TECNOLOGÍAS DE INFORMACIÓN Y CIBERSEGURIDAD

ANÁLISIS DE NORMATIVAS Y REGULACIONES EN CIBERSEGURIDAD

Caso de Estudio: Ciberataque a IFX Networks

NOMBRES	Alex Camus, Antonio Morales
CARRERRA	Ingeniería Informática
ASIGNATURA	[TI3V34] Fundamentos de Seguridad de la Información
PROFESOR	Sergio Muñoz Sasso
FECHA	09-04-25

Índice

1 Introducción

1.1 Antecedentes

El 12 de septiembre de 2023, IFX Networks, una compañía de telecomunicaciones y servicios de almacenamiento en la nube que opera en 17 países de América Latina, sufrió un ataque de ransomware atribuido al grupo ciberdelincuente RansomHouse [6]. Este incidente afectó varias de sus máquinas virtuales, provocando la interrupción de servicios críticos para instituciones públicas y privadas en diversos países, incluyendo Chile, Colombia y Panamá.

En Chile, uno de los servicios más afectados fue la plataforma estatal mercadopublico.cl, encargada de gestionar las compras del gobierno, lo que generó un impacto significativo en diversos servicios gubernamentales y dejó en evidencia la vulnerabilidad de sistemas que manejan información sensible, tanto del sector público como privado.

1.2 Objetivo General

Analizar el caso del ciberataque a IFX Networks desde la perspectiva de las normativas y regulaciones nacionales e internacionales aplicables en materia de ciberseguridad, identificando los elementos normativos, delitos informáticos, marcos regulatorios, responsabilidades legales y tratamiento de datos personales relacionados con el incidente.

1.3 Objetivos Específicos

- Identificar los elementos normativos nacionales e internacionales aplicables al caso del ciberataque a IFX Networks.
- Determinar las acciones que constituyen delitos informáticos según la normativa vigente en Chile.
- Comparar los diversos marcos regulatorios aplicables según el tipo de industria involucrada.
- Analizar las responsabilidades legales relacionadas con el crimen informático según la normativa vigente en Chile.
- Evaluar el tratamiento adecuado de datos personales según la Ley de Protección de la Vida Privada (Ley 19.628).

2 Elementos Normativos Aplicables

2.1 Normativa Nacional

2.1.1 Ley 21.663: Ley Marco de Ciberseguridad

La Ley 21.663, promulgada el 26 de marzo de 2024 y publicada el 8 de abril de 2024, establece la institucionalidad, principios y normativa general para estructurar, regular y coordinar las acciones de ciberseguridad en Chile [3]. Esta ley es particularmente relevante para el caso de IFX Networks por los siguientes aspectos:

- **Creación de la Agencia Nacional de Ciberseguridad (ANCI):** Como organismo rector en materia de ciberseguridad, la ANCI tiene la facultad de dictar protocolos y estándares para prevenir, reportar y resolver incidentes de ciberseguridad.
- **Categorización de Servicios Esenciales y Operadores de Importancia Vital:** IFX Networks, al ser proveedor de servicios de telecomunicaciones e infraestructura digital que soporta servicios críticos como mercadopublico.cl, calificaría como un Operador de Importancia Vital según el artículo 5° de la ley, lo que le impone obligaciones específicas:
  - Implementar un sistema de gestión de seguridad de la información continuo
  - Elaborar e implementar planes de continuidad operacional y ciberseguridad
  - Realizar operaciones de revisión, ejercicios y simulacros
  - Adoptar medidas oportunas para reducir el impacto de incidentes
  - Contar con certificaciones de seguridad
  - Informar a los potenciales afectados sobre incidentes
- **Obligación de Reportar:** El artículo 9° establece que las instituciones deben reportar ciberataques e incidentes de ciberseguridad al CSIRT Nacional tan pronto como sea posible, siguiendo un esquema definido (alerta temprana, actualizaciones e informe final).

