

Política de prevención del delito, privacidad y ética corporativa

ACTUALIZADO EL 01 DE
JULIO DE 2026

MENSAJE DEL GERENTE GENERAL

En Cibertrend, nuestra conducta ética es de máxima prioridad. Actuamos con honestidad, integridad y respeto, incluso mientras competimos para ganar en un mercado dinámico y en constante evolución.

Nuestras Normas de Conducta Empresarial proporcionan una guía clara para todos los colaboradores de Cibertrend a nivel corporativo. Cada uno de nosotros está regido por sus principios, y todos somos responsables de cumplir y promover los valores que representan. Les insto a leer detenidamente nuestras Normas de Conducta Empresarial, comprenderlas y, en caso de enfrentar situaciones difíciles, recurrir a ellas como referencia. Si en algún momento no tienen la certeza de cómo proceder, no duden en acercarse a mi equipo, a sus líderes o al área de Recursos Humanos para solicitar orientación.

Finalmente, si observan o escuchan acerca de una conducta que les preocupe o consideren inapropiada, los animo a reportarlo a través de nuestro canal de denuncias anónimo: **denuncia@cibertrend.com**. Nos tomamos muy en serio cualquier denuncia, investigamos de manera exhaustiva y, cuando se descubre una conducta inapropiada, exigimos responsabilidad a quienes corresponda. Además, en Cibertrend no toleramos represalias contra aquellos empleados que expresan sus preocupaciones de manera honesta y de buena fe.

Gracias por su compromiso para asegurar que Cibertrend continúe creciendo de la manera correcta, con integridad y respeto en todo lo que hacemos.



Armando Salas Saleh
Gerente General

CUMPLIMIENTO DE LA LEY N°20.393

En cumplimiento con la Ley 20.393 sobre responsabilidad penal de las Personas Jurídicas, CIBERTREND adopta un firme compromiso con la prevención de delitos como el lavado de activos, financiamiento del terrorismo, cohecho a funcionario público nacional o extranjero, receptación, corrupción entre particulares, administración desleal, negociación incompatible y apropiación indebida.

Por ello, CIBERTREND puede ser legalmente responsable por los delitos cometidos por sus empleados, colaboradores y otras personas en el ejercicio de sus funciones dentro de la empresa.

Para mitigar estos riesgos, implementamos un Modelo de Prevención del Delito (MPD) que organiza, administra y supervisa las medidas de control necesarias para prevenir dichas infracciones. Este modelo establece directrices claras para una operación ética y efectiva, definiendo roles y responsabilidades específicas.

Los pilares fundamentales de nuestro modelo son:

- Designación de un Encargado de Prevención de Delitos.
- Asignación de recursos y facultades para la prevención.
- Implementación de un Sistema de Prevención de Delitos.
- Supervisión y mejora continua del sistema.

Nuestro código de conducta y ética anti-corrupción refleja nuestro compromiso inquebrantable con la transparencia, integridad y el respeto en todas nuestras actividades. Rechazamos de manera categórica cualquier tipo de soborno, extorsión o práctica corrupta, asegurando que nuestras decisiones y acciones estén guiadas por la honestidad. Además, promovemos un entorno de trabajo libre de acoso laboral, donde cada empleado es tratado con dignidad y respeto.

No toleramos ninguna forma de hostigamiento o conducta inapropiada. Fomentamos un ambiente donde cualquier irregularidad, ya sea relacionada con sobornos, corrupción o acoso, pueda ser denunciada de manera segura y confidencial.

Nuestro marco ético, que aborda también a nuestras filiales, define la forma en que actuamos en cada una de nuestras actividades diarias, los negocios y la integridad de nuestros equipos de trabajo.

