

DELITOS INFORMÁTICOS

EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL

DR. SANTIAGO ACURIO DEL PINO



AGENDA

01 ¿QUÉ SON LOS DELITOS INFORMÁTICOS?

Conceptos, tipicidad

02 LEGISLACIÓN

Delitos tipificados en el COIP

03 CONCLUSIONES

Qué hacemos cuando nos sucede un incidente

01

¿Qué son los delitos informáticos?

TEORÍA DEL DELITO

- El delito es la conducta típica, antijurídica, culpable y punible



DELITO

Punibilidad

Culpabilidad

Antijuridicidad

Tipicidad

Conducta (Acto u Omisión)

5

Pasos

DIGITALIZACIÓN DE LA SOCIEDAD

La llamada «**digitalización de la sociedad**» exige garantizar que las herramientas tecnológicas utilizadas tienen la capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas prestan o hacen accesibles: lo que se ha denominado **resiliencia**.

ASPECTOS IMPORTANTES

- 
- 
- Son cometidos cada vez más por el crimen organizado y grupos terroristas
 - Están creciendo rápidamente alrededor del mundo.
 - Son una barrera para el Comercio Telemático
 - Producen una excesiva lesividad
 - Son de carácter transfronterizo
 - Son delitos de carácter ocupacional
 - Se aprovechan de la automatización de los programas o sistemas

LA REALIDAD ES QUE.....

Permite la organización mundial de una actividad delictiva rentable

- Robo de identidad
- Venta de herramientas para “hacking”
- Creación de “malware” personalizado
- Renta de “botnets”
- Operaciones de “spamming”
- Lavado de dinero
- Violaciones a la propiedad intelectual



DEPENDENCIA

Las sociedades de todo el mundo dependen considerablemente de las TIC, por lo que son muy vulnerables



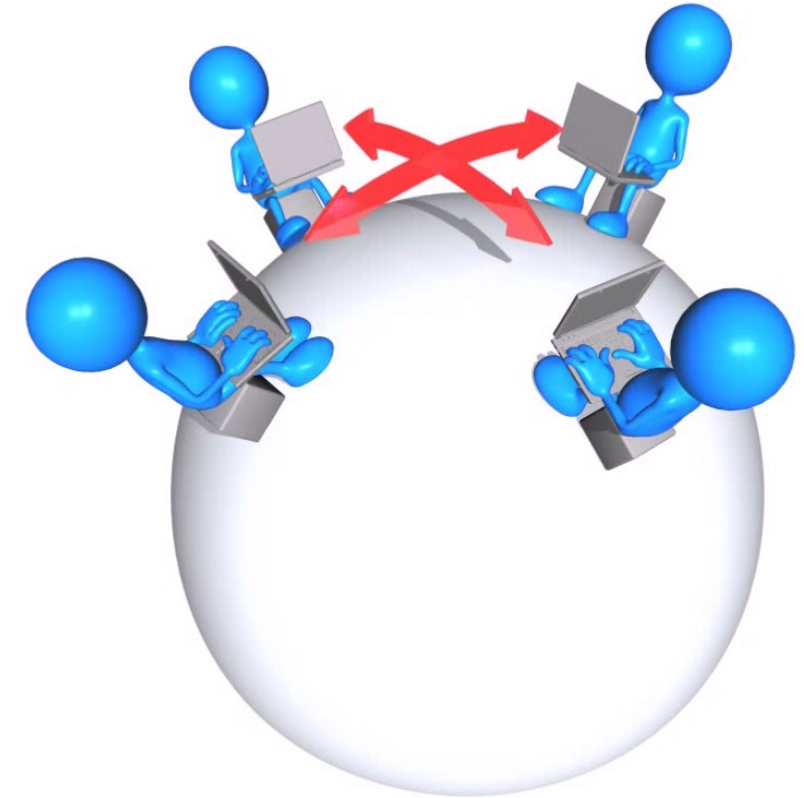
FACTOR CRIMINÓGENO



- La informática y sus aplicaciones se han convertido en factores criminógenos, ya que proporcionan grandes posibilidades de cometer hechos ya punibles o merecedores de una pena.
- Se convierte entonces el procesamiento informático de datos en un relevante factor criminógeno.
- La mayor facilidad del acceso y conocimiento de la información procesada por parte de los autores de estos hechos punibles, facilita la comisión de estos hechos.

FACTOR CRIMINÓGENO

- Se trata de hechos en donde lo característico es la permanencia y el automatismo, dado esto por las especiales particularidades de los sistemas informáticos y telemáticos, ya que cuando se procesan datos es posible repetir dicho procesamiento cuantas veces sea necesario.
- Se tratan de hechos que pueden producir una lesividad excesiva, producen efectos con gran expansión no tiene los límites físicos de los delitos clásicos.



EL PORQUÉ LA PROLIFERACIÓN DE ESTE FENÓMENO DELICTIVO

Factor 1

Desconocimiento de los nuevos sistemas de tratamiento de información.



Factor 2

La inexistencia y precariedad de los sistemas de seguridad



Factor 3

Falta de leyes y normativas especiales



LIBERTAD INFORMÁTICA

Libertad Informática consiste, como expresión de la libertad del individuo, en el derecho de utilizar lícita y libremente, con los límites constitucionales y legales la tecnología informática creando para el efecto un entorno virtual individual.

