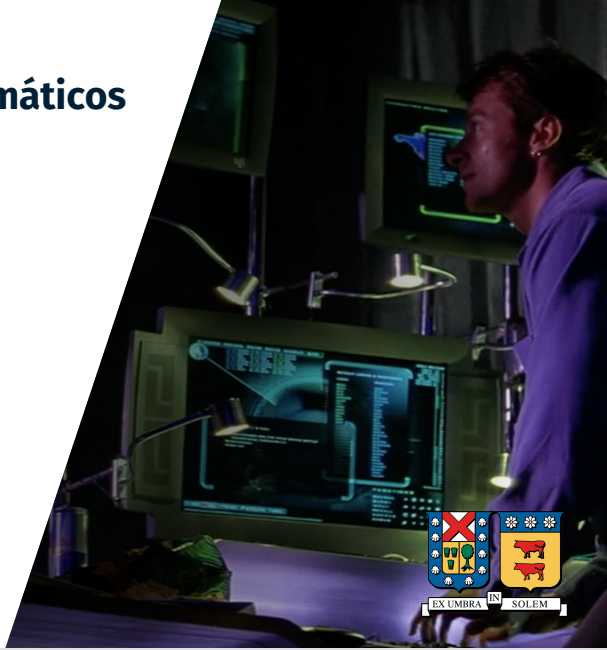
Ley 21.459: Ley de Delitos Informáticos



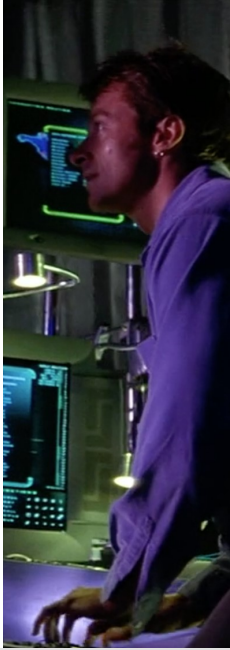
Informática Legal y Derecho Informático
INF300 - 2025-2

Toledo Correa, Pedro

Departamento de Informática
Universidad Técnica Federico Santa María

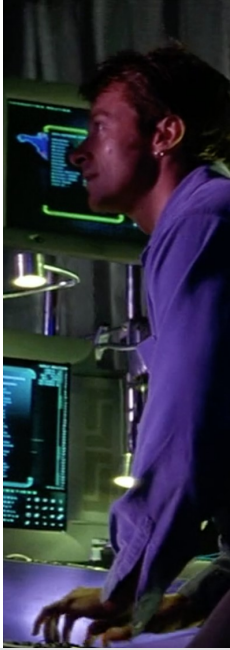
15 de octubre de 2025 - v1.0

Tabla de contenidos



Ley 21.459

- **Ley 19.223**
  TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA (1993)[1]
- **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 (2022)[2]
- **Tratado 135 del Consejo de Europa**[3]
  Convención sobre el cibercrimen



[1] https://www.bcn.cl/leychile/navegar?idNorma=30590

[2] https://www.bcn.cl/leychile/navegar?idNorma=1177743

[3] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Contenido

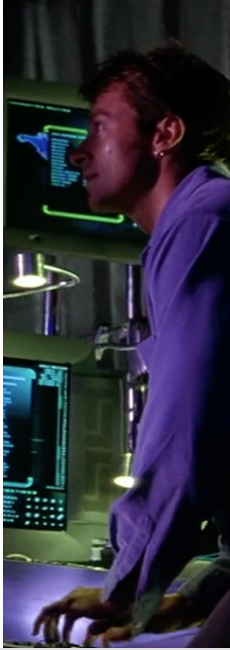
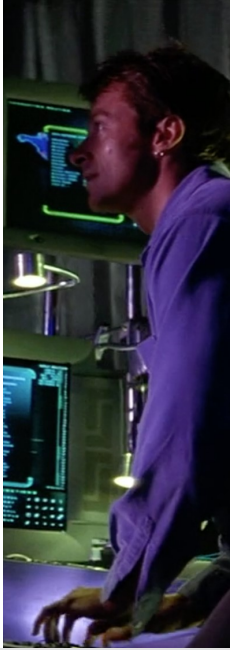
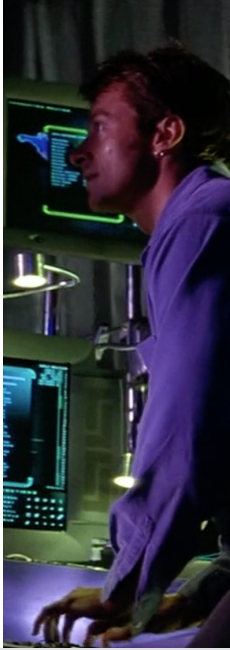


Tabla de contenidos



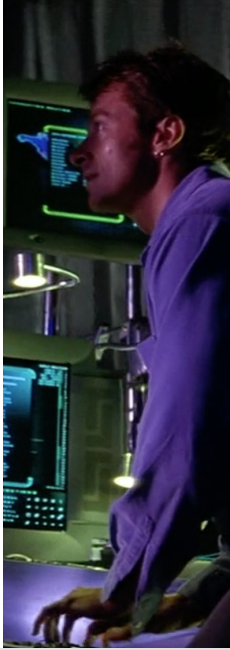
Convenio de Budapest

- Convenio sobre Ciberdelincuencia
- Primer tratado internacional dedicado a combatir los delitos informáticos y la criminalidad en el ciberespacio
- Adoptado por el Consejo de Europa en 2001, con participación de países no europeos como Estados Unidos, Japón y Canadá
- Enfoque en la armonización de leyes, mejora de la cooperación internacional y fortalecimiento de capacidades técnicas para enfrentar el cibercrimen



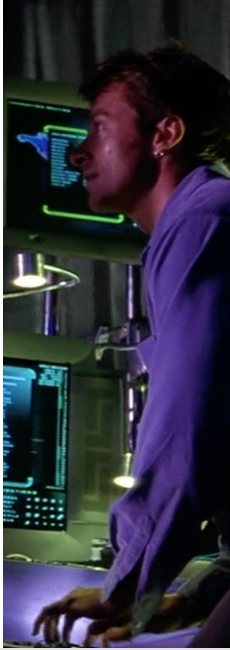
Orígenes

- Surge ante el crecimiento exponencial de los delitos informáticos en la década de 1990
- Elaborado por el Consejo de Europa con contribuciones de otros países, incluidas naciones de fuera del continente europeo
- Adoptado el 23 de noviembre de 2001, entró en vigor el 1 de julio de 2004
- Primer tratado en establecer una base legal para la cooperación internacional contra el cibercrimen



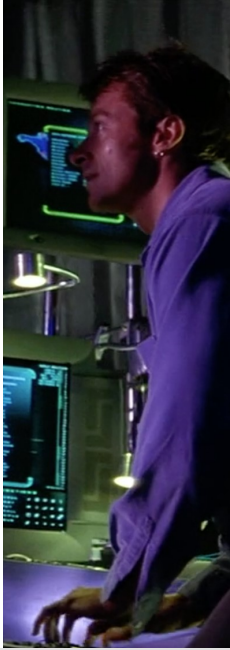
Objetivos

- Definir y tipificar los delitos informáticos de manera uniforme entre los países firmantes
- Establecer procedimientos efectivos para la recopilación de pruebas digitales, protegiendo los derechos humanos y las libertades fundamentales
- Fortalecer la cooperación y asistencia internacional para investigar y procesar los delitos cibernéticos
- Fomentar el intercambio de información y experiencias entre países para mejorar la capacidad de respuesta



Chile y el Convenio

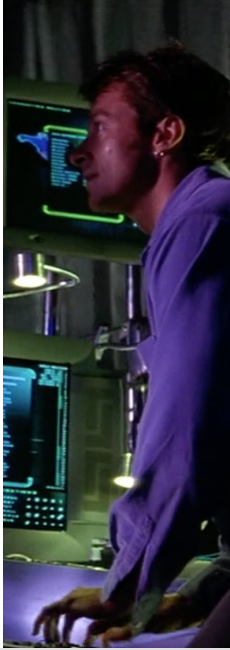
- Chile ratifica el convenio como estado No Miembro del Concejo de Europa[4]
  - 2017/04/20 Ratifica
  - 2017/08/01 Entra en vigencia
- Declaraciones
  - Artículos 2 y 3 en la ley 19.223
  - Artículo 127 en el Artículo 187 del Código Penal



[4] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Chile y el Convenio
Reservas

- Artículo 4.2
- Artículo 6.1
- Articulo 9.2.b y 9.2.c
- Articulo 22.1.b[5]
- Articulo 29.4[6]



[5] A bordo de un buque

[6] Denegación de conservación de evidencia cuando no se cumple doble tipificación penal

Chile y el Convenio
Autoridades

- Artículo 24.7 - Extradiciones
  Ministerio de Relaciones Exteriores
- Artículo 27.2.1 - Asistencia
  Ministerio Público, Unidad de Extradicción y Cooperación Internacional
- Artículo 35 - Asistencia
  Ministerio Público, Unidad de Extradicción y Cooperación Internacional

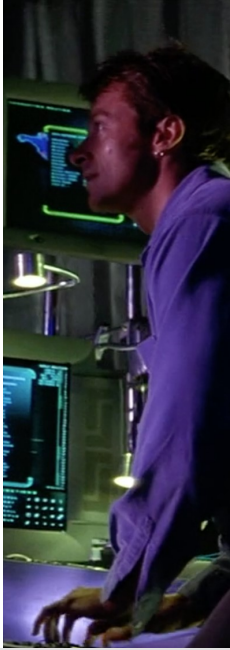
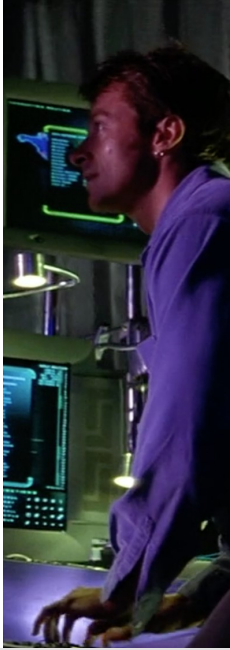
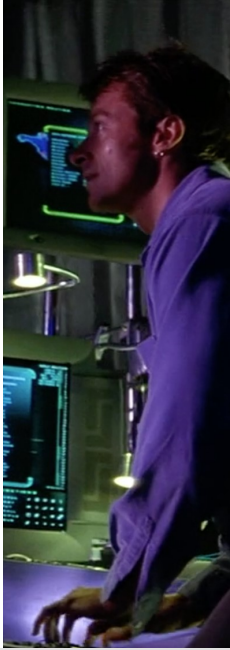


Tabla de contenidos



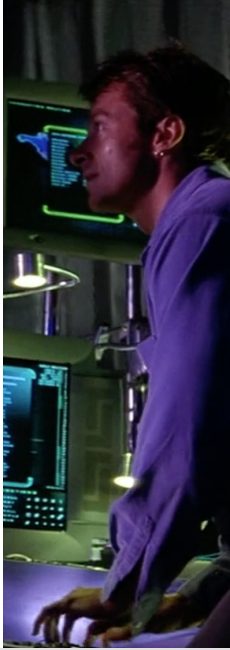
Artículo 1: Definiciones - Sistema informático

“computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;



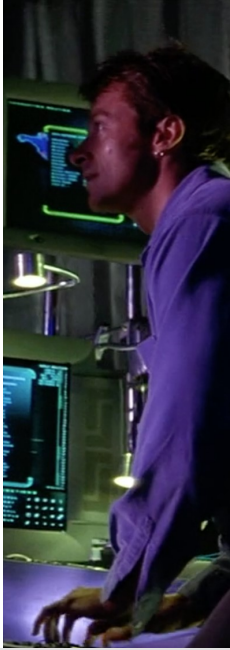
Artículo 1: Definiciones - Datos informáticos

“computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;



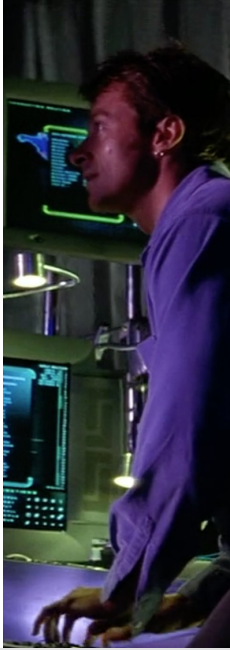
Artículo 1: Definiciones - Proveedor de servicio

“service provider” means:
i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.



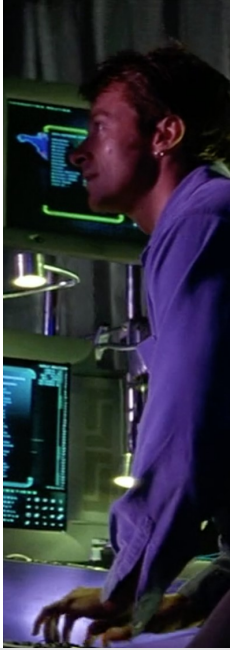
Artículo 1: Tráfico de datos

“traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.



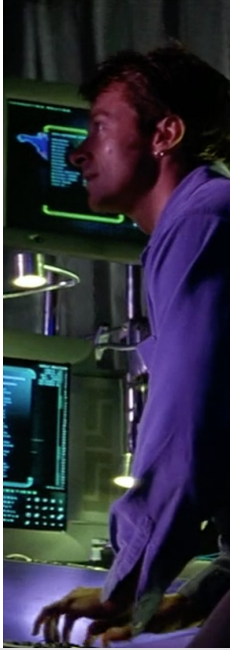
Artículo 2: Acceso ilegal a sistemas informáticos

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.



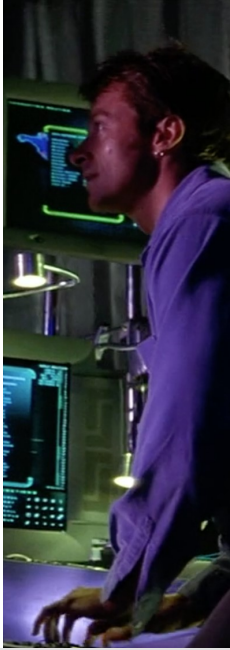
Artículo 2: Acceso ilegal a sistemas informáticos

- Tipificación del delito de acceso ilegal a sistemas informáticos
- Requisitos para la punibilidad de esta conducta
- Excepciones y circunstancias atenuantes



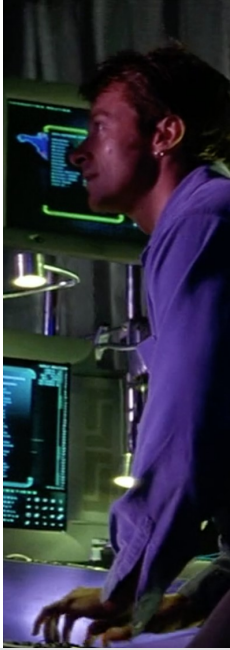
Artículo 3: Intercepción en sistemas informáticos

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.



Artículo 3: Intercepción en sistemas informáticos

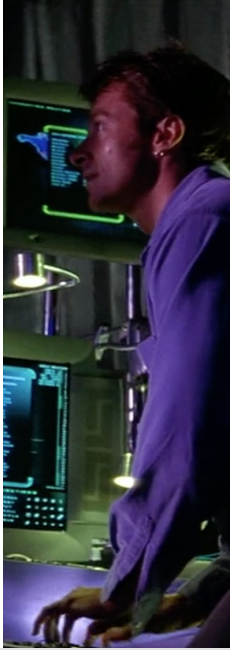
- Definición de interferencia en sistemas informáticos
- Requisitos para la punibilidad de esta conducta
- Consideraciones sobre daños y perjuicios



Artículo 4: Interferencia en datos informáticos

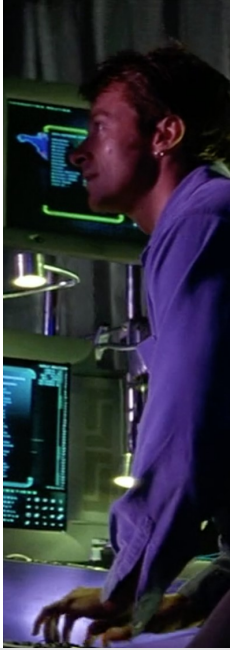
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.



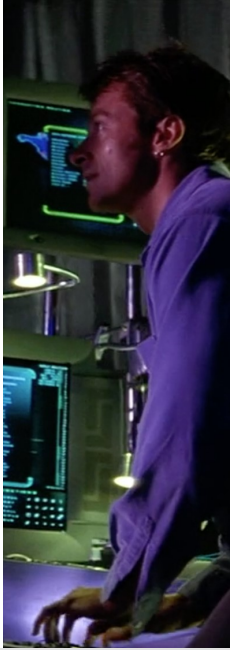
Artículo 4: Interferencia en datos informáticos

- Definición de interferencia en datos informáticos
- Requisitos para la punibilidad de esta conducta
- Tipos de interferencia cubiertos
- Chile se reserva el no aplicar el párrafo segundo



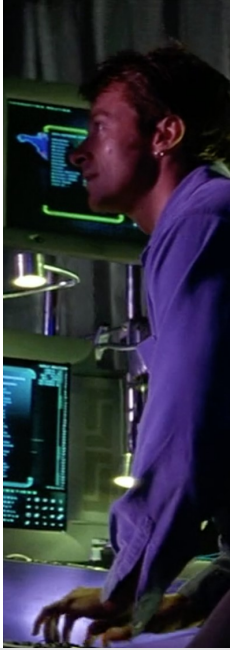
Artículo 5: Interferencia en sistemas informáticos

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.



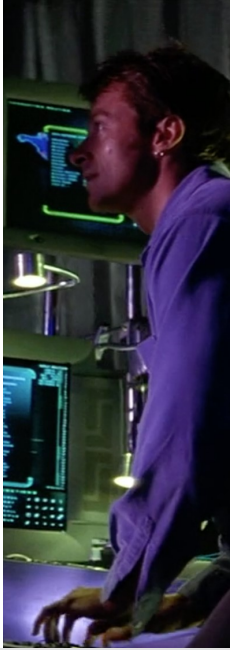
Artículo 5: Interferencia en sistemas informáticos

- Definición de interferencia en sistemas informáticos
- Requisitos para la punibilidad de esta conducta
- Tipos de interferencia cubiertos



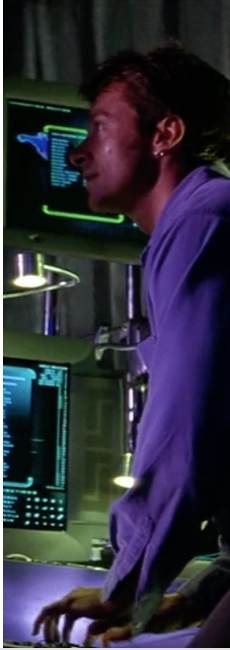
Artículo 6: Abuso de dispositivos

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right...



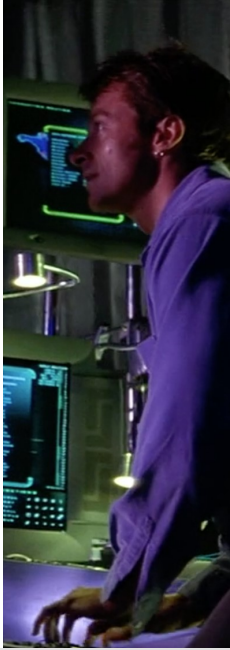
Artículo 6: Abuso de dispositivos

- Tipificación del abuso de dispositivos informáticos
- Producción, venta, obtención para uso propio o distribución de dispositivos
- Excepciones y circunstancias atenuantes
- Chile se reserva el no aplicar el párrafo primero



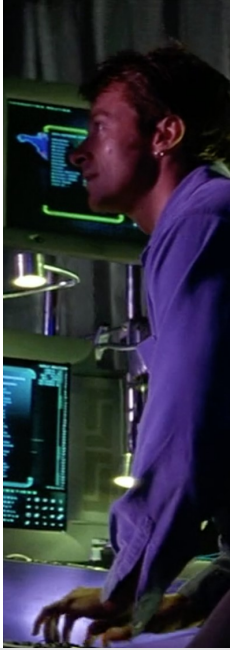
Artículo 7: Falsedad informática

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.



Artículo 7: Falsedad informática

- Definición de falsedad informática
- Requisitos para la punibilidad de esta conducta
- Casos de manipulación de datos informáticos



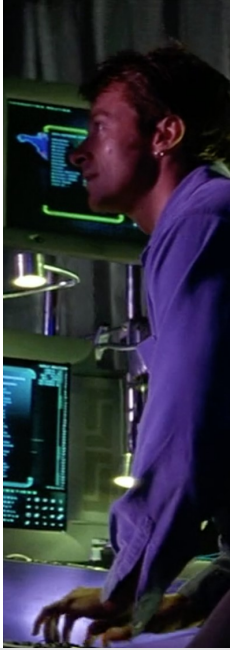
Artículo 8: Fraude informático

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

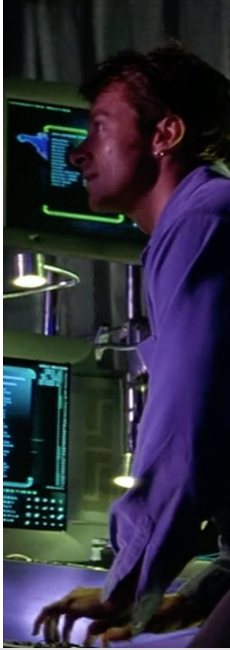
b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.



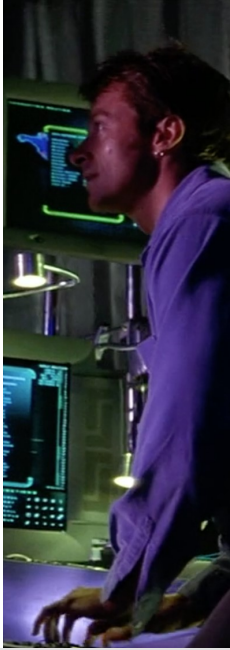
Artículo 8: Fraude informático

- Definición de fraude informático
- Requisitos para la punibilidad de esta conducta
- Casos de uso indebido de dispositivos o datos informáticos



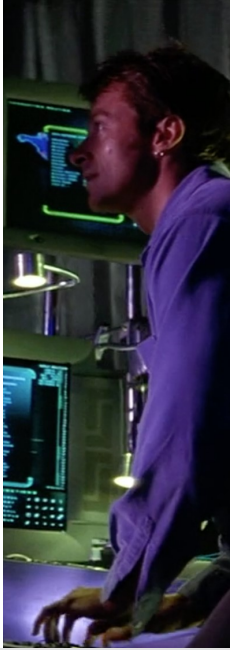
Artículo 9: Pornografía infantil

- Definición de pornografía infantil en entornos digitales
- Tipificación de delitos relacionados con pornografía infantil
- Obligaciones de los Estados para combatir este tipo de delitos
- Chile se reserva el no aplicar los incisos 2.b y 2.c



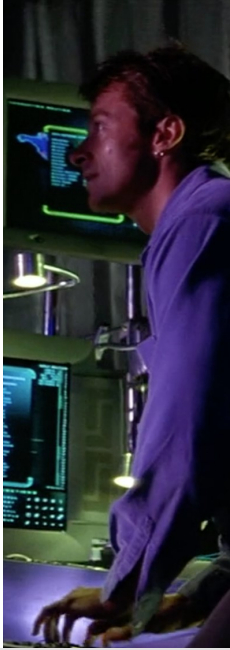
Artículo 10: Delitos relacionados con infracciones de derechos de autor

- Definición de delitos relacionados con derechos de autor en entornos digitales
- Requisitos para la punibilidad de estas conductas
- Armonización con leyes nacionales sobre propiedad intelectual



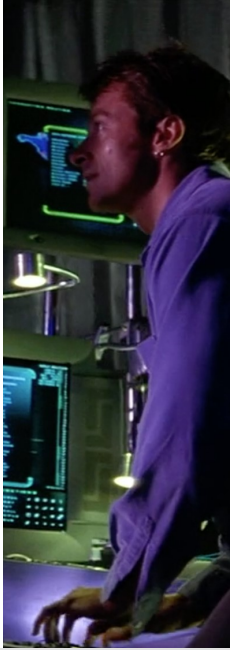
Artículo 11: Jurisdicción

- Establecimiento de jurisdicción para los delitos cibernéticos
- Criterios de territorialidad, nacionalidad y residencia
- Cooperación entre Estados para evitar conflictos de jurisdicción



Artículo 12: Responsabilidad de las personas jurídicas

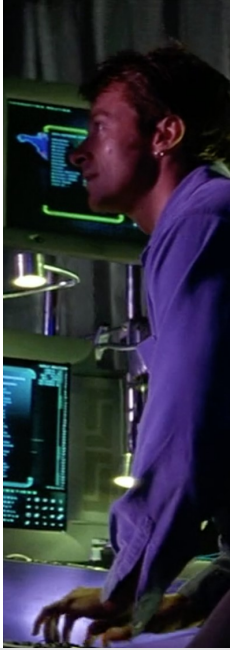
- Responsabilidad penal o de otro tipo de las personas jurídicas
- Sanciones aplicables a las personas jurídicas
- Medidas de supervisión y control



Artículo 13: Sanciones y medidas

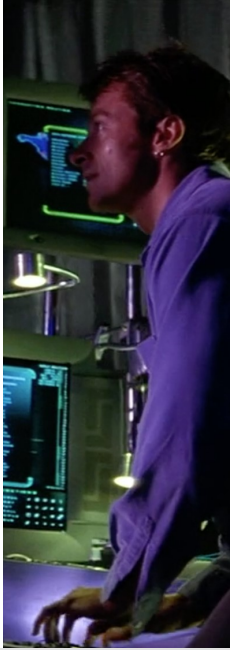
1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.



Artículo 13: Sanciones y medidas

- Establecimiento de sanciones penales efectivas, proporcionales y disuasorias
- Aplicación de medidas como el decomiso y la confiscación
- Consideraciones sobre la gravedad de los delitos



Contenido

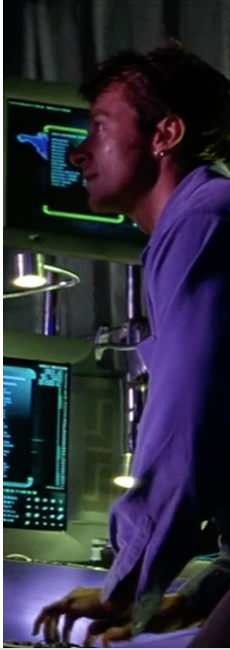
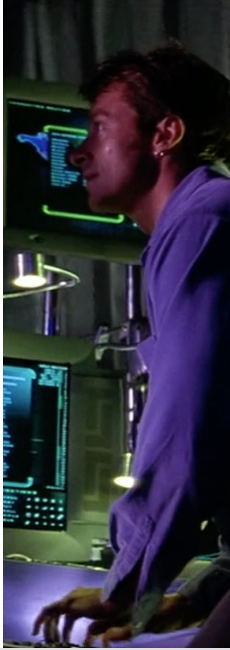
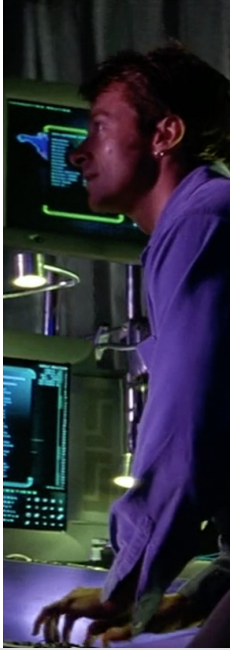


Tabla de contenidos



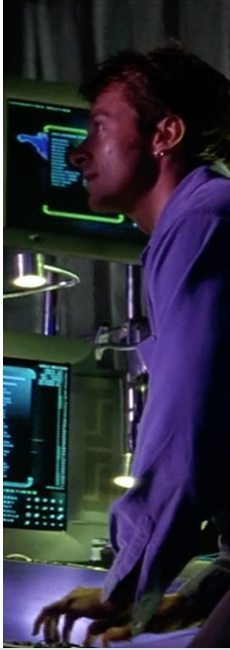
Antecedentes históricos

- **Ley 19.223 (1993)**
  - Primera legislación chilena sobre delitos informáticos
  - Marco normativo básico para abordar criminalidad digital emergente
  - Tipificación limitada de conductas cibernéticas
  - Necesidad de actualización ante el avance tecnológico
- **Evolución tecnológica**
  - Crecimiento exponencial del uso de Internet y dispositivos digitales
  - Sofisticación de métodos de ciberdelincuencia
  - Internacionalización de los delitos informáticos



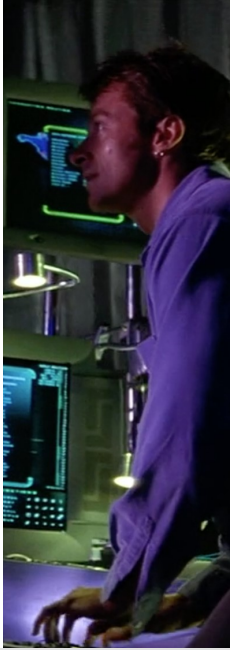
Convenio de Budapest: Motor de cambio

- **Ratificación de Chile (2017)**
  - Compromiso internacional de modernizar legislación
  - Armonización con estándares internacionales
  - Mejora de la cooperación internacional
- **Obligaciones derivadas del Convenio**
  - Tipificación de nuevos delitos informáticos
  - Establecimiento de procedimientos de investigación
  - Fortalecimiento de capacidades técnicas y judiciales
  - Cooperación en intercambio de información y evidencia



Proceso legislativo

- **Necesidad de reforma integral**
  - Obsolescencia de la Ley 19.223
  - Vacíos legales en nuevas modalidades delictivas
  - Presión internacional por cumplimiento del Convenio
- **Elaboración y tramitación**
  - Participación de expertos en ciberseguridad
  - Consulta con organismos internacionales
  - Análisis de experiencias comparadas



Principales innovaciones

- **Ampliación del catálogo de delitos**
  - Nuevas figuras penales acordes al Convenio de Budapest
  - Tipificación específica de ataques a sistemas críticos
  - Inclusión de delitos relacionados con dispositivos maliciosos
- **Modernización de definiciones**
  - Conceptos técnicos actualizados
  - Adaptación a nuevas tecnologías
  - Clarificación de elementos constitutivos
- **Fortalecimiento procedimental**
  - Herramientas de investigación más efectivas
  - Cooperación internacional mejorada

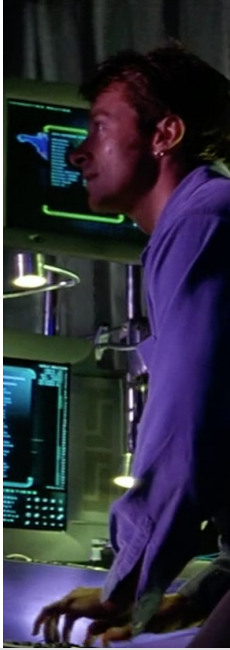
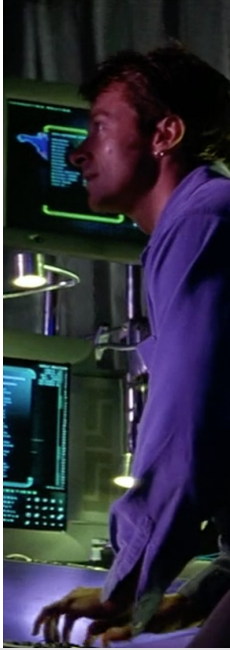
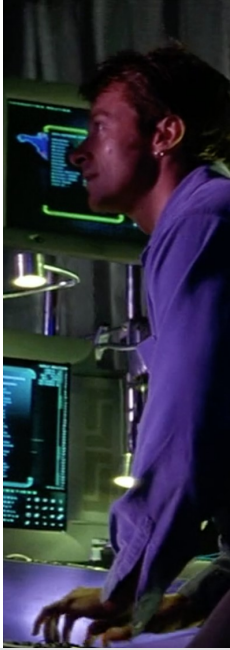


Tabla de contenidos



Penas en Chile

- Prisión en su grado mínimo
  1 día a 60 días
- Presidio o reclusión menor
  - Grado mínimo
    61 días a 540 días
  - Grado medio
    541 días a 3 años
  - Grado máximo
    3 años y un día a 5 años
- Presidio o reclusión mayor
  - Grado mínimo
    5 años y un día a 10 años
  - Grado medio
    10 años y un día a 15 años
  - Grado máximo
    15 años y un día a 20 años



Penas en Chile

- Presidio perpetuo
  - Simple
    Permite solicitar libertad condicional después de cumplir 20 años de reclusión efectiva
  - Calificado
    Permite solicitar libertad condicional después de cumplir 40 años de reclusión efectiva

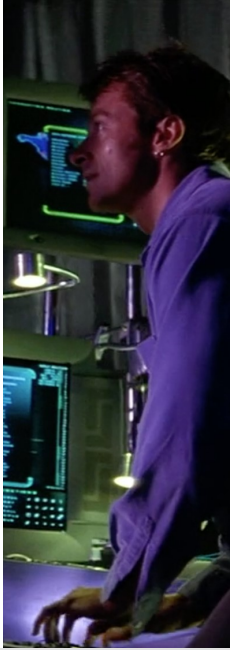
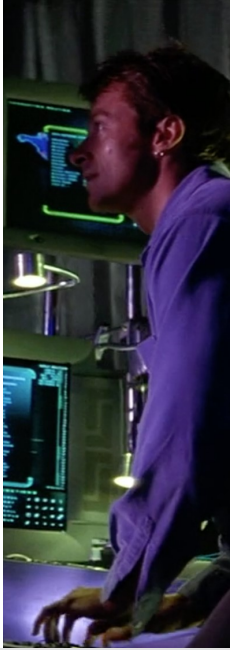
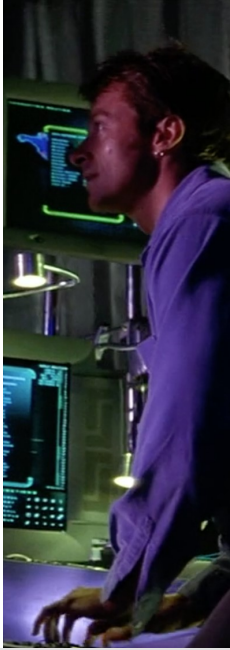


Tabla de contenidos



Artículo 1

Ataque a la integridad de un sistema informático
El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en sus grados medio a máximo.

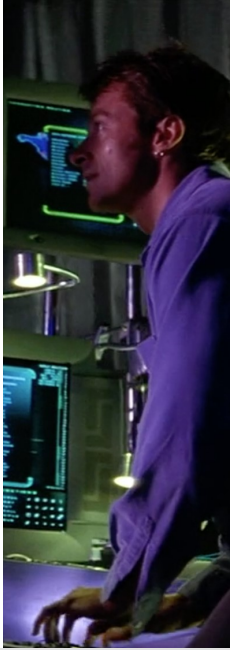


Artículo 2

Acceso ilícito

El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

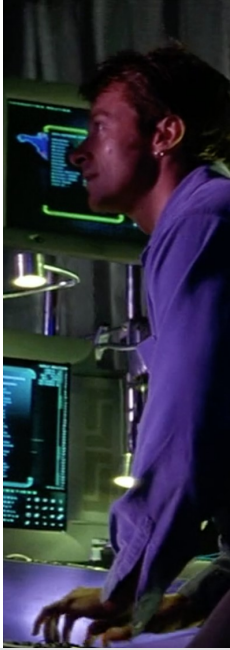


Artículo 3

Interceptación ilícita

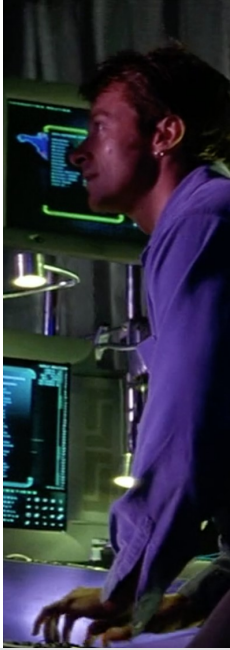
El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.

El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo.



Artículo 4

Ataque a la integridad de los datos informáticos
El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.

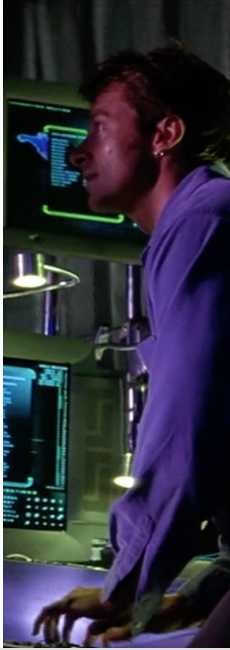


Artículo 5

Falsificación informática

El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.

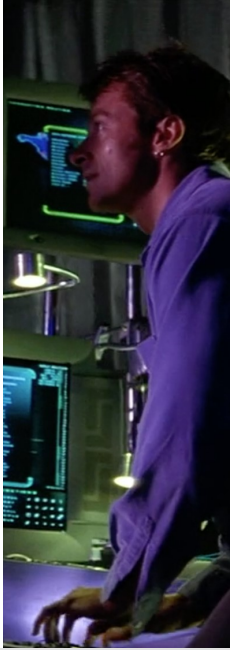
Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.



Artículo 6

Receptación de datos informáticos

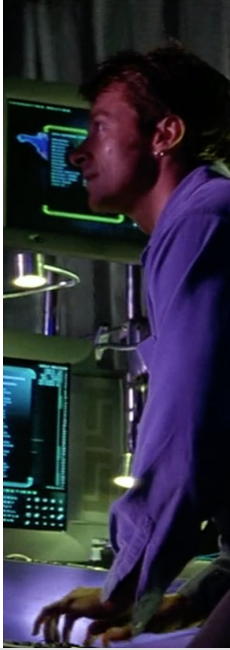
El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.



Artículo 7

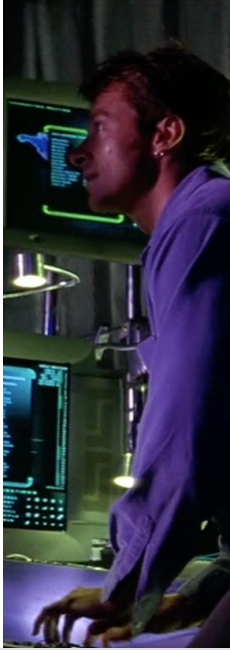
Fraude informático

El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule 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, será penado con distintas penas de presidio y multas, dependiendo del valor del perjuicio.



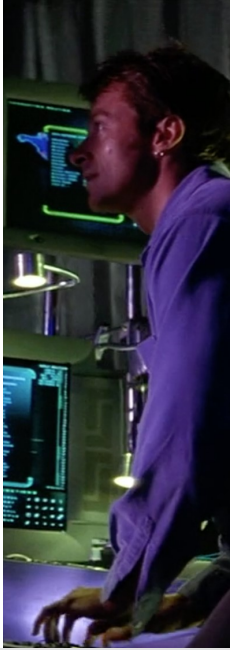
Artículo 8

Abuso de los dispositivos
El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales.



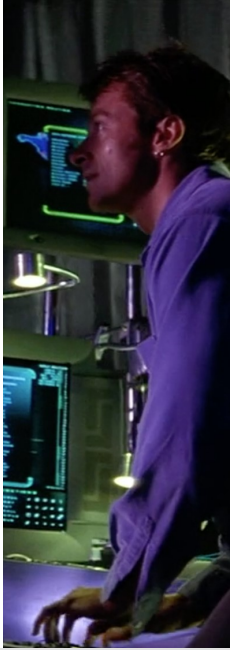
Artículo 9

- Derogado por Ley 21694, artículo tercero, D.O. 04.09.2024.
- Referencia original: https://www.bcn.cl/leychile/navegar?idNorma=1177743&idVersion=2022-06-20
- Ley que modifica: https://www.bcn.cl/leychile/navegar?idNorma=1206373



Artículo 10

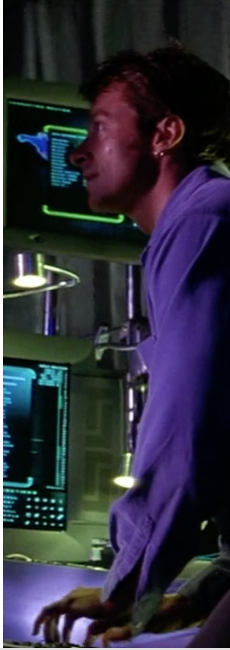
Circunstancias agravantes
Constituyen circunstancias agravantes de los delitos de que trata esta ley:
1) Cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función.
2) Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.
Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, la pena correspondiente se aumentará en un grado.



Artículo 15 - Datos Informáticos

Datos informáticos

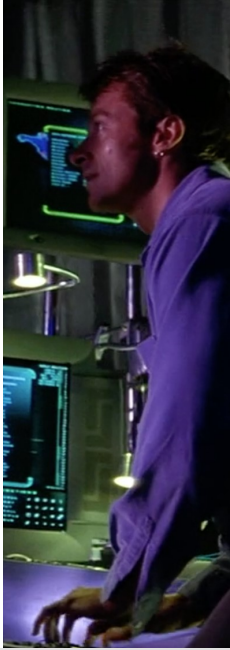
Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.



Artículo 15 - Sistema Informático

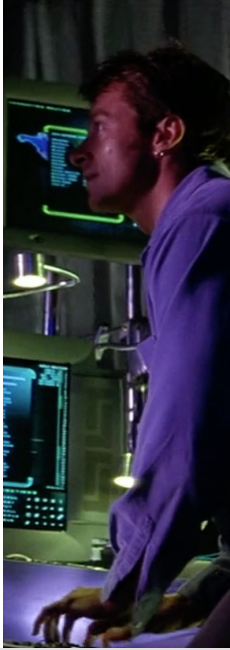
Sistema informático

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.



Artículo 15 - Prestadores de Servicios

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.



¿Preguntas?

Fotografía de fondo:
The Avocado
Plantilla del tema:
https://github.com/ptoledo-teaching/pt-slides