Es deber de los directores, ejecutivos y empleados de CIBERTREND, cumplir la normativa que establece la responsabilidad penal de las personas jurídicas, en los delitos de lavado de activos, financiamiento del terrorismo, cohecho a funcionario público nacional o extranjero, receptación,

soborno entre particulares, negociación incompatible, apropiación indebida, administración desleal, contaminación de aguas, delitos relacionados con la veda de productos, pesca ilegal de recursos del fondo marino y procesamiento, almacenamiento de productos escasos (colapsados o sobreexplotados) sin acreditar origen legal (o cualquier otro delito que sea considerado dentro de ésta Ley en el futuro). Con la finalidad de prevenir la comisión de estos delitos, la Compañía ha designado a un Encargado de Prevención del Delito (EPD), quien tiene la misión de implementar un modelo de organización, administración y supervisión adecuada para prevenir y sancionar la ocurrencia de dichos ilícitos. La prohibición de incurrir en los delitos tipificados en esta Ley aplica también a Clientes, Proveedores y, en general, a quienes prestan servicios a CIBERTREND sin ser parte de ésta, para lo cual la Compañía deja establecidas estas obligaciones en los respectivos contratos de servicios. Por lo tanto, se prohíbe en forma expresa, a los empleados de CIBERTREND y externos, lo cual incluye a los contratistas, proveedores, distribuidores, asesores, agentes, clientes, etc., a realizar cualquier acto que pueda configurar los delitos descritos y las modificaciones que en el futuro pueda realizar a la presente ley que para todos los efectos legales se entienden incluidas dentro del presente capítulo.

CUMPLIMIENTO DE LA LEY N°19.913

CIBERTREND, de acuerdo con la Ley N°19.913, que crea la Unidad de Análisis Financiero (UAF) y modifica ciertas disposiciones en materia de Lavado y Blanqueo de Activos y según lo indicado en su párrafo 2°, artículo 3°, es sujeto obligado que debe cumplir con las obligaciones señaladas en dicho cuerpo legal y en los oficios y circulares que emanen de dicha unidad fiscalizadora. Para enfrentar el lavado de dinero y el financiamiento del terrorismo y sus delitos base, los trabajadores de CIBERTREND deben adecuar sus decisiones y actuaciones a lo previsto en el Manual de Prevención de Lavado de Activos y Financiamiento del Terrorismo y la norma interna complementaria referida en el Reglamento Interno de Orden, Higiene y Seguridad. Asimismo, quienes trabajan en CIBERTREND o participan en su gestión, han de tomar las responsabilidades individuales organizacionales, sean de orden civil, penal o administrativo, en especial, aquella que se relacionen con clientes o proveedores de empresas o servicios públicos, han de tener especial cuidado en abstenerse de incurrir en cualquier conducta que pudiese significar o interpretarse como ofrecer o consentir en dar a un empleado público, chileno o extranjero, algún beneficio, con el objeto de obtener ventajas y privilegios distintos a los establecidos en sus funciones o de concretar negocios personales.

Todos cuantos intervienen en la gestión de CIBERTREND, deben comunicar al Oficial de Cumplimiento, cualquier conducta que pudiese ser constitutiva de los delitos de lavado de activos

y financiamiento del terrorismo, ya sea, de miembros o personas ligadas a CIBERTREND, de clientes, proveedores o terceros.

CUMPLIMIENTO DE LA LEY N°19.913

Delitos base o precedentes de lavado de activos Se les denomina “delitos base o precedentes” de lavado de activos (LA) a aquellos cuyo producto de origen ilícito (dinero o bienes) se busca ocultar o disimular. La Ley N° 19.913, establece en el artículo 27, letra a), que “será castigado con presidio mayor, en sus grados mínimo a medio, y multa de 200 a 1.000 Unidades Tributarias Mensuales (UTM), el que de cualquier forma oculte o disimule el origen ilícito de determinados bienes, a sabiendas de que provienen, directa o indirectamente, de la perpetración de hechos constitutivos de alguno de los delitos contemplados en las siguientes legislaciones:

- Ley N° 20.000, que sanciona el tráfico ilícito de estupefacientes y sustancias psicotrópicas.
- Ley N° 18.314, que determina las conductas terroristas y fija su penalidad.
- Artículo 10 de la Ley N° 17.798, sobre control de armas.
- Título XI de la Ley N° 18.045, sobre mercado de valores.
- Título XVII del DFL N° 3, del Ministerio de Hacienda, de 1997, Ley General de Bancos.
- Artículo 168 en relación con el artículo 178, N° 1, ambos del DFL N° 30, del Ministerio de Hacienda, de 2005, que aprueba el texto refundido, coordinado y sistematizado del DFL N° 213, del Ministerio de Hacienda, de 1953, sobre Ordenanza de Aduanas.
- Inciso segundo del artículo 81 de la Ley N° 17.336, sobre propiedad intelectual.
- Artículos 59 y 64 de la Ley N° 18.840, orgánica constitucional del Banco Central de Chile.
- Párrafo tercero del número 4º del artículo 97 del Código Tributario.
- Párrafos 4, 5, 6, 9 y 9 bis del Título V y párrafo 10 del Título VI, todos del Libro Segundo del Código Penal.
- Artículos 141, 142, 366 quinquies, 367, 374 bis, 411 bis, 411 ter, 411 quáter, 411 quinquies, y los artículos 468 y 470, numerales 1,8 y 11, en relación con el inciso final del artículo 467 del Código Penal.
- Artículo 7 de la Ley N°20.009, que limita la responsabilidad de los titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude.

CUMPLIMIENTO DE LA LEY N°21643

En CIBERTREND, nos comprometemos a mantener un ambiente de trabajo seguro, respetuoso y libre de cualquier forma de acoso laboral, acoso sexual o violencia en el lugar de trabajo. Consideramos inaceptable cualquier comportamiento que afecte la dignidad de nuestros colaboradores o que genere un entorno laboral hostil. La prevención es el primer pilar para evitar estos incidentes, y para ello fomentamos una cultura de respeto mutuo y tolerancia cero frente a cualquier tipo de abuso. Realizamos capacitaciones periódicas para todos nuestros colaboradores, a fin de asegurar que comprendan plenamente sus responsabilidades y los comportamientos que constituyen acoso o violencia, así como las consecuencias de incurrir en dichas acciones.

La empresa establece canales de denuncia confidenciales, accesibles y confiables para que cualquier colaborador que sienta que ha sido víctima o testigo de acoso o violencia pueda reportarlo sin temor a represalias. Todo reporte será tratado con la mayor seriedad y confidencialidad posible. El equipo de Recursos Humanos, junto con el comité de Ética y Cumplimiento, será el responsable de realizar investigaciones exhaustivas, imparciales y objetivas. Dichas investigaciones incluirán entrevistas con las partes implicadas, recolección de pruebas y, en su caso, la implementación de medidas preventivas mientras se resuelve la situación. Nos aseguramos de que todas las partes tengan la oportunidad de expresar su versión de los hechos, respetando siempre los derechos de los involucrados y siguiendo estrictamente los principios de justicia y equidad.

Una vez finalizada la investigación, y si se determina que ha habido acoso, sexual o laboral, o cualquier forma de violencia, la empresa tomará medidas disciplinarias proporcionales a la gravedad de la infracción, que pueden incluir advertencias formales, suspensiones o, en los casos más graves, la terminación de la relación laboral del infractor. Es importante destacar que estas sanciones no solo aplican a los empleados, sino a cualquier persona que trabaje o colabore con CIBERTREND, incluyendo contratistas, proveedores y consultores externos.

Nuestra política de prevención y sanción busca proteger el bienestar de cada miembro de la empresa, garantizando que todos puedan desempeñar sus labores en un ambiente de respeto y seguridad. Cualquier represalia contra quienes denuncien actos de acoso o violencia está estrictamente prohibida y será sancionada severamente, reafirmando nuestro compromiso con la creación de un entorno laboral sano y equitativo para todos.