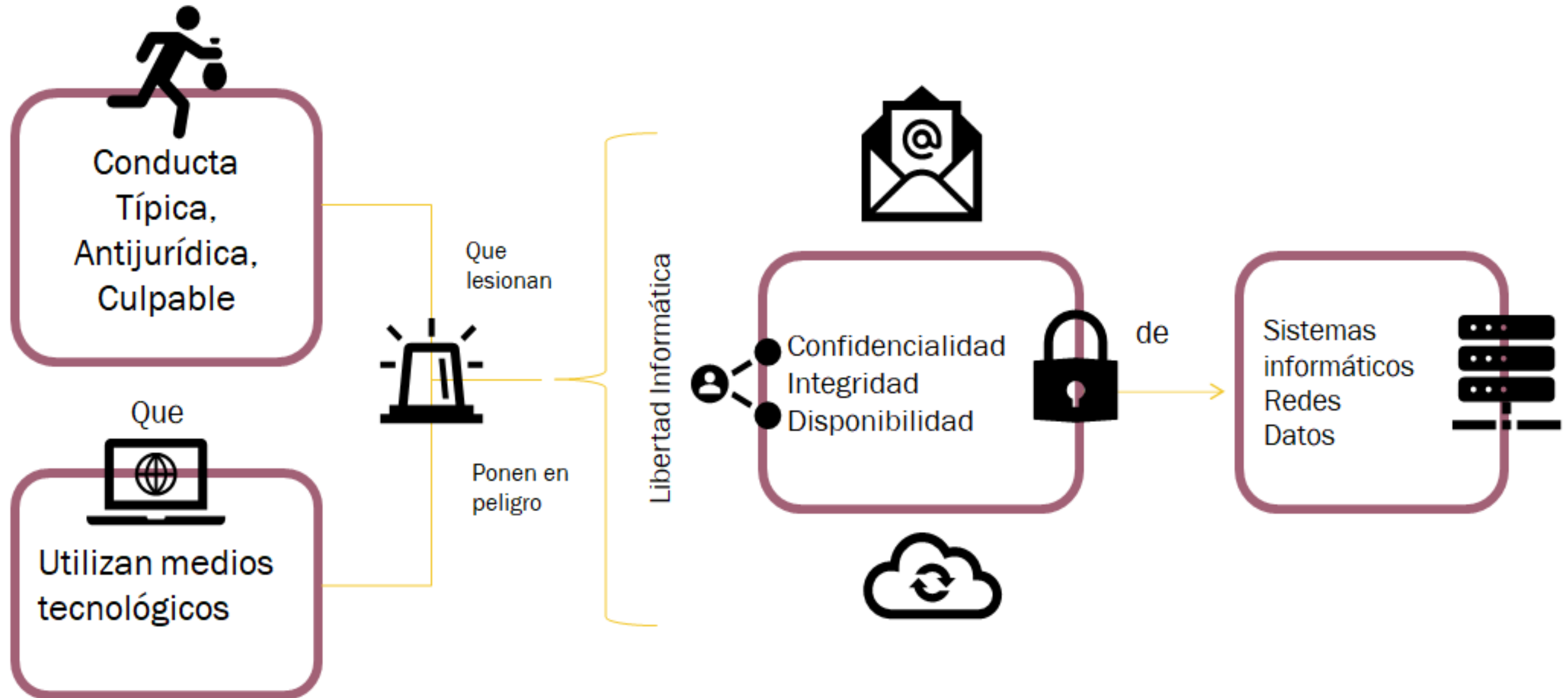


DELITOS INFORMÁTICOS

- Los “**DELITOS INFORMÁTICOS**” son: *toda conducta típica, antijurídica y culpable que utiliza medios tecnológicos que lesionan o ponen en peligro la libertad informática, esto es afectando la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos.*



CONCEPTO DE DELITO INFORMÁTICO



LIBERTAD INFORMÁTICA

De forma que los delitos informáticos pueden verse como violación de esa libertad informática, como infracción de las distintas libertades a las que puede extenderse el empleo de estas tecnologías.