2.1.2 Ley 21.459: Ley de Delitos Informáticos

Esta ley, que deroga y reemplaza a la antigua Ley 19.223, tipifica figuras penales relativas a la informática en conformidad con el Convenio de Budapest [2]. En relación al caso de IFX Networks, son relevantes los siguientes delitos tipificados:

- **Ataque a la integridad de un sistema informático (Art. 3):** El ransomware utilizado por RansomHouse obstaculizó el funcionamiento de los sistemas de IFX Networks.
- **Acceso ilícito (Art. 2):** Los atacantes accedieron sin autorización a los sistemas informáticos de IFX Networks.
- **Interceptación ilícita (Art. 5):** Si durante el ataque se interceptaron datos transmitidos desde o hacia los sistemas de IFX Networks.
- **Abuso de dispositivos (Art. 8):** El desarrollo y uso de herramientas específicas para ejecutar el ransomware.

2.1.3 Ley 19.628: Sobre Protección de la Vida Privada

Esta ley regula el tratamiento de los datos personales y es relevante dado que el ataque a IFX Networks puede haber comprometido datos personales de usuarios y clientes [1]. La ley establece:

- La obligación de adoptar medidas de seguridad adecuadas para proteger los datos personales (Art. 11)
- La responsabilidad por los daños causados por el tratamiento indebido de datos personales
- El deber de confidencialidad sobre los datos personales a los que se tenga acceso

2.2 Normativa Internacional

2.2.1 Convenio de Budapest

El Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) es el primer tratado internacional que busca abordar los delitos informáticos mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones [5]. Chile se adhirió a este convenio, lo que ha influido directamente en la actualización de su legislación nacional, particularmente con la promulgación de la Ley 21.459. En relación al caso IFX Networks, el Convenio de Budapest es relevante por:

- Definición de delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos
- Establecimiento de mecanismos de cooperación internacional para la investigación de ciberdelitos
- Promoción de la asistencia mutua entre países para la persecución de grupos como RansomHouse

2.2.2 Estándares y Normas Internacionales

- **ISO/IEC 27001:** Establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI)
- **NIST Cybersecurity Framework:** Marco de referencia para la gestión de riesgos de ciberseguridad
- **GDPR (Reglamento General de Protección de Datos):** Aunque es una regulación europea, establece estándares internacionales para la protección de datos personales que podrían ser relevantes para IFX Networks si maneja datos de ciudadanos europeos

3 Delitos Informáticos en el Caso IFX Networks

3.1 Identificación de Delitos según la Ley 21.459

En el caso del ataque de ransomware a IFX Networks, podemos identificar los siguientes delitos informáticos según la Ley 21.459 [2]:

Tipo de Delito	Descripción en el Caso
Ataque a la integridad de un sistema informático (Art. 3)	El grupo RansomHouse utilizó ransomware para impedir y obstaculizar el normal funcionamiento de los sistemas informáticos de IFX Networks, afectando servicios críticos como mercadopublico.cl.
Acceso ilícito (Art. 2)	Los atacantes accedieron de manera no autorizada a los sistemas de IFX Networks, vulnerando medidas de seguridad.
Daño informático (Art. 4)	El ransomware provocó la alteración, eliminación o inutilización de datos informáticos.
Receptación de datos informáticos (Art. 7)	Si RansomHouse comercializó o distribuyó datos obtenidos del ataque.
Fraude informático (Art. 6)	La exigencia de un rescate a cambio de restaurar el acceso a los sistemas y datos.
Abuso de dispositivos (Art. 8)	El desarrollo, obtención y distribución de programas informáticos diseñados para la comisión de los delitos anteriores.

3.2 Modalidad “Ransomware as a Service”

Un aspecto particularmente relevante en este caso es la modalidad ‘Ransomware as a Service” utilizada por RansomHouse, donde el código malicioso se alquila a otras partes a cambio de una comisión por cada ataque exitoso. Esta modalidad plantea desafíos adicionales desde el punto de vista legal:

- **Asociación ilícita (Art. 292 del Código Penal):** La estructura organizativa de RansomHouse podría constituir una asociación ilícita para cometer delitos informáticos.
- **Responsabilidad compartida:** Tanto los desarrolladores del ransomware como quienes lo utilizan podrían ser considerados coautores de los delitos.
- **Jurisdicción internacional:** Dado que estos grupos operan a nivel transnacional, se requiere la cooperación internacional amparada en el Convenio de Budapest para su persecución [5].