CUMPLIMIENTO DE LA LEY N° 21719

En cumplimiento con la Ley N° 21.719, que regula el tratamiento y protección de los datos personales y crea la Agencia de Protección de Datos Personales, CIBERTREND adopta un firme compromiso con la seguridad, privacidad y confidencialidad de la información de sus clientes, empleados, proveedores y colaboradores. Por ello, la empresa asume la responsabilidad legal y ética de garantizar que todo tratamiento de datos se realice bajo los principios de licitud, finalidad, proporcionalidad, calidad y seguridad, implementando medidas técnicas y organizativas adecuadas para prevenir accesos no autorizados, pérdidas o fugas de información.

Para mitigar los riesgos asociados y asegurar el estricto cumplimiento normativo, implementamos un proceso de Gestión de Privacidad y Protección de Datos que organiza, administra y supervisa los flujos de información dentro de la organización. Los pilares fundamentales de nuestro modelo son:

- Designación de un delegado de Protección de Datos (DPD).
- Implementación de políticas estrictas de consentimiento y transparencia.
- Garantía y facilitación del ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) de los titulares.
- Evaluación de impacto y mejora continua de nuestros sistemas de seguridad de la información.

Este marco de protección de datos personales y seguridad de la información es de cumplimiento obligatorio para todos los directores, ejecutivos y empleados de CIBERTREND. Asimismo, estas obligaciones y prohibiciones se extienden de manera expresa a clientes, proveedores, contratistas y cualquier tercero que preste servicios o actúe en representación de la Compañía, quedando explícitamente establecidas en los respectivos contratos de servicios para asegurar un estándar unificado de integridad y respeto a la privacidad.

COMITÉ DE ÉTICA

El Comité de Ética es un órgano de control interno que depende de la gerencia general de CIBERTREND y que tiene por objeto velar por el cumplimiento de las reglas del Código de Ética y Conducta, el establecimiento y desarrollo de los procedimientos necesarios para el cumplimiento de este Código, así como la interpretación, gestión y supervisión de las normas de actuación contenidas en los mismos y la resolución de los conflictos que su aplicación pudiera plantear. Toda conducta no ética reportada por cualquier medio, será manejada con la máxima discreción y protección para el empleado, para que éste no se vea perjudicado de ninguna manera y en ningún momento. Por esta razón, el Comité de Ética efectuará una instancia de análisis y revisión de la conducta no ética reportada, con el fin de aplicar medidas de corrección y mejora cuando corresponda. El Comité de Ética está integrado por el Gerente General, Gerente de recursos humanos y Abogado o fiscal. Los miembros del Comité que tengan interés directo o indirecto en cualquier asunto que el Comité de Ética deba conocer o esté conociendo, deberán hacerlo presente a los demás e inhabilitarse para conocer del asunto respectivo.

Las principales funciones del Comité de Ética corresponden a:

- Velar por el cumplimiento del Código de Ética y Conducta.
- Aprobar las modificaciones sugeridas al Código de Ética y Conducta.
- Analizar las denuncias recibidas, a través de los canales dispuestos por CIBERTREND, para identificar aquellas que estén bajo el alcance del Modelo de Prevención de Delitos o se encuentren asociadas a escenarios de delitos establecidos en la Ley Chilena N°20.393 y la Ley N°19.913 y el Sistema de prevención antilavado de activos y financiamiento del terrorismo.

Coordinar, a través de la designación de responsables, plazos de investigación y seguimiento, las investigaciones derivadas de las denuncias que tienen implicancia en el Modelo de Prevención de Delitos o se encuentren asociadas a escenarios de delito de la Ley Chilena N°20.393 y al Sistema de Prevención antilavado de activos y financiamiento del terrorismo de la Ley N°19.913.

- Apoyar al Encargado de Prevención de Delitos (EPD) y al Oficial de Cumplimiento en las diferentes actividades de control que éstos efectúan, principalmente en el proceso de identificación y análisis de denuncias que apliquen al Modelo de Prevención de Delitos, la Ley 19.913, la determinación de investigaciones y la posible aplicación de sanciones al respecto.
- Solicitar reportes de denuncias al Encargado de Prevención de Delitos y al Oficial de Cumplimiento, cuando las circunstancias lo ameriten (por ejemplo, mayor detalle de investigación, seguimiento de las denuncias, estatus de las denuncias).