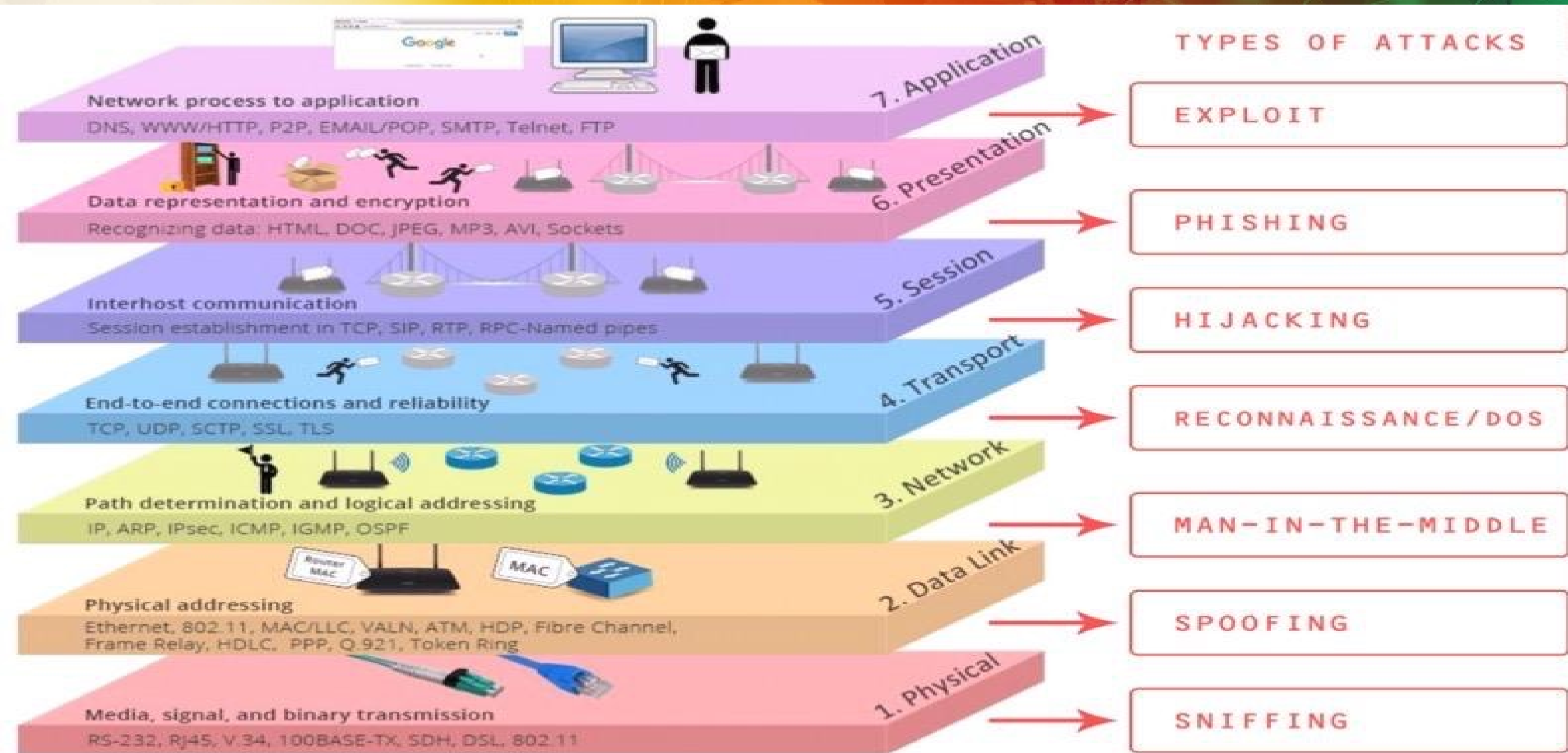
ES ATRACTIVO EL DELITO INFORMÁTICO

Para analizar este apartado tomemos en cuenta lo siguiente:

- **Objeto pequeño:** la información que se ataca está almacenada en contenedores pequeños: no es necesario un camión para robar un banco, llevarse las joyas, el dinero, etc.
- **Contacto físico: no** existe contacto físico en la mayoría de los casos. Se asegura el anonimato y la integridad física del propio delincuente.
- **Alto valor:** el objeto codiciado tiene un alto valor. Los datos (el contenido a apropiarse) puede valer mucho más que el soporte que los almacena: servidor, computador, disco, CD, etc.

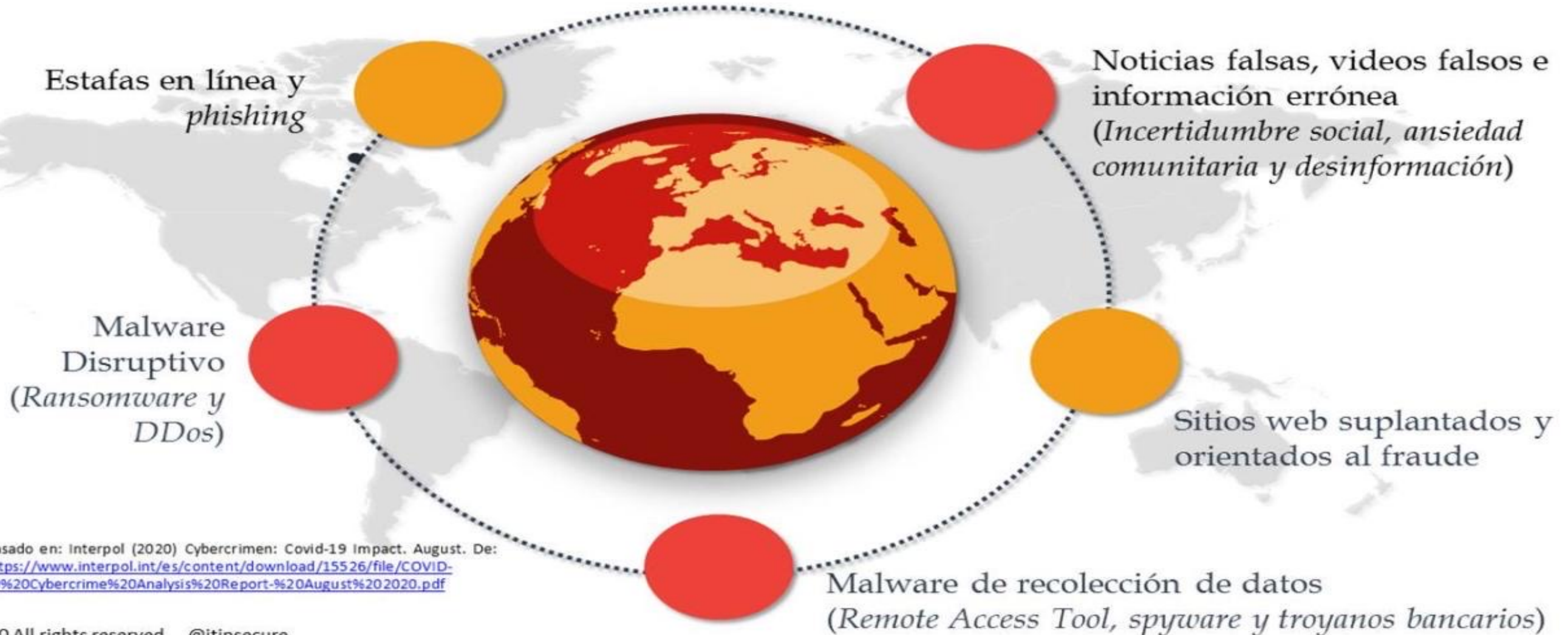
Aunque no será la única, una de las herramientas de protección de datos más efectiva es el uso de técnicas criptográficas.

