ON·NET FIBRA

Política acerca de Delitos Informáticos

InfraCo

Versión	Documentos	Fecha
1	Política acerca de Delitos Informáticos	01/09/2022

ÍNDICE DE CONTENIDO

POLÍTICA ACERCA DE DELITOS INFORMÁTICOS

1. OBJETIVO Y MARCO NORMATIVO

La presente Política acerca de Delitos Informáticos (en adelante, la "Política") constituye la norma marco que establece los lineamientos generales de InfraCo SpA (en adelante, la "Compañía"), en relación con los delitos establecidos en la Ley N° 21.459.

Con fecha 20 de junio de 2022 se publicó la Ley N° 21.459 que "*Establece normas sobre Delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapes*t", la cual viene a reemplazar la antigua ley que tipificaba figuras penales relativas a la informática, que data de 1993, a fin de ajustar a las nuevas formas de criminalidad en esta materia.

En general, las medidas más relevantes tienen relación con la tipificación de ocho nuevos delitos informáticos correspondientes a (i) Ataque a la integridad de un sistema informático; (ii) Acceso ilícito; (iii) Intercepción Ilícita; (iv) Ataque a la integridad de los datos informáticos; (v) Falsificación informática; (vi) Receptación de datos informáticos; (vii) Fraude informático; y, (viii) Abuso de dispositivos.

2. ÁMBITO DE APLICACIÓN

Este Política es de obligatorio cumplimiento para todos los procesos y actividades de la Compañía, así como para todo el Personal de la Compañía independientemente de su posición o nivel de jerarquía o el área al que pertenezcan, incluyendo empleados, directores, accionistas y cualquier otra persona natural o jurídica que actúe en representación o interés de la Compañía.

La presente Política tiene por objeto prevenir la comisión de los ilícitos establecidos en la Ley N° 21.459 y que con ello se comprometa la eventual responsabilidad penal de InfraCo SpA, de conformidad a lo dispuesto por la Ley N° 20.393 sobre Responsabilidad Penal de las Personas Jurídicas.

Por ello, la Política recibe aplicación ya sea en relación al uso, por parte de integrantes de la organización, de equipos informáticos entregados por la Compañía, como también respecto del uso de equipos o dispositivos de propiedad personal de los integrantes de la organización o de propiedad de un tercero, cuando aquellos sean utilizados con el fin de ejercer labores o trabajos para la Compañía.

Como política general, la Compañía declara su más estricta adhesión a la normativa que rige su actividad, ya sea normativa local o internacional, y establece que se encuentra estrictamente prohibido cometer cualquiera de los delitos establecidos en la Ley N° 21.459.

3. DEFINICIONES

3.1 **Datos informáticos**: Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una

función.

3.2 **Sistema informático**: Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

3.3 **Prestadores de servicios**: Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

4. CONDUCTAS CONSTITUTIVAS DE DELITO

(i) **Ataque a la Integridad de un Sistema Informático.** Está prohibido obstaculizar o impedir el normal funcionamiento, total o parcial, de un sistema informático de terceros **través** de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.

(ii) **Acceso Ilícito.** Está prohibido acceder a un sistema informático sin autorización, o excediendo la autorización otorgada y superando barreras técnicas o medidas tecnológicas de seguridad. También se encuentra prohibido acceder a un sistema informático con el ánimo de apoderarse o usar la información contenida en él, así como también obtener y divulgar la información obtenida de esta manera.

(iii) **Interceptación Ilícita.** Está prohibido interceptar, interrumpir o interferir indebidamente, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de estos. sin autorización de su emisor. Además, está prohibido, sin contar con la debida autorización, captar, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas proveniente de los mismos.

(iv) **Ataque a la Integridad de los Datos Informáticos.** Está prohibido alterar, dañar o suprimir indebidamente datos informáticos, ya sea de la Compañía o de terceros, siempre que con ello se cause un daño grave al titular de los mismos.

(v) **Falsificación Informática.** Está prohibido introducir, alterar, dañar o suprimir datos informáticos, con la intención de que éstos sean tomados como auténticos o utilizados para generar documentos auténticos.

(vi) **Receptación de Datos Informáticos.** Está prohibido comercializar, transferir o almacenar a cualquier título datos informáticos provenientes de los delitos de acceso ilícito, interceptación ilícita y falsificación informática con el mismo objeto u otro fin ilícito, conociendo su origen ilícito o no pudiendo menos que conocerlo.
La Compañía incorporará cláusulas en los contratos con Terceras Partes que permitan asegurar el origen lícito de los datos informáticos entregados a InfraCo por parte de las Terceras Partes con las cuales contrata.