CONTRAVERSIONES AL CÓDIGO DE ÉTICA

Se entiende como tal, cualquier incumplimiento de lo normado en el presente Código de Ética y Conducta o de cualquier otra conducta que transgreda una norma interna de la Compañía, las Leyes o en su sentido amplio, el orden público y las buenas costumbres, en especial, las conductas tipificadas como delitos por la Ley N° 20.393 y a la Ley N° 19.913, como también, la corrupción, el fraude, los abusos de autoridad, el peligro para la salud y seguridad pública de los trabajadores, o cualquier mala práctica a las buenas costumbres, incluido su ocultamiento y cualquier forma de participación en hechos no deseados. Cada empleado es responsable de velar por el cumplimiento del Código de Ética y Conducta y de poner en conocimiento de la Compañía cualquier circunstancia que él estime, de buena fe, que puede constituir una violación o infracción de estos. Si se toma conocimiento de una conducta o situación cuestionable, inadecuada o de aparente incumplimiento, que pueda constituir una contravención al Código de Ética y Conducta, el empleado tiene la obligación de comunicar oportunamente dicha situación a su jefatura inmediata y/o haciendo uso de los Canales habilitados por la Compañía. Atendida la gravedad de los hechos, las medidas y sanciones que se aplicarán serán las establecidas en el Reglamento Interno de Orden, Higiene y Seguridad o las previstas en los contratos con terceros, según corresponda. Ello sin perjuicio de la infracción que pudiera derivarse de lo dispuesto en la legislación y de la responsabilidad civil o penal, que en cada caso sea exigible.

CANAL DE DENUNCIA

Con el objeto de mantener los más altos estándares de ética en los negocios, CIBERTREND ha establecido canales formales de denuncia, específicamente un Canal de Denuncia, y procedimientos para la denuncia e investigación de infracciones al Código de Ética y de Conducta. La Compañía velará porque las denuncias se traten de manera confidencial, sin perjuicio de la información que sea necesaria entregar para la mejor conducción del proceso de investigación a que se dé lugar. También velará porque no se adopten acciones adversas en contra de un empleado, por el hecho de haber reportado de buena fe una posible infracción. Adicionalmente, CIBERTREND tiene establecidos mecanismos de auditoría y de control interno, como parte del quehacer permanente y habitual de la Compañía, orientados a verificar el cumplimiento de la normativa contenida en el Código de Ética y Conducta como asimismo el cumplimiento de todas aquellas normativas internas que dicte la Compañía, entre ellas el Modelo de Prevención de Delitos implementado en conformidad a la ley 20.393 y al Sistema de Prevención de delitos anti lavado de activos y financiamiento del terrorismo de la ley N°19.913.

CONSULTAS GENERALES

Para consultas generales o ante cualquier duda acerca del presente Código y las materias de su contenido deberán solicitar orientación ya sea a su Supervisor inmediato, Gerente de Área, al Encargado de Prevención de Delitos y/o al Oficial de Cumplimiento. Todos los empleados deberán leer cuidadosamente el Código de Ética y Conducta de CIBERTREND y luego firmar el documento “Recepción de Conformidad”, como muestra de su adhesión.

Vigencia: El presente Código de Ética y Conducta, en su tercera versión, fue aprobado por el Gerente General de CIBERTREND en fecha 26 de enero de 2023 entrando en vigor en forma inmediata.

CANAL DE DENUNCIAS

Cualquier persona, dentro o fuera de la organización puede entregar anónimamente una denuncia, la cual será investigada por un comité impar de integrantes y sumariar a la o las personas involucradas. En Cibertrend no toleramos represalias contra aquellos empleados que expresan sus preocupaciones de manera honesta y de buena fe.

El canal de denuncias anónimo es: denuncia@cibertrend.com