DONDE ESTÁN LOS ATAQUES



CIBERCRIMEN EN LA PANDEMIA

Cibercrimen en medio de la pandemia *Análisis del INTERPOL Cybercrime Threat Response*



02

Tipos existentes en el COIP

ATAQUES CONTRA LOS SISTEMAS DE INFORMACIÓN

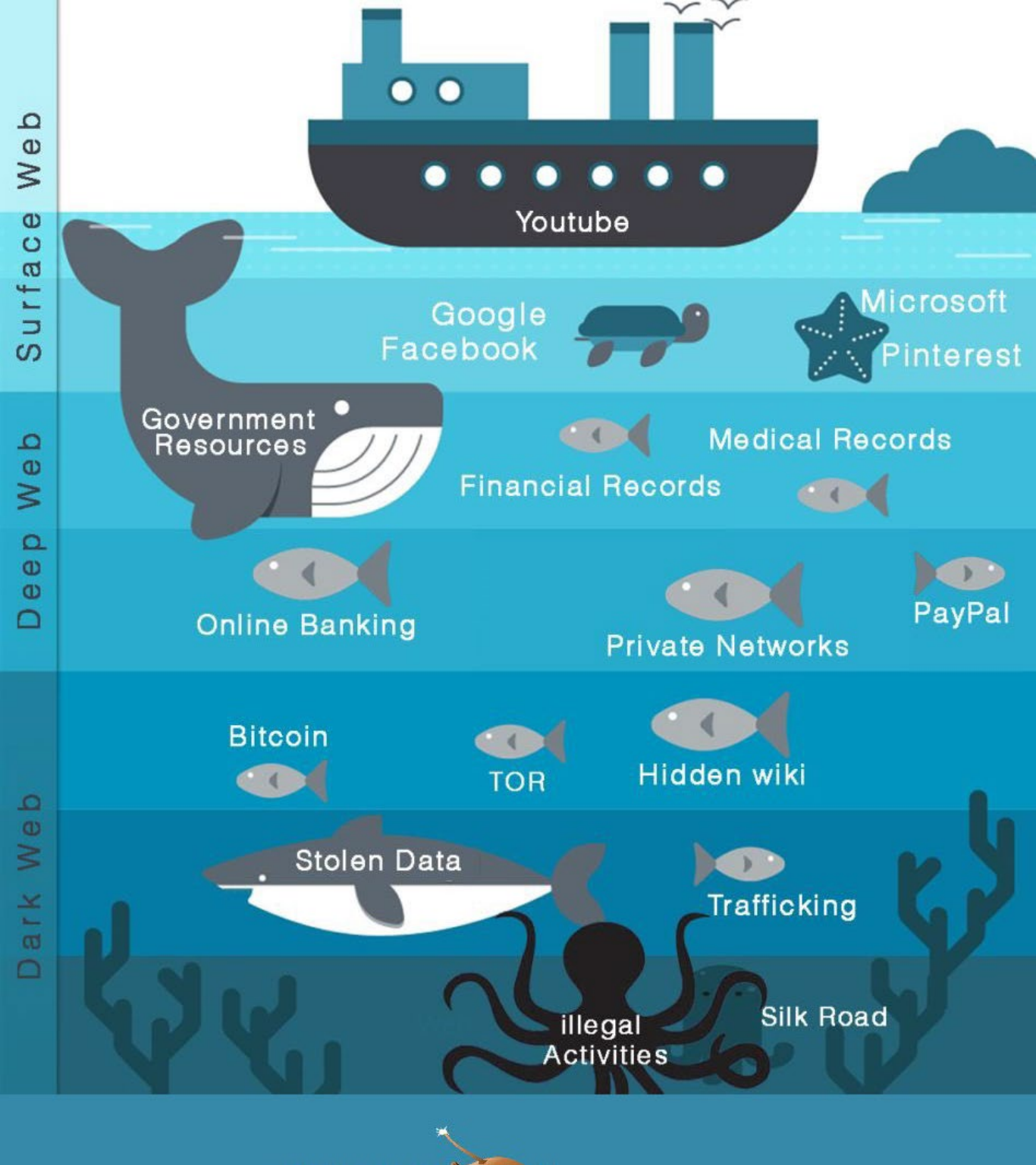
- **Interceptación ilegal**
 - Interceptación de información hacia, desde o dentro de un sistema
- **Acceso ilegal**
 - Puede comprometer la información o la confidencialidad
- **Interferencia de información**
 - Dañar, borrar, deteriorar, alterar, suprimir
- **Interferencia del sistema**
 - Obstaculizar seriamente el funcionamiento de un sistema
- **Mal uso de dispositivos**
 - Dispositivos de acceso, *passwords*



DELITOS INFORMÁTICOS Y DELITOS RELACIONADOS CON LAS COMPUTADORAS



- **Falsificación informática**
 - Con intención de que sus efectos se consideren auténticos
- **Fraude informático**
 - Interferir sistemas o información con intención de defraudar
- **Pornografía infantil**
 - Producción, oferta, distribución, adquisición, posesión
- **Violación a la propiedad intelectual**
 - Violaciones premeditadas cometidas a escala comercial



QUE PODEMOS ENCONTRAR..

AHORA LOS ATACANTES TIENEN
MUCHOS RECURSOS E INFORMACIÓN.

LA PREGUNTA ES POR DONDE
EMPEZAR

DELITOS EN EL COIP

- Pornografía Infantil: **Art. 103**
 - Pena de trece a dieciséis años.
- Posesión de Pornografía Infantil: **Art. 104**
 - Pena de diez a trece años
- Grooming: **Art. 173**
 - Pena uno a tres años o de tres a cinco años
- Oferta de servicios sexuales a través de medios electrónicos. **Art. 174**
 - Pena de siete a diez años



INSTIGACIÓN AL SUICIDIO

154.1

- **Sujeto Activo**, cualquier persona natural
 - **Conducta:** Induzca o dirija mediante amenazas, consejos, órdenes concretas, retos.
 - **Medio:** Por cualquier tipo de comunicación (verbal, física digital, electrónica existente)
 - **Resultado:** Que la víctima se provoque daño a si misma o ponga fin a su vida, siempre que se demuestre que dicha influencia fue determinante para el resultado dañoso
 - **Pena:** Uno a Tres años



CIBERACOSO



Comete ciberacoso, toda persona quien hostigue o amenace por medio de las Tecnologías de la Información y Telecomunicaciones (TICS), redes sociales, correo electrónico o cualquier otro espacio digital y cause un daño a la dignidad personal, o afecte la paz, la tranquilidad o la seguridad de las personas.

CONTRAVENTIONES: ACOSO ACADÉMICO Y ESCOLAR

ACOSO ACADÉMICO: Se entiende por acoso académico a toda conducta negativa, intencional, metódica y sistemática de agresión, intimidación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza, incitación a la violencia, hostigamiento o cualquier forma de maltrato psicológico, verbal, físico que, de forma directa o indirecta, dentro o fuera del establecimiento educativo,

SUJETO ACTIVO Y MEDIOS: Se dé por parte de un docente, autoridad o con quienes la víctima o víctimas mantiene una relación de poder asimétrica que, en forma individual o colectiva, atenten en contra de una o varias personas, por cualquier medio incluyendo a través de las tecnologías de la información y comunicación.

SANCIONES: Esta contravención será sancionada con una o más de las medidas no privativas de libertad previstas en los números 1, 2, 3 y 6 del artículo 60 de este Código, y además el juzgador impondrá las medidas de reparación integral que correspondan según el caso.

ACOSO ESCOLAR ENTRE PARES: Cuando el ACOSO ACADÉMICO se de entre estudiantes niñas, niños y adolescentes, se aplicarán las medidas socioeducativas no privativas de libertad correspondientes y el tratamiento especializado reconocido en la ley de la materia, garantizando los derechos y protección especial de niñas, niños y adolescentes.

DELITOS EN EL COIP

- **Hostigamiento. — Art. 154.2**

- Sujeto Activo, puede ser una persona natural o jurídica
 - **Conducta:** Hostigue a través de cualquier medio tecnológico o digital, moleste, perturbe o angustie de forma insistente o reiterada a otra persona
 - **Pena:** 6 mes a un año y uno a tres años, si son menores de edad



- **Ciberacoso Sexual. — Art. 166**

- Sujeto Activo, cualquier persona
 - **Conducta:** Solicitar actos de naturaleza sexual prevalido de su situación de autoridad o jerarquía, para los utiliza cualquiera de las tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales.
 - **Pena:** Uno a cinco años

DELITOS EN EL COIP

- El término **happy slapping** (bofetada feliz, en español) nació en Reino Unido en 2005
- El **happy slapping** consiste en la grabación de una agresión física, verbal o sexual y su **difusión online mediante las tecnologías digitales** (páginas, blogs, chats, redes sociales, etc.).
- Lo más común es que esta violencia se difunda por alguna red social y, en ocasiones, puede hacerse viral.



• **Happy slapping Art. 160 (Acoso Sexual) y 171 (Violación)**

- Sujeto Activo, cualquier persona
 - **Conducta:** Se grabe o transmita un abuso sexual o violación con cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación, O se agrede físicamente a la víctima, y dicha agresión también sea grabada o transmitida.
 - **Pena: 3 a 5 años; 7 a 10 años: Abuso sexual**
 - **Pena: 19 a 23 años: Violación**

DELITOS EN EL COIP



Violación del Derecho a la Intimidad.

Art. 178

- Mensajes de datos
- Vídeos
- Datos Personales

No son aplicables estas normas para la persona que divulgue grabaciones de audio y video en las que interviene personalmente, ni cuando se trata de información pública de acuerdo a lo previsto en la ley.

Pena de uno a tres años

DELITOS EN EL COIP



- **Revelación de secreto o información personal de terceros. Art. 179 inciso 2**
- Sujeto Activo, cualquier persona
 - **Conducta:** Revele o divulgue a terceros: contenido digital, mensajes, correos, imágenes, audios o vídeos o cualquier otro contenido íntimo de carácter sexual de una persona en contra de su voluntad.
 - **Pena: uno a tres años**

DEFRAUDACIONES: ART. 186

Sujeto Activo: Cualquier persona

Conducta:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, **clonada**, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, **clonen** o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.



Pena de cinco a siete años.

DELITOS DEL COIP

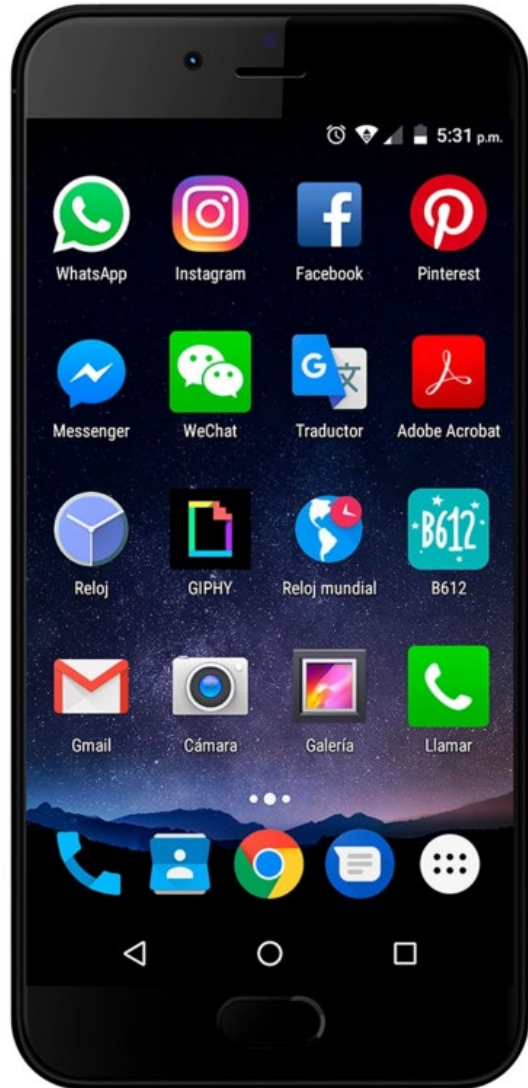
Sujeto Activo: Cualquier persona

Conducta:

- Prestación Ilegal de Servicios de Telecomunicaciones **Art. 188.**
 - **Pena de seis meses a dos años.**
- Ofrezca, preste o comercialice servicios públicos de luz eléctrica, telecomunicaciones o agua potable.
 - **Pena uno a tres años.**
- Apropiación fraudulenta de por medios electrónicos: **Art. 190**
 - **Pena uno a tres años.**
- Reprogramación o modificación de información de equipos terminales móviles: **Art. 191**
 - **Pena uno a tres años.**



DELITOS EN EL COIP



- Intercambio, comercialización o compra de información de equipos terminales móviles. **Art. 192**
- Reemplazo de identificación de terminales móviles. **Art. 193**
- Comercialización ilícita de terminales móviles. **Art. 194**
- Infraestructura ilícita. **Art. 195**

Pena de 1 a 3 años

DELITOS EN EL COIP

- **Actos Lesivos a los derechos de Autor Art. 208.B**
- Sujeto Activo, cualquier persona natural o jurídica
 - **Conducta:** Vulnere a sabiendas los derechos de autor o derechos conexos .
 - Fabrique, importe, exporte, venda, arriende o de cualquier forma distribuya al público un dispositivo, sistema o software que permita descifrar una señal de satélite cifrada portadora de programas o en general de telecomunicaciones, sin autorización del distribuidor legítimo de esa señal; o, de cualquier forma, eluda, evada, inutilice o suprima un dispositivo, sistema software que permita a los titulares del derecho controlar la utilización de sus obras o prestaciones, el cual posibilite impedir o restringir cualquier uso no autorizado de estos.
 - **Pena:** Seis meses a un año, comiso y multa de ocho hasta trescientos salarios básicos unificados del trabajador en general



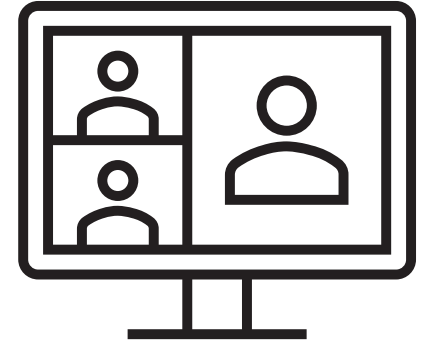
DELITOS EN EL COIP



- Suspensión, alteración o suposición de la identidad y estado civil por medios electrónicos. **Art. 211**
 - Pena uno a tres años
- Revelación ilegal de información de bases de datos. **Art. 229**
 - Pena uno a tres años
 - **Sujeto Activo Calificado:** Funcionario Público o encargado de las Bases de Datos, empleado bancario.
 - De tres a cinco años

DELITOS EN EL COIP

- Interceptación de comunicaciones: **Art. 230.1**
- Pharming y Phishing **Art. 230.2**
- Diseminación, posesión o introducción de programas informáticos, mensajes de datos y todo contenido digital para realizar Pharming y Phishing. **Art. 230.3**
- Duplicación de información de tarjetas de debito y crédito. **Art. 230.4**
- Producción, fabricación, distribución, posesión o facilitación de materiales, dispositivos electrónicos o sistemas informáticos para duplicación de tarjetas de debito y crédito. **Art. 230.5**



Penal de 3 a 5 años

DELITOS EN EL COIP



- **Fraude Informático. Art. 231.**
 - Mulas del fraude informático. Art. 231.2
 - **Pena de tres a cinco años.**
- **Ataque a la integridad de sistemas informáticos. Art. 232**
 - Diseño, venta, distribución de malware
 - Destrucción de infraestructura física
 - **Pena de tres a cinco años.**
 - Destrucción de bienes informáticos para la prestación del servicios informáticos
 - *Prestación de un servicio público o vinculado con la seguridad ciudadana*
 - **Pena de cinco a siete años.**

DELITOS EN EL COIP

- **Acceso no autorizado a sistemas de información. Art. 234**
 - La persona que sin autorización acceda en todo o en parte a un sistema informático, sistema telemático o de telecomunicaciones
 - O se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema
 - Explota ilegítimamente el acceso logrado.
 - Modificar un portal web.
 - Desvía o redirecciona el tráfico de datos o voz
 - Ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos
 - **Penal de tres a cinco años.**



DELITOS EN EL COIP

- **Falsificación Informática Art. 234.1**
- Sujeto Activo, cualquier persona
 - **Conducta:** Provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos.
 - Con la misma pena será sancionado la persona que utilice el mensaje de datos o contenido digital falsificado
 - **Pena: Tres a cinco años**



NORMAS COMUNES



Art. 234.2.- Agravación de las penas. - La práctica de los hechos que se describen en los artículos 232, 234 y 234.1 será sancionada con pena agravada en un tercio de su pena máxima si logra perturbar de forma grave o duradera a un sistema informático que apoye una actividad destinada a asegurar funciones sociales críticas, como cadenas de abastecimiento, salud, seguridad y bienestar económico de las personas, o funcionamiento regular de los servicios públicos.

Art. 234.3.- Responsabilidad de personas jurídicas. - A los delitos de esta Sección es aplicable la responsabilidad prevista en los artículos 49 y 71 de este Código.

DELITOS EN EL COIP

- **Terrorismo. Art. 366.1**
 - La persona que respecto de un transporte terrestre, una nave o aeronave, plataformas fijas marinas, se apodere de ella, ejerza control sobre la misma por **medios tecnológicos (...)**

Pena 10 a 13 años



NÚMERO DE DENUNCIAS SOBRE DELITOS INFORMÁTICOS EN ECUADOR

Tipos de delitos	2014*	2015	2016	2017	2018	2019	2020**	
Suplantación de identidad	1355	3920	4152	3676	4180	4607	2162	24 052
Falsificación y uso de documento falso	1048	2594	3117	3183	3292	3231	1448	17 913
Apropiación fraudulenta por medios electrónicos	507	1280	1045	960	1451	1746	1033	8022
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	54	141	145	218	236	246	175	1215
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	21	80	108	159	202	166	85	821
Ataque a la integridad de sistemas informáticos	49	77	76	86	87	113	51	539
Interceptación ilegal de datos	38	55	82	63	41	87	45	411
Transferencia electrónica de activo patrimonial	17	59	47	54	38	49	31	295
Revelación ilegal de base de datos	29	24	24	22	44	34	18	195
Total	3118	8230	8796	8421	9571	10 279	5048	53 463

*Desde agosto - **Hasta agosto

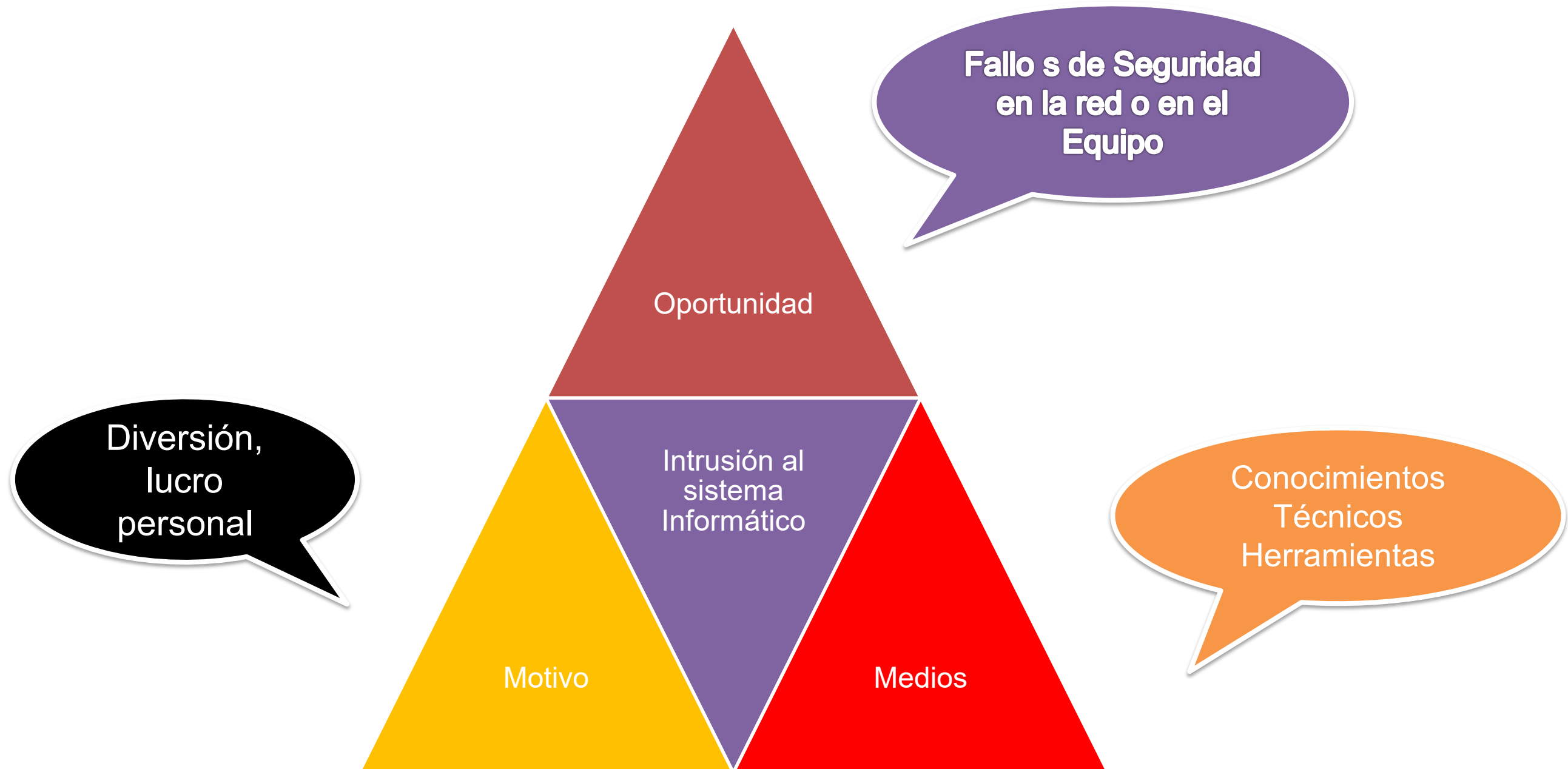
03

Conclusiones

TRIANGULO DE LA INTRUSIÓN

Para poder llevar a cabo un ataque informático los intrusos deben disponer de los **medios técnicos, los conocimientos y las herramientas** adecuadas, deben contar con una determinada **motivación o finalidad**, y además una determinada oportunidad que facilite el desarrollo del ataque.

TRIANGULO DE LA INTRUSIÓN



CONCLUSIONES

1. Los delitos informáticos todos son **Dolosos**
2. Los delitos informáticos son de tipo **ocupacional**:
 - El **90 %** de los ataques son realizados por insiders y solo el **10%** por outsiders
3. Mantenga un nivel de **paranoia** debidamente administrada
4. El **agresor** tarde o temprano tendrá éxito. Prepárese para un incidente.
5. Las **personas** y las **máquinas** van a fallar. Monitoree su comportamiento y **actué**



PARTE DE LA SOLUCIÓN

CONVENIO SOBRE LA CIBERDELINCUENCIA CONVENIO DE BUDAPEST

@JonhnyMendoza

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, mejor conocido como **Convenio de Budapest**, fue firmado en Hungría el 23 de noviembre de 2001 y entró en vigor el 01 de julio de 2004.

Su objetivo es alentar a los países miembro a aplicar una política penal común con la finalidad de proteger a la sociedad del ciberdelito mediante la adopción de legislación idónea y facilitar la cooperación internacional en la materia.



Es el primer tratado internacional vinculante sobre delitos informáticos, relacionados con violaciones a los derechos de autor, fraude informático, pornografía infantil y violaciones de la seguridad de la red.

El Convenio cuenta con un Protocolo Adicional que penaliza los actos de índole racista y xenófoba distribuidos por medio de sistemas informáticos.

Evolución del Cibercrimen

Nueva Transformación Digital

ANONIMATO, SORPRESA, CONOCIMIENTO, DESORIENTACIÓN, ENMASCARAMIENTO

Blockchain

- Uso de criptomonedas
- Transacciones en la darkweb
- Tokenización de activos

Inteligencia Artificial

- Videos falsos
- Campañas señuelo
- Ataques cognitivos

Internet de las Cosas

- Extorsiones personalizadas
- Espionaje y Botnets
- Modificación de firmware

Computación en la nube/borde

- Librerías desactualizadas
- Vulnerab. desconocidas
- Plataformas "serverless"

Analítica de datos

- Inteligencia de amenazas
- Perfilación de objetivos
- Ataques furtivos móviles

CRIMEN COMO SERVICIO

**MAYOR
CONECTIVIDAD**

**MAYOR
VISIBILIDAD**

**MAYOR
INTERACCIÓN**