4 Comparación de Marcos Regulatorios

4.1 Marcos Regulatorios según Tipo de Industria

Según la Política Nacional de Ciberseguridad 2023-2028 [7], los diferentes sectores de la industria deben cumplir con marcos regulatorios específicos:

Tipo de Industria	Marco Regulatorio	Aplicabilidad al Caso
Telecomunicaciones y Proveedores de Servicios Digitales	▪ Ley 21.663 (Ciberseguridad) [3] ▪ Ley General de Telecomunicaciones ▪ Normativas de la Subsecretaría de Telecomunicaciones	IFX Networks, como proveedor de servicios de telecomunicaciones e infraestructura digital, está sujeta a estas regulaciones específicas que establecen estándares de seguridad y continuidad operacional.
Contratación Pública	▪ Ley de Compras Públicas ▪ Normativas de ChileCompra	La plataforma mercadopublico.cl, afectada por el ataque, está sujeta a regulaciones específicas en materia de contratación pública que incluyen requisitos de seguridad y disponibilidad.
Sector Financiero	▪ Normativas de la Comisión para el Mercado Financiero ▪ Estándares PCI DSS (para servicios de pago)	Si el ataque afectó a entidades financieras o servicios de pago que eran clientes de IFX Networks, estas regulaciones serían aplicables.
Sector Salud	▪ Normativas del Ministerio de Salud ▪ Ley 20.584 (Derechos y Deberes de los Pacientes)	En caso de que instituciones de salud hayan sido afectadas por el ataque y se haya comprometido información médica.

4.2 Análisis Comparativo de Normativas Aplicables

Normativa	Enfoque	Obligaciones	Sanciones
Ley 21.663 (Ciberseguridad) [3]	Preventivo y reactivo	▪ Implementar sistemas de gestión de seguridad ▪ Reportar incidentes ▪ Planes de continuidad operacional	Multas de hasta 40.000 UTM para Operadores de Importancia Vital
Ley 21.459 (Delitos Informáticos) [2]	Punitivo	N/A (tipifica delitos)	Penas de privación de libertad y multas
Ley 19.628 (Protección de Datos) [1]	Preventivo y de garantía de derechos	▪ Medidas de seguridad para datos personales ▪ Consentimiento para el tratamiento ▪ Derechos ARCO	Indemnización de perjuicios
Convenio de Budapest [5]	Marco internacional de cooperación	▪ Tipificación homogénea de delitos ▪ Cooperación internacional	Según legislación nacional de cada país

5 Responsabilidades Legales en Delitos Informáticos

5.1 Responsabilidades Penales

De acuerdo con la Ley 21.459 [2], las responsabilidades penales en el caso del ciberataque a IFX Networks recaen principalmente en:

- **Autores directos:** Miembros del grupo RansomHouse que ejecutaron el ataque.
- **Facilitadores:** Personas o entidades que proporcionaron las herramientas para el ataque bajo el modelo Ransomware as a Service".
- **Cómplices:** Quienes, sin ser autores, facilitaron conscientemente los medios para la comisión del delito.

Las penas asociadas varían según el delito específico. Por ejemplo:

- **Ataque a la integridad de un sistema informático:** presidio menor en su grado medio a máximo (541 días a 5 años)
- **Acceso ilícito:** presidio menor en su grado mínimo a medio (61 días a 3 años)
- **Daño informático:** presidio menor en su grado medio a máximo (541 días a 5 años)

5.2 Responsabilidades Civiles

La responsabilidad civil implica la obligación de indemnizar los daños y perjuicios causados y puede recaer en:

- **Atacantes:** Por los daños directos causados por el ciberataque.
- **IFX Networks:** Potencial responsabilidad por negligencia si se demuestra que no implementó medidas de seguridad adecuadas según los estándares de la industria. Según el artículo 2314 del Código Civil, *"El que ha cometido un delito o cuasidelito que ha inferido daño a otro, es obligado a la indemnización"*.[4]

5.3 Responsabilidades Administrativas

En el ámbito administrativo, IFX Networks podría enfrentar:

- **Sanciones bajo la Ley 21.663:** Si se determina que no cumplió con las obligaciones de ciberseguridad aplicables a los Operadores de Importancia Vital [3].
- **Sanciones sectoriales:** Impuestas por reguladores específicos como la Subsecretaría de Telecomunicaciones.
- **Otras medidas administrativas:** Como la obligación de implementar medidas correctivas o planes de remediación.