(vii) **Fraude Informático.** Está prohibido manipular un sistema informático mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, con

la finalidad de obtener un beneficio económico para sí o para un tercero, causando perjuicio a otro. También está prohibido facilitar a otro los medios con que se comete el fraude informático.

(viii) **Abuso de Dispositivos.** Está prohibido entregar u obtener para su utilización, importar, difundir o realizar otra forma de puesta a disposición dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otro dato similar, creados o adaptados para cometer los delitos de ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita y ataque a la integridad de los datos informáticos o de los delitos de uso fraudulento de tarjetas de pago y transacciones electrónicas de la ley N° 20.009.

5. CAPACITACIÓN Y DIFUSIÓN

La Compañía reconoce la importancia de la capacitación y la difusión tanto de las políticas que integran el Modelo de Prevención de Delitos, como de la presente Política. En este sentido, el Encargado de Prevención de Delitos: (i) planifica e implementa las actividades de capacitación del Personal de la Compañía, en función de sus exigencias, posición, especialización, nivel de riesgo, entre otros, así como la comunicación para Terceras Partes; y, (ii) revisa y actualiza el contenido de las sesiones de capacitación, evalúa su efectividad e implementa las mejoras que considere relevantes.

6. ORIENTACIÓN

Siempre que exista alguna duda sobre el cumplimiento o posible incumplimiento de este Política deberá consultarse al Encargado de Prevención de Delitos y/o al Encargado de Ciberseguridad, pidiendo su opinión en el tema sin necesidad que ésta sea emitida o enviada de manera formal.

Para otras situaciones que no están cubiertas en este Política o en las que se destinan o emplean recursos e impliquen riesgos de los delitos establecidos en la Ley N° 21.459, el Encargado de Prevención de Delitos debe ser consultado para mayor orientación, antes de tomar una decisión o llevar a cabo la operación o actividad correspondiente.

7. CANALES DE DENUNCIA

Si el Personal de la Compañía o una Tercera Parte tuviesen motivos razonables o fundados para creer que alguna acción u omisión incumple este Política u otras políticas y procedimientos de la Compañía, debe comunicarlo inmediatamente a través de los canales de denuncia:

a. Casilla de correo electrónico: compliance@onnetfibra.com.
b. A través de la página web: https://www.onnetfibra.com/asuntos-legales/formulario-denuncias.
c. Denuncia directa y personal ante el Encargado de Prevención de Delitos.
d. Comunicación al superior jerárquico. El Personal de la Compañía puede comunicar por escrito a su superior jerárquico sobre cualquier violación a la presente Política. Estas denuncias serán derivadas al Encargado de Prevención de Delitos. El superior jerárquico tiene en estos casos el deber de preservar y garantizar la confidencialidad de la identidad del denunciante.

e. Denuncia anónima en el formulario de denuncia de la Compañía https://www.onnetfibra.com/asuntos-legales/formulario-denuncias. Sin perjuicio de lo anterior, la Compañía agradece que el denunciante entregue sus datos, para poder realizar la investigación correspondiente de la forma más exhaustiva posible.

La denuncia será tramitada de acuerdo a lo determinado en la Política de "Canal de Denuncias y Procedimiento de Investigaciones Internas", el Modelo de Prevención de Delitos y toda política interna aplicable del InfraCo SpA.

La Compañía toma en serio todos los reclamos o denuncias sobre represalias y, consecuentemente, los investiga para determinar las acciones o medidas correctivas que correspondan. Siguiendo la misma línea, la Compañía no tolerará represalias de ningún tipo contra ninguna persona que, de buena fe, reporte una presunta violación de la normativa anticorrupción vigente o de este Política.

8. ACCIONES Y MEDIDAS CORRECTIVAS

El Personal de la Compañía debe velar por el buen uso del sistema informático de InfraCo, así como de los dispositivos entregados por la Compañía para el desarrollo de sus actividades laborales. Los delitos especificados en la presente Política están prohibidos incluso si éstos son cometidos a través de equipos o dispositivos de uso personal, cuando su uso se esté relacionado con las labores para las que fue contratado por InfraCo.

Cualquier incumplimiento de este Política puede tener consecuencias graves para la Compañía, para el Personal de la Compañía y/o Terceras Partes, tanto a nivel económico, como comercial, legal y sobre todo reputacional. En este sentido, el Personal de la Compañía involucrado en incumplimientos a este Política y cualquier otra política que sea aplicable, podrán ser sancionados hasta con el despido de la Compañía, sin perjuicio de las sanciones penales o civiles previstas en la legislación local.