9.7 Comunicación del Programa

TechBackup SpA implementará mecanismos de comunicación interna destinados a:

- Difundir el Programa de Integridad y sus actualizaciones.
- Recordar obligaciones y prohibiciones relevantes.
- Reforzar el uso del Canal de Denuncias.

## CAPÍTULO 10

# MONITOREO, SUPERVISIÓN Y MEJORA CONTINUA

## 10.1 Principio de mejora continua

El Programa de Integridad de TechBackup SpA se concibe como un **sistema dinámico**, sujeto a monitoreo permanente y mejora continua, conforme a la evolución de riesgos, normativa aplicable y contexto operativo de la empresa.

## 10.2 Monitoreo del Programa

El monitoreo tiene por objeto verificar:

- El cumplimiento efectivo de las políticas y procedimientos.
- La correcta aplicación de controles y medidas de mitigación.
- La existencia y calidad de registros y evidencia documental.
- La respuesta oportuna frente a denuncias e incidentes.

## 10.3 Responsable del monitoreo

El monitoreo del Programa es responsabilidad del **Oficial de Cumplimiento**, quien contará con el **apoyo técnico externo de MAXING** para labores de revisión, análisis y fortalecimiento del sistema.

## 10.4 Herramientas de supervisión

Para efectos de supervisión, podrán utilizarse, entre otras, las siguientes herramientas:

- Revisiones periódicas de cumplimiento.
- Auditorías internas de integridad.
- Revisión de la matriz de riesgos.
- Análisis de indicadores de cumplimiento.
- Verificación de capacitación y comunicaciones.

## 10.5 Gestión de hallazgos

Los hallazgos detectados durante el monitoreo deberán:

- a) Ser documentados formalmente.
- b) Ser evaluados según su gravedad y riesgo.
- c) Dar lugar a medidas correctivas proporcionales.
- d) Ser comunicados a la alta dirección cuando corresponda.

## 10.6 Actualización del Programa

El Programa de Integridad será actualizado cuando:

- Se identifiquen nuevas fuentes de riesgo.
- Existan cambios normativos relevantes.
- Se detecten debilidades en controles existentes.
- Ocurra un incidente relevante o reiterado.

Toda actualización deberá quedar **documentada y formalmente aprobada**.

## 10.7 Evidencia y demostrabilidad

El monitoreo y la mejora continua deberán generar evidencia suficiente para demostrar, ante terceros, que el Programa de Integridad:

- Existe formalmente.
- Se encuentra implementado.
- Funciona de manera efectiva.
- Es objeto de revisión y mejora permanente.

## CAPÍTULO 11

# RÉGIMEN DE SANCIONES Y CONSECUENCIAS DEL INCUMPLIMIENTO

## 11.1 Principio de responsabilidad

TechBackup SpA establece un **régimen formal de sanciones** aplicable a toda persona que infrinja la legislación vigente, las políticas internas o las disposiciones del presente Programa de Integridad.

El régimen sancionatorio se funda en los principios de:

- Legalidad
- Proporcionalidad
- Objetividad
- Debido proceso
- Trazabilidad documental

El incumplimiento del Programa constituye una **infracción grave**, independiente de que derive o no en responsabilidad penal o administrativa.

## 11.2 Sujetos sujetos a sanción

El régimen de sanciones se aplica a:

- Representante Legal
- Oficial de Cumplimiento
- Trabajadores y colaboradores
- Proveedores, contratistas y terceros relacionados

Cuando corresponda, las sanciones se aplicarán sin perjuicio de las responsabilidades civiles, penales o administrativas que pudieren derivarse.



### 11.3 Tipos de infracciones

Se consideran infracciones al Programa, entre otras:

- a) Incumplimiento de obligaciones legales aplicables.
- b) Vulneración de políticas y procedimientos del Programa.
- c) Omisión de deberes de reporte o denuncia.
- d) Entrega de información falsa o incompleta.
- e) Represalias contra denunciantes de buena fe.
- f) Obstrucción de investigaciones internas.

### 11.4 Medidas disciplinarias internas

Según la gravedad del incumplimiento, TechBackup SpA podrá aplicar una o más de las siguientes medidas:

- Amonestación verbal o escrita.
- Medidas correctivas formales.
- Suspensión de funciones.
- Término de la relación laboral o contractual.
- Terminación de contratos con terceros.

Las medidas adoptadas deberán quedar **debidamente documentadas**.

### 11.5 Denuncia a autoridades competentes

Cuando los hechos investigados revistan carácter de delito o infracción administrativa grave, TechBackup SpA evaluará la **denuncia ante las autoridades competentes**, conforme a la legislación vigente.

## 11.6 Registro y trazabilidad sancionatoria

Toda sanción aplicada deberá quedar respaldada mediante registros formales que indiquen:

- Hechos que motivan la sanción.
- Normas infringidas.
- Medida adoptada.
- Fecha y responsables de la decisión.

Estos registros constituyen evidencia obligatoria del funcionamiento del Programa.

## CAPÍTULO 12

# MATRIZ DE RIESGOS DE INTEGRIDAD Y CUMPLIMIENTO

## 12.1 Rol estructural de la Matriz de Riesgos

La **Matriz de Riesgos** constituye el núcleo técnico del Programa de Integridad de TechBackup SpA.

Todas las políticas, procedimientos, controles y medidas descritas en los capítulos anteriores **responden directamente a riesgos identificados en esta matriz**, asegurando coherencia, proporcionalidad y trazabilidad.

## 12.2 Objetivo de la Matriz de Riesgos

La Matriz de Riesgos tiene por objeto:

- Identificar riesgos de integridad y cumplimiento propios de la empresa.
- Evaluar probabilidad e impacto de dichos riesgos.
- Determinar niveles de riesgo inherente y residual.
- Definir controles y responsables.
- Generar respaldo demostrable ante fiscalizaciones y auditorías.

## 12.3 Metodología aplicada

La Matriz de Riesgos se construye conforme a una metodología estructurada que considera:

- Proceso o actividad expuesta.
- Riesgo identificado.
- Evento de riesgo.
- Normativa asociada.
- Probabilidad.
- Impacto.
- Nivel de riesgo inherente.
- Controles existentes o propuestos.
- Nivel de riesgo residual.
- Responsable del control.

## 12.4 Riesgos críticos considerados

Sin perjuicio de su actualización periódica, la Matriz de Riesgos de TechBackup SpA considera, a lo menos, los siguientes **riesgos críticos**:

### *a) Riesgos asociados a Ley N° 20.393*

- Cohecho en relaciones comerciales o públicas.
- Uso indebido de intermediarios o terceros.
- Operaciones sin respaldo documental suficiente.

### *b) Riesgos asociados a Ley N° 19.886*

- Conflictos de interés en procesos de contratación pública.
- Relación indebida con funcionarios públicos.
- Falta de trazabilidad en ofertas, contratos y ejecuciones.

### *c) Riesgos operativos y comerciales*

- Pagos sin justificación contractual.
- Manipulación o alteración de información comercial.
- Uso indebido de activos o información sensible.

## 12.5 Ejemplo estructural de matriz (referencial)

| Proceso | Riesgo                | Normativa  | Probabilidad | Impacto | Riesgo Inherente | Control              | Responsable | Riesgo Residual |
|---------|-----------------------|------------|--------------|---------|------------------|----------------------|-------------|-----------------|
| Ventas  | Cohecho               | Ley 20.393 | Media        | Alta    | Alto             | Política Antisoborno | OC          | Bajo            |
| Compras | Conflictos de interés | Ley 19.886 | Media        | Media   | Medio            | Declaración jurada   | OC          | Bajo            |

La versión completa y detallada de la Matriz de Riesgos se incorpora como **Anexo obligatorio** del Programa, con actualización periódica.

## 12.6 Actualización y revisión

La Matriz de Riesgos será revisada:

- Al menos una vez al año.
- Frente a cambios normativos.
- Ante incidentes relevantes.
- Cuando se modifique la actividad o estructura de la empresa.

Toda actualización deberá quedar **documentada, fechada y aprobada**.

## CAPÍTULO 13

# VIGENCIA, APROBACIÓN, DIFUSIÓN Y COMPROMISO FINAL

## 13.1 Aprobación formal del Programa de Integridad

El presente **Programa de Integridad y Cumplimiento Normativo** ha sido **formalmente aprobado por la Alta Dirección de TechBackup SpA**, mediante la suscripción de la Carta de Compromiso y la adopción expresa de cada uno de sus capítulos y anexos como **normativa interna obligatoria**.

La aprobación del Programa implica su incorporación plena al sistema de gestión de la empresa, con carácter **vinculante y exigible**, sin excepciones.

## 13.2 Vigencia del Programa

El Programa de Integridad entra en vigencia a contar de la fecha de su aprobación formal y se mantendrá plenamente vigente mientras:

- TechBackup SpA desarrolle actividades comerciales.
- Existan relaciones laborales, contractuales o comerciales vinculadas a la empresa.
- Sea exigible el cumplimiento de la normativa aplicable.

La vigencia del Programa es **indefinida**, sin perjuicio de las actualizaciones que correspondan conforme al Capítulo 10.

## 13.3 Obligatoriedad y alcance final

El cumplimiento del Programa es **obligatorio** para:

- El Representante Legal.
- El Oficial de Cumplimiento interno.
- Todos los trabajadores, colaboradores y dependientes.
- Proveedores, contratistas y terceros, cuando actúen en nombre, beneficio o interés de TechBackup SpA.

El desconocimiento, omisión o interpretación errónea del Programa **no exime de responsabilidad**.

### 13.4 Difusión interna y comunicación

TechBackup SpA se obliga a:

- Difundir el Programa de Integridad entre su personal.
- Facilitar el acceso al contenido del Programa y sus anexos.
- Informar oportunamente cualquier actualización o modificación relevante.

La difusión podrá realizarse mediante medios físicos, digitales o capacitaciones formales, dejando **respaldo documental verificable**.

### 13.5 Compromiso de cumplimiento

La adopción del presente Programa refleja el compromiso institucional de TechBackup SpA con:

- La legalidad y el cumplimiento normativo.
- La probidad y la ética empresarial.
- La prevención de delitos y conductas indebidas.
- La transparencia en sus relaciones comerciales y públicas.

Este compromiso es permanente y constituye un **pilar estratégico** de la gestión empresarial.

### 13.6 Cierre formal del Programa

Con la aprobación del presente capítulo y de sus anexos obligatorios, TechBackup SpA declara **formalmente implementado** su Programa de Integridad y Cumplimiento Normativo, conforme a:

- Ley N° 19.886 y su reglamento vigente.
- Ley N° 20.393 integrada operativamente.
- Ley N° 18.575.
- Ley N° 21.121.
- Estrategia Nacional de Integridad Pública.
- Enfoque ISO 37301 / ISO 37001.

| Fecha      | Versión | Descripción                         | Responsable     | Cargo       |
|------------|---------|-------------------------------------|-----------------|-------------|
| 28-01-2026 | TB-1.0  | Programa de Integridad y Compliance | Daniel Caniuman | Responsable |