5.4 Obligaciones Post-Incidente

Tras un incidente como el sufrido por IFX Networks, la normativa vigente establece ciertas obligaciones [3]:

Obligación	Base Legal
Reportar el incidente al CSIRT Nacional	Artículo 9° de la Ley 21.663
Adoptar medidas para reducir el impacto y evitar la propagación	Artículo 8° letra e) de la Ley 21.663
Informar a los potenciales afectados	Artículo 8° letra g) de la Ley 21.663
Colaborar con las autoridades en la investigación	Principio de cooperación con la autoridad (Art. 3° Ley 21.663)
Revisar y actualizar planes de ciberseguridad	Artículo 8° letra c) de la Ley 21.663

6 Tratamiento de Datos Personales

6.1 Obligaciones según la Ley 19.628

La Ley 19.628 sobre Protección de la Vida Privada [1] establece diversas obligaciones en relación al tratamiento de datos personales que son relevantes para el caso de IFX Networks:

- **Deber de seguridad (Art. 11):** El responsable del registro o banco de datos debe cuidar de ellos con la debida diligencia, haciéndose responsable de los daños. En el caso de IFX Networks, esto implica la implementación de medidas técnicas y organizativas adecuadas para proteger los datos personales de sus clientes.
- **Principio de finalidad (Art. 9):** Los datos personales deben utilizarse solo para los fines para los cuales fueron recolectados, a menos que provengan de fuentes accesibles al público.
- **Consentimiento del titular (Art. 4):** El tratamiento de datos personales solo puede realizarse con el consentimiento del titular o cuando la ley lo autorice.
- **Deber de confidencialidad (Art. 7):** Las personas que trabajan en el tratamiento de datos personales están obligadas a guardar secreto sobre los mismos.

6.2 Impacto del Ciberataque en la Protección de Datos

El ataque de ransomware a IFX Networks pudo haber comprometido datos personales de sus clientes, lo que generaría las siguientes implicaciones según la normativa vigente [1]:

- **Violación de seguridad de datos:** El ataque constituye una brecha de seguridad que podría haber expuesto datos personales.
- **Responsabilidad por daños:** IFX Networks podría ser responsable por los daños causados a los titulares de los datos comprometidos, especialmente si se demuestra que no implementó medidas de seguridad adecuadas.
- **Obligación de notificación:** Aunque la Ley 19.628 no contempla específicamente la obligación de notificar brechas de seguridad, la Ley 21.663 [3] sí establece esta obligación para los Operadores de Importancia Vital.

6.3 Derechos de los Titulares de Datos

Los titulares de datos personales que pudieron haber sido afectados por el ciberataque tienen los siguientes derechos según la Ley 19.628 [1]:

Derechos ARCO

- **Derecho de Acceso (Art. 12):** Derecho a exigir información sobre los datos relativos a su persona, su procedencia y destinatario, y el propósito del almacenamiento.
- **Derecho de Rectificación (Art. 12):** Derecho a que se modifiquen los datos erróneos, inexactos, incompletos o desactualizados.
- **Derecho de Cancelación (Art. 12):** Derecho a que se eliminen los datos cuyo almacenamiento carece de fundamento legal o cuando estén caducos.
- **Derecho de Oposición (Arts. 3 y 12):** Derecho a oponerse al tratamiento de sus datos personales cuando no ha otorgado consentimiento.

En el contexto del ataque a IFX Networks, los titulares de datos podrían ejercer estos derechos para conocer si sus datos fueron comprometidos y qué medidas se han tomado para protegerlos.

