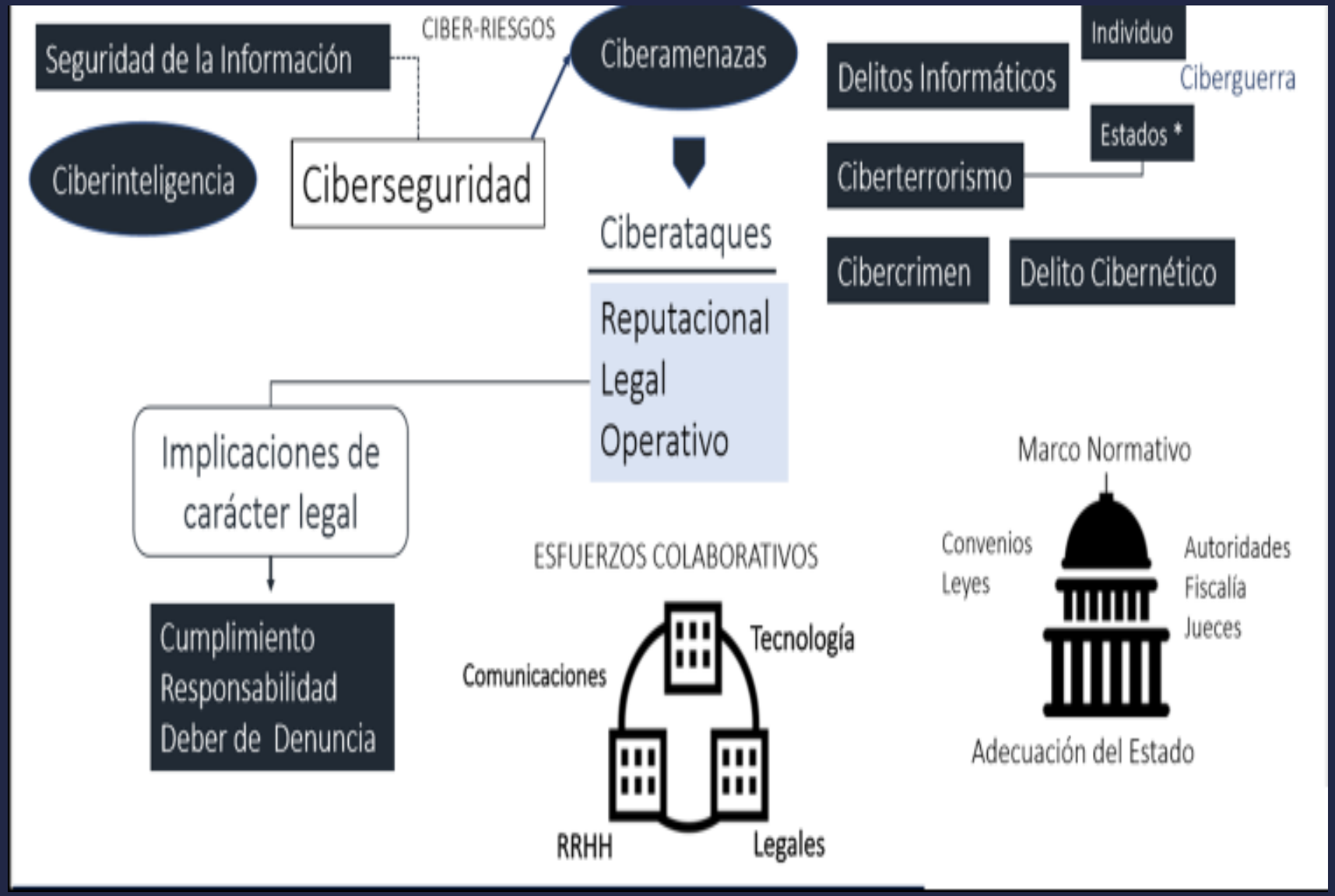
DELITOS A LA SEGURIDAD DE LAS REDES Y DE LOS SISTEMAS INFORMATICOS

Ing. Hernán José Zepeda Castro

Abog. Carlos Gustavo Quiroz

LA SEGURIDAD DE LAS REDES INFORMÁTICAS



TIPOS DE DELITOS INFORMATICOS (EN EL AMBITO INTERNACIONAL)

Clasificación según el "Convenio sobre la Ciberdelincuencia" de 1 de Noviembre de 2001

Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en Noviembre de 2001 se firmó en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa".

Este convenio es de obligatorio cumplimiento para todos los Estados que ratifican el mismo.

En este convenio se propone una clasificación de los delitos informáticos en cuatro grupos:

DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS

1. Acceso ilícito a sistemas informáticos.
2. Interceptación ilícita de datos informáticos.
3. Interferencia en el funcionamiento de un sistema informático.
4. Abuso de dispositivos que faciliten la comisión de delitos

Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger

DELITOS INFORMÁTICOS

1. Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
2. Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

DELITOS RELACIONADOS CON EL CONTENIDO

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

DELITOS RELACIONADOS CON INFRACCIONES DE LA PROPIEDAD INTELECTUAL Y DERECHOS AFINES

Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en Enero de 2008 se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa" que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

Difusión de material xenófobo o racista.

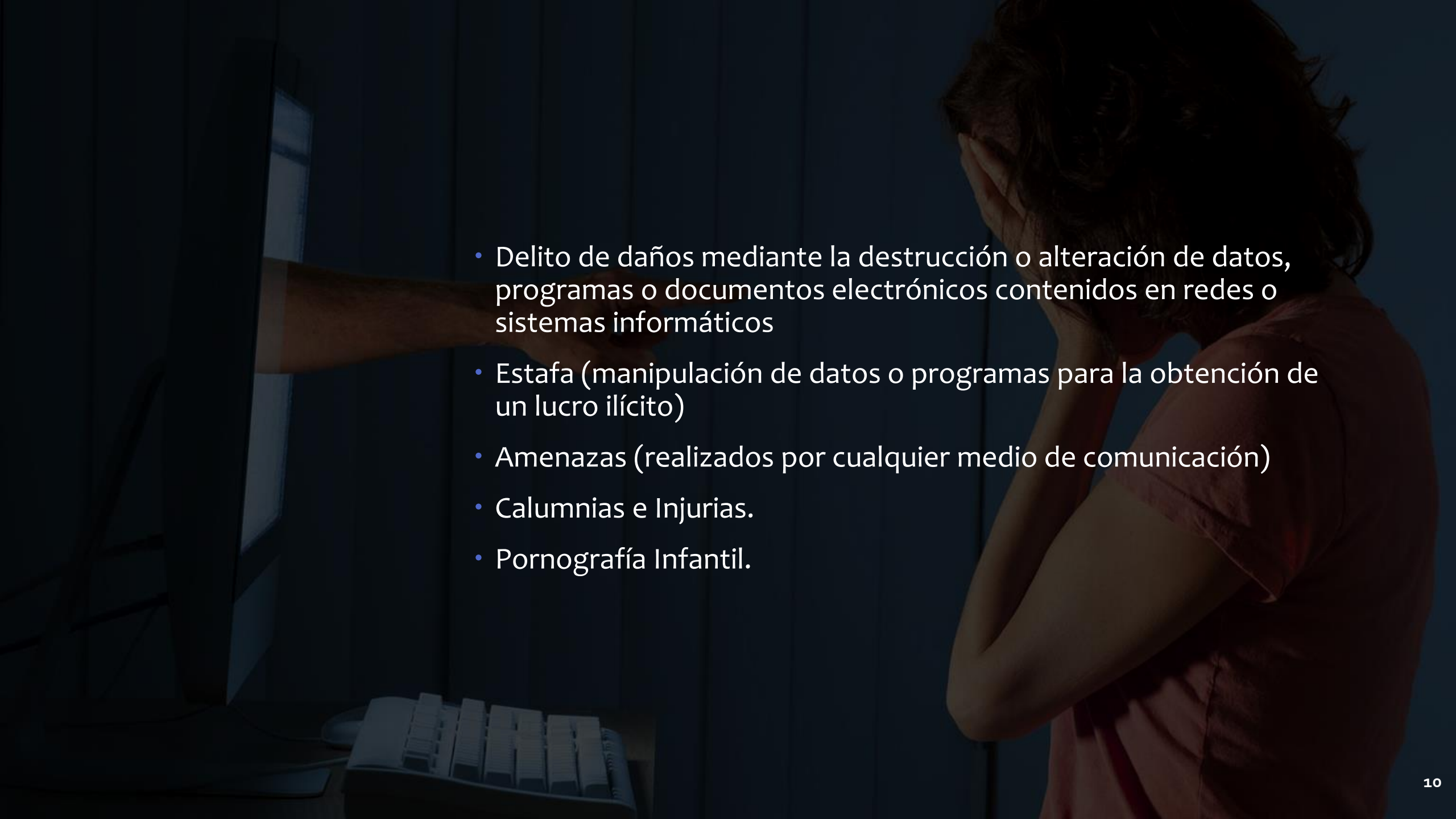
Insultos o amenazas con motivación racista o xenófoba.

Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

LA UTILIZACION DE LA INTERNET PARA LA COMISION DE DELITOS, VULNERA LOS SIGUIENTES DERECHOS:

- **Derecho a la intimidad** (derecho de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos.
- **Derecho a la propiedad intelectual, protección a los derechos de autor** (copia u distribución no autorizada de programas de ordenador y tendencia de medios para suprimir dispositivos utilizados para proteger dichos programas)

- **FALSIFICACIONES** (DOCUMENTOS COMO SOPORTE MATERIAL QUE EXPRESE O INCORPORE DATOS, FALSIFICACION DE TARJETAS DE DEBITO Y CREDITO, ELABORACION DE PROGRAMAS DE ORDENADOR QUE BUSCAN DUPLICAR INFORMACION PARA LUEGO UTILIZARLA CON FINES DELICTIVOS)



- Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos
- Estafa (manipulación de datos o programas para la obtención de un lucro ilícito)
- Amenazas (realizados por cualquier medio de comunicación)
- Calumnias e Injurias.
- Pornografía Infantil.

EN EL AMBITO NACIONAL

- Se determina en el código Penal la imposición de medidas de prisión y multas a las personas que infrinjan lo establecido en este código y las leyes especiales (ley derechos de autor y derechos conexos, ley de propiedad intelectual, así como la seguridad de las redes y de los sistemas informaticos)

ES IMPORTANTE RESALTAR QUE EN LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL E INDUSTRIAL (PROPIEDAD INTELECTUAL, PROPIEDAD INDUSTRIAL, SEGURIDAD DE LAS REDES Y DE LOS SISTEMAS INFORMATICOS) CONVERGEN SITUACIONES COMUNES A SER LAS SIGUIENTES:

a) Utilización de medios tecnológicos de difusión (comunicación y publicidad)
b) Explotación ilícita de una marca u obra.
c) Finalidad comercial.
d) Animo de lucro para quien lo utiliza.
e) Perjuicios a terceros (duelos de las obras o marcas)
f) El común denominador de estos delitos es que se carece de autorización o consentimiento para la utilización de dichas obras o marcas.

DELITOS CONTRA LA PROPIEDAD INTELECTUAL

Art. 389 Contra el derecho de autor y los derechos conexos: Quien con **ánimo de lucro**, en **perjuicio de tercero** y **sin autorización de los titulares** de los correspondientes derechos de autor y conexos o de sus cesionarios: reproduce, distribuye, comunica públicamente o transforma una obra literaria, artística o científica o cualquier prestación o propiedad protegida por derecho de autor y conexos.

De igual manera quien sin autorización del titular y con animo de lucro, almacena, importa o exporta ejemplares de dichas obras, prestaciones, producciones o ejecuciones, cuando estén destinadas a ser distribuidas o comunicadas públicamente.

ALGUNAS AGRAVANTES QUE SE TOMAN EN CUENTA:

Cuando exista plagio, negando la autoriza real de la obra o de partes esenciales de la misma por medio de la atribucion propia o de tercero de su paternidad.

Cuando la explotacion ilicita supone la divulgacion original de la obra en contra de la voluntad del autor y sin estar permitida por la ley de derechos de autor.

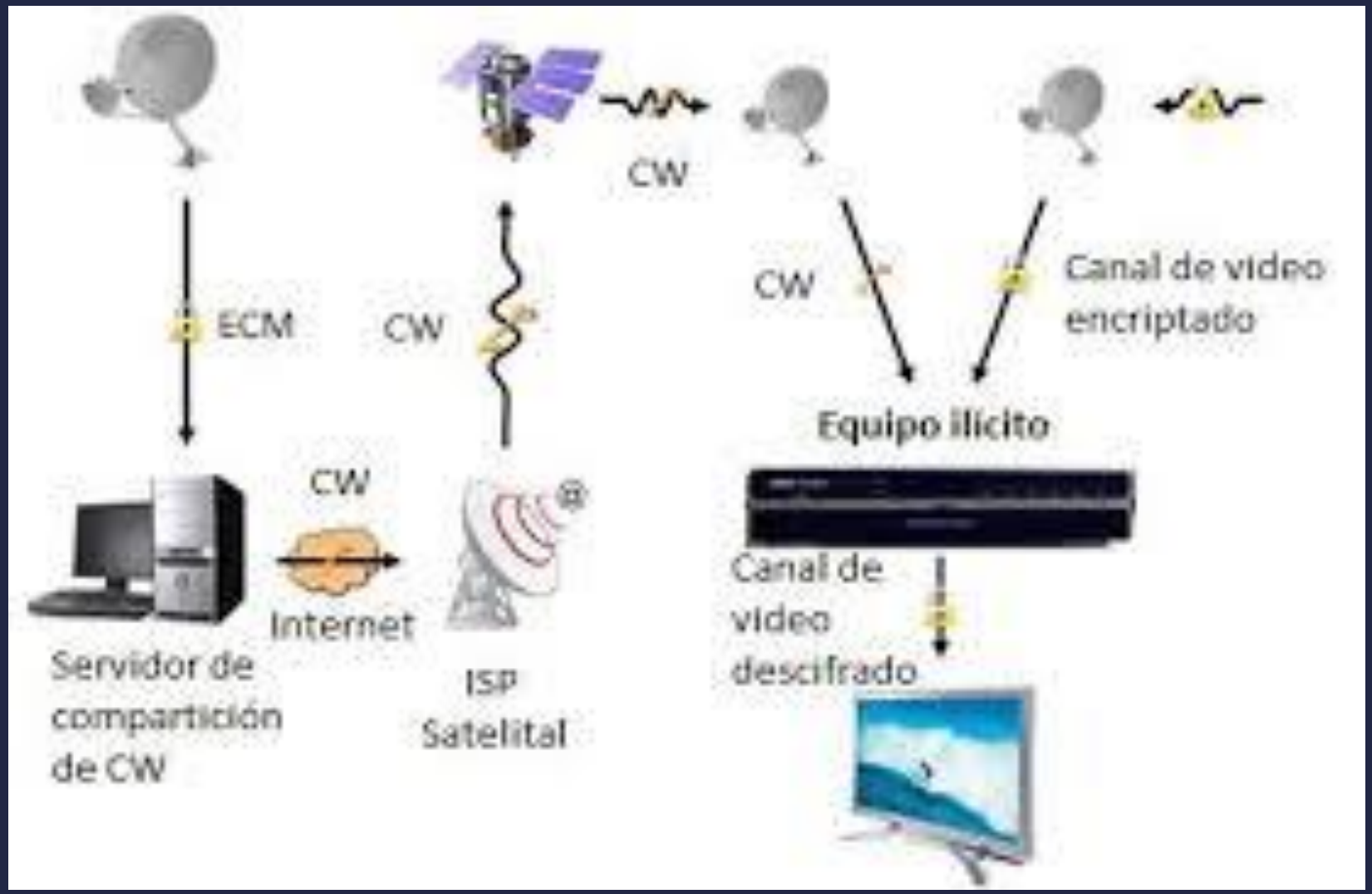
La explotacion ilicita se realiza infringiendo el derecho a la integridad de la obra.

ALGUNAS MUESTRAS DE PLAGIO EN MARCAS

DISFRUTE ILICITO DE SERVICIOS DE ACCESO CONDICIONAL

Art. 391. Quien con ánimo de lucro y sin autorización, facilita el acceso inteligible a un servicio de radiodifusión, sonora o televisiva emitido por la vía electrónica, analógica, digital terrestre, satélite o internet o a servicios interactivos prestados a distancia por vía electrónica.

Quien con ánimo de lucro y sin autorización, fabrica, ensambla, modifica, importa, exporta, vende, arrienda, instala, mantiene, sustituye o de cualquier forma distribuye o comercializa dispositivos o sistemas que sirvan para acceder fraudulentamente a un servicio de acceso condicional.


CW
ECM
CW
CW
Canal de video encriptado
Equipo ilicito
CW
Internet
Canal de video descifrado
Servidor de compartición de CW
ISP Satelital

ELUSION DE MEDIDAS TECNOLOGICAS

Art. 392 Quien sin autorización de los respectivos titulares, con animo de lucro y en perjuicio de tercero elude o evade cualquier medida tecnológica eficaz que esté dirigida a impedir la vulneración de los derechos de autor y derechos conexos.

Se castiga a quien elabora, fabrica, reproduce, distribuye, importa o exporta, o pone a disposición del publico con una finalidad comercial, con animo de lucro y en perjuicio de tercero, cualquier programa, herramienta, medio o procedimiento, dirigido a facilitar de forma ilegitima la supresión o neutralización de cualquier medida tecnológica especialmente destinada a impedir la vulneración del derecho de autor y derechos conexos.

DELITOS CONTRA LA PROPIEDAD INDUSTRIAL

Art. **393 Uso ilegitimo de patente**, quien con fines industriales y comerciales, sin consentimiento del titular de una patente, modelo de utilidad o diseño industrial y con conocimiento de su registro, fabrica, importa, utiliza, ofrece o pone en venta productos o procesos amparados por tales derechos.

Art. 394 Uso ilegitimo de distintivos o marcas registradas quien obteniendo beneficio con fines industriales o comerciales, sin consentimiento del titular de un signo distintivo o de una marca registrada y con conocimiento de su registro, conductas: **1)** fabrica, produce, importa o almacena productos que incorporan un signo distintivo idéntico, similar o confundible con aquel; **2)** ofrece distribuye o comercializa productos que incorporan un signo distintivo idéntico, similar o confundible con aquel.


Gordon's
THE ORIGINAL
Gin
LONDON DRY GIN
Snackrite
Stackers
SALT & VINEGAR
Snackrite
Stackers
ORIGINAL
Snackrite
Stackers
SOUR CREAM & ONION
INSTANT WIN
1 of 4000 £10
MORRISONS VOUCHERS
Pringles
SALT & VINEGAR
INSTANT WIN
1 of 4000 £10
MORRISONS VOUCHERS
Pringles
Original
INSTANT WIN
1 of 4000 £10
MORRISONS VOUCHERS
Pringles
SOUR CREAM & ONION
CANDEREL
TESCO
Low Calorie
Granulated
Sweetener
Aspartame-based
table-top sweetener

DESCUBRIMIENTO Y REVELACION DE SECRETO INDUSTRIAL O COMERCIAL

Art. 395 Quien para obtener ilegalmente un secreto de empresa se apodera por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se referían al mismo, intercepta las comunicaciones o de cualquier otro modo ilegitimo se procura dicha información reservada.

Quien revela o utiliza en provecho propio el secreto de empresa así obtenido; así como quien sin autorización de su titular, revela o utiliza en provecho propio un secreto de empresa al que ha accedido legítimamente pero con deber de reserva.


COMPANY
CLIENTS
DATA
Confidential

DISPOSICIONES COMUNES

Art. 396 Se debe tomar en cuenta algunas circunstancias que agravaran en hecho: **1)** El hecho reviste especial trascendencia económica atendiendo al beneficio obtenido, al perjuicio causado o al valor de los objetos ilícitamente producidos; **2)** El hecho es cometido en el ámbito de un grupo delictivo organizado; **3)** Se utiliza a menores de 18 años para cometer estos delitos.

Art. 397 Responsabilidad de las personas jurídicas, a parte de la pena de clausura de los locales y establecimientos, se pueden imponer otras sanciones: **1)** Suspensión de las actividades especificas en las que se produjo el delito; **2)** Prohibición de realizar en el futuro las actividades especificas en cuyo ejercicio se haya cometido, favoreciendo o encubierto el delito; **3)** Inhabilitación para obtener subvenciones y ayudas publicas para contratar con el sector publico y para gozar de los beneficios e incentivos fiscales o de la seguridad social.

DELITOS RELATIVOS CONTRA LA SEGURIDAD DE LAS REDES INFORMÁTICAS CONCEPTOS GENERALES Y OBJETO DE PROTECCIÓN

¿En qué consiste una red informática? Son dos o más ordenadores conectados entre sí; que comparten recursos:

✓ ya sea de hardware (periféricos, sistemas de almacenamiento…) o;

✓ software (archivos, datos, programas, aplicaciones) ¿Cuál es el propósito de protección de la red informática? Establecer mecanismos de seguridad contra todo tipo de espionajes como el industrial, el sabotaje de sistemas, etc

CONCEPTOS GENERALES

Otra definición de **red informática**: Consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática. Involucra la autorización del acceso a datos en la red, que es controlada por el administrador de la red.

En que consiste un **Programa Informático**: Es la secuencia de instrucciones o indicaciones necesarias para que el sistema informático pueda realizar una función o una tarea u obtener un determinado resultado.

Sistema informático: Es un sistema que permite almacenar y procesar información, es el conjunto de partes interrelacionadas: hardware, software y personal informativo.

El **bien jurídico protegido,** es la información:

✓ como un valor económico,

✓ como un valor intrínseco de la persona

✓ Por el valor de su fluidez y trafico jurídico y;

✓ Por los sistemas que la procesan o automatizan.

ART. 398.- ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS

✓ "… Quien, vulnerando las medidas de seguridad establecidas para impedirlo; accede sin autorización a todo o en parte de un sistema informático…."

CONCEPTOS GENERAL DE UN SISTEMA INFORMATICO (Art.398 NCP)

Consiste en un dispositivo o conjunto de dispositivos interconectados o relacionados entre sí, que permiten, gracias a un programa, el tratamiento automatizado de datos informáticos, de manera que abarca tanto el hardware como el software necesario para su funcionamiento.

Bien Jurídico Protegido en el artículo 398:

La seguridad de la información comprendiéndose esta como:

✓ como un valor económico,

✓ como un valor intrínseco de la persona

✓ Por el valor de su fluidez y trafico jurídico y;

✓ Por los sistemas que la procesan o automatizan.

SUJETOS QUE INTERVIENEN:

Sujetos Activos: Pueden ser:

Cualquier persona, estudiantes, terroristas, figuras del crimen organizado, pueden esconderse en incontables enlaces, desvanecerse sin dejar rastros, despachar directamente comunicaciones, esconder pruebas en paraísos informáticos (países que carecen de leyes o experiencia para seguirles la pista.

Sujetos Pasivos:

Pueden ser: Cualquier persona natural o jurídica

✓ Empresas públicas o privadas

✓ Organizaciones gubernamentales o no gubernamentales,

✓ Organismos Internacionales)

TIPICIDAD:

TIPICIDAD OBJETIVA: El verbo rector que describe la conducta típica recae sobre el sujeto activo que:

- ✓ **vulnera las medidas de seguridad** (qué debemos comprender por medidas de seguridad de un sistema informático) diseñado para impedir que personas sin autorización puedan accesar al mismo.

✓ **Logra accesar** (a información) sin autorización (del titular del sistema informático) a todo o en parte de un sistema informático.

TIPICIDAD SUBJETIVA Este tipo de delito requiere de un **comportamiento doloso** por cuanto debe:

➢ **Tener conocimiento actual de lo que hace** (vulnerar las medidas de seguridad del sistema informático diseñadas para impedir el acceso sin autorización del titular) y;

➢ **Querer realizar lo que se ha propuesto**.

DAÑOS A DATOS Y SISTEMAS INFORMATICOS
Art. 399

Quien por cualquier medio y sin autorización introduce, borra, deteriora, altera, suprime o hace inaccesible de forma grave, datos informáticos.

Quien sin estar autorizado, inutiliza total o parcialmente el funcionamiento de un sistema informático, impidiendo el acceso al mismo o imposibilitando el desarrollo de alguno de sus servicios.

CONCEPTOS GENERALES:

En qué consiste una base de datos?

➢ Una base de datos: es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite. Es un sistema de archivos electrónicos.

BIEN JURÍDICO PROTEGIDO: La Información o sistema de datos informáticos.

TIPICIDAD OBJETIVA

a) Verbos rectores que describen la conducta típica: Primer párrafo El sujeto activo que por cualquier medio y sin autorización:

b) ✓ introduce

c) ✓ borra

d) ✓ deteriora

e) ✓ altera suprime o hace inaccesible de forma grave.

Verbos rectores que describen la conducta típica en el segundo párrafo

✓ Inutiliza total o parcialmente el funcionamiento de un sistema informático

✓ Impide el acceso al mismo o;

✓ imposibilitando el desarrollo de alguno de sus servicios.

❖ Ambos casos describen la modalidad de daños en los datos y sistemas

TIPICIDAD SUBJETIVA: Este tipo de delito requiere de un **comportamiento doloso** por cuanto debe **tener conocimiento actual de lo que hace y querer realizar** cualesquiera de los verbos rectores antes descritos, con el propósito o intención manifiesta y deliberada de dañar los datos y sistemas informáticos a un tercero.

ART. 400 ABUSO DE DISPOSITIVO

La fabricación , importación , venta , facilitación o la obtención , para su utilización de dispositivos , programas informáticos, contraseñas o códigos de acceso, destinados o adaptados para la comisión de los delitos de daños informáticos o de acceso ilícito a sistemas informáticos.

¿ En qué consiste el abuso de sistemas informáticos ? conlleva al uso de computadoras para hacer algo inapropiado e ilegal; es la ejecución de un ordenador o computadora. También se les denomina ciberataques y forman parte de la criminalidad informática como conjunto de actividades que se llevan acabo utilizando un elemento informático.


12:45
SAMSUNG
10:27

SUJETOS QUE INTERVIENEN

Sujeto Activo: Pueden ser: Cualquier persona, no exige cualidades o características especificas (conocimientos en el área informática): ✓ estudiantes, ✓ terroristas, ✓ figuras del crimen organizado.

Pueden esconderse en incontables enlaces, desvanecerse sin dejar rastros, despachar directamente comunicaciones, esconder pruebas en paraísos informáticos.

Sujetos pasivos: Pueden ser: Cualquier persona natural o jurídica: ✓ Empresas públicas o privadas ✓ Organizaciones gubernamentales o no gubernamentales; ✓ Organismos Internacionales; etc.

TIPICIDAD OBJETIVA Requiere de un comportamiento de carácter doloso. Los verbos rectores que describen la conducta típica en este delito se circunscriben así: La conducta típica del sujeto activo consistirá en: ✓ fabricación ✓ importación ✓ venta ✓ facilitación o la obtención

¿Con que propósito? Para utilizar dispositivos; programas informáticos; contraseñas o códigos de acceso. Que sean destinados o adaptados para la comisión de los delitos de daños informáticos o de acceso ilícito a sistemas informático.

TIPICIDAD SUBJETIVA Este tipo de delito requiere de un comportamiento de carácter doloso; por cuanto el sujeto activo deberá tener conocimiento actual de lo que hace y querer realizar cualesquiera de los verbos rectores que determinan el propósito y comportamientos antes descritos.

SUPLANTACION DE IDENTIDAD ART. 401

Quien con ánimo defraudatorio y a través de las tecnologías de la información y la comunicación suplanta la identidad de una persona natural o jurídica.

¿ En qué consiste la suplantación de identidad ? Suplantar la identidad electrónica puede definirse como el tratamiento de datos personales sin consentimiento de su titular. En otras palabras se trata de una actividad maliciosa en la que un atacante se hace pasar por otra persona.

Sujeto Activo: Pueden ser: Cualquier persona: ✓ estudiantes, ✓ terroristas, ✓ figuras del crimen organizado, Pueden esconderse en incontables enlaces, desvanecerse sin dejar rastros, despachar directamente comunicaciones, esconder pruebas en paraísos informáticos.

Sujetos pasivos: Pueden ser: Cualquier persona natural o jurídica ✓ Empresas públicas o privadas ✓ Organizaciones gubernamentales o no gubernamentales. ✓ Organismos Internacionales.

TIPICIDAD OBJETIVA El sujeto activo debe actuar con: ➢ ánimo defraudatorio (elemento normativo del tipo objetivo) y; ➢ A través de las tecnologías de la información y la comunicación (qué comprendemos por las nuevas tecnologías de Información y comunicación) El verbo rector que determina la conducta típica, en este caso es suplantar la identidad de una persona natural o jurídica (Empresa Individual o Social, una ONG, etc.)

TIPICIDAD SUBJETIVA Este tipo de delito siendo de carácter doloso, requiere: ➢ Que el sujeto activo realice la acción típica de suplantar la identidad de la persona natural y jurídica con pleno conocimiento de lo que hace (saber actual); ➢ Que actúe con animo defraudatorio es decir con plena intención de generar un engaño hacia quien dirige la acción típica.

Se exigirá en este caso que el sujeto activo cause un perjuicio (grave o leve) con el abuso de los dispositivos al sujeto pasivo de la conducta típica. ➢ Lo que no es cuestionable es que debe querer realizar la acción que se propone en este caso de abusar de los dispositivos informáticos en perjuicio de un tercero

REGLAS ESPECIALES DE JURISDICCION ART.404

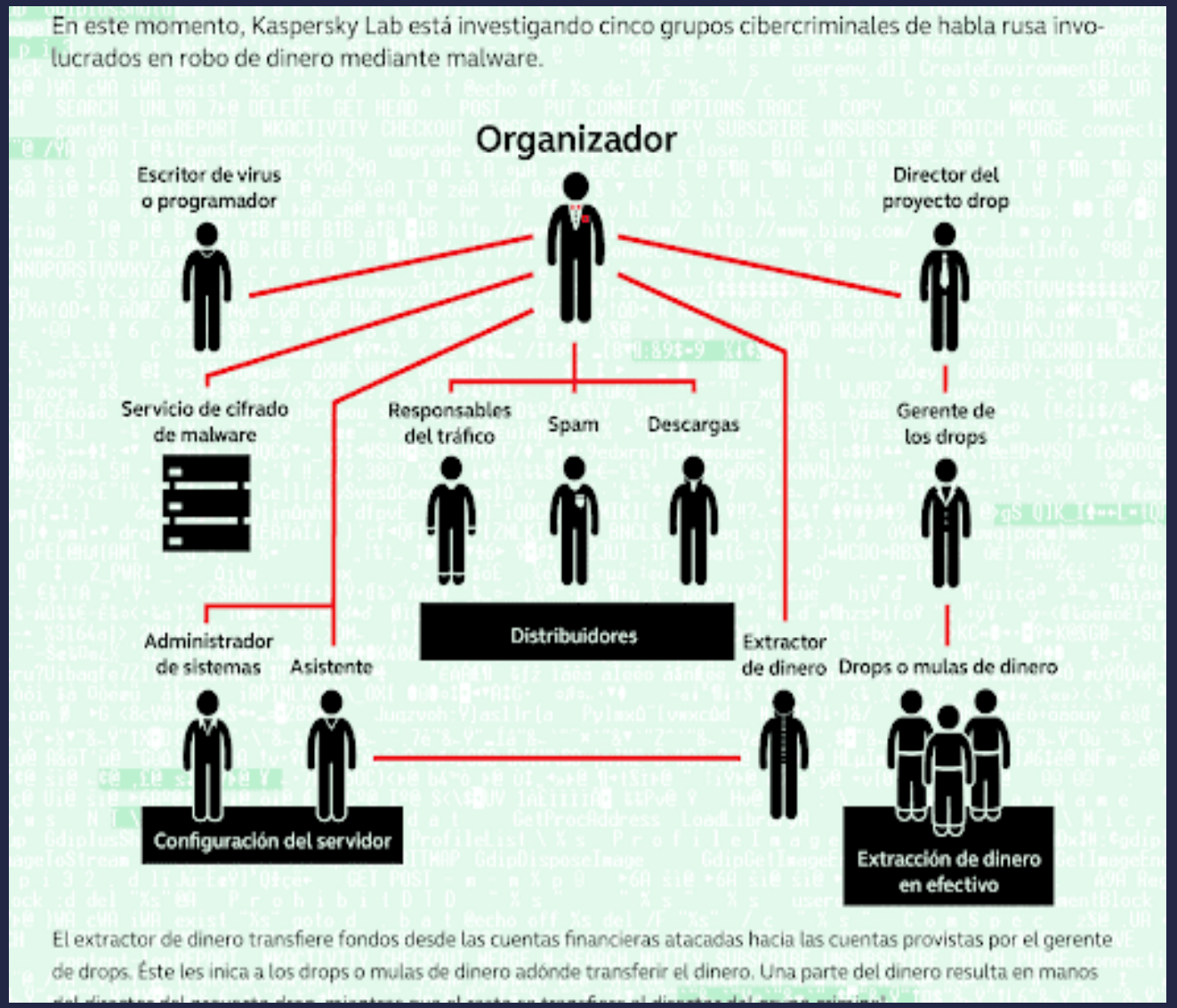
Los Órganos Jurisdiccionales nacionales deben conocer de los delitos informáticos, cuando se ejecuten en los casos siguientes:

1) En Honduras, aunque se dirijan contra datos o sistemas informáticos situados fuera de éste; o

2)Contra datos o sistemas informáticos situados en Honduras, aunque el culpable hubiese actuado desde fuera del territorio nacional.

➢ Importante: Los hackers pueden cometer estos delitos desde cualquier parte del mundo.

COMO ESTÁ ORGANIZADO UN GRUPO CIBERCRIMINIAL



COMO FUNCIONAN LAS ESTRUCTURAS CRIMINALES