7 Conclusiones

El análisis del ciberataque a IFX Networks revela varias conclusiones importantes respecto a la aplicación de normativas y regulaciones de ciberseguridad:

1. **Marco normativo en evolución:** Chile ha avanzado significativamente en materia de ciberseguridad con la promulgación de la Ley 21.663 [3] y la Ley 21.459 [2], alineándose con estándares internacionales como el Convenio de Budapest [5]. Sin embargo, el caso IFX Networks demuestra que aún existen desafíos en la implementación efectiva de estas normativas.

2. **Responsabilidades compartidas:** La ciberseguridad no es responsabilidad exclusiva de un actor. Tanto los proveedores de servicios como IFX Networks, las autoridades reguladoras y los usuarios finales tienen roles y responsabilidades específicas en la prevención y gestión de incidentes. La Política Nacional de Ciberseguridad 2023-2028 [7] enfatiza este enfoque de responsabilidad compartida.

3. **Importancia de la gestión preventiva:** El incidente subraya la importancia de implementar medidas preventivas robustas, especialmente para operadores de servicios esenciales. Las obligaciones establecidas en la Ley 21.663 para los Operadores de Importancia Vital buscan precisamente reforzar este enfoque preventivo [3].

4. **Desafíos en la persecución de ciberdelitos:** La naturaleza transnacional del grupo RansomHouse y su modelo de Ransomware as a Service"plantea desafíos significativos para la persecución penal, evidenciando la necesidad de una cooperación internacional efectiva bajo marcos como el Convenio de Budapest [5].

5. **Protección de datos como prioridad:** El caso demuestra que la protección de datos personales debe ser una prioridad en las estrategias de ciberseguridad, no solo por las obligaciones legales bajo la Ley 19.628 [1], sino también por el impacto reputacional y financiero que puede tener una brecha de datos.

El marco normativo y regulatorio chileno ha avanzado significativamente con la Ley Marco de Ciberseguridad [3] y la actualización de la Ley de Delitos Informáticos [2], proporcionando herramientas más efectivas para abordar incidentes como el ataque a IFX Networks. Sin embargo, la efectividad de estas normativas dependerá de su correcta implementación, de la capacidad técnica de las organizaciones y de la coordinación entre los diferentes actores del ecosistema de ciberseguridad, tal como lo destaca el CSIRT de Gobierno en su alerta sobre este incidente [6].

La experiencia de IFX Networks debe servir como un llamado de atención para todas las organizaciones, especialmente aquellas que gestionan infraestructuras críticas o datos sensibles, sobre la importancia de adoptar un enfoque proactivo en materia de ciberseguridad, cumpliendo no solo con las obligaciones legales mínimas sino implementando las mejores prácticas de la industria.

Referencias

[1] Biblioteca del Congreso Nacional de Chile. *Ley 19.628: Sobre protección de la vida privada*. Legislation. 1999. URL: https://www.bcn.cl/leychile/navegar?idNorma=141599.

[2] Biblioteca del Congreso Nacional de Chile. *Ley 21.459: Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest*. Legislation. 2022. URL: https://www.bcn.cl/leychile/navegar?idNorma=1177743.

[3] Biblioteca del Congreso Nacional de Chile. *Ley 21.663: Ley Marco de Ciberseguridad*. Legislation. 2024. URL: https://www.bcn.cl/leychile/navegar?idNorma=1197626.

[4] *Código Civil de la República de Chile*. Santiago de Chile: Editorial Jurídica de Chile, edición actualizada. URL: https://www.bcn.cl/leychile/navegar?idNorma=172986.

[5] Consejo de Europa. *Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest)*. International Treaty. 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[6] CSIRT de Gobierno de Chile. *Alerta de seguridad cibernética: Ataque de ransomware a IFX Networks*. Security Alert. CSIRT de Gobierno de Chile, 2023. URL: https://csirt.gob.cl/alertas/10cnd23-00108-01/.

[7] Gobierno de Chile. *Política Nacional de Ciberseguridad 2023-2028*. Policy Document. Gobierno de Chile, 2023. URL: https://anci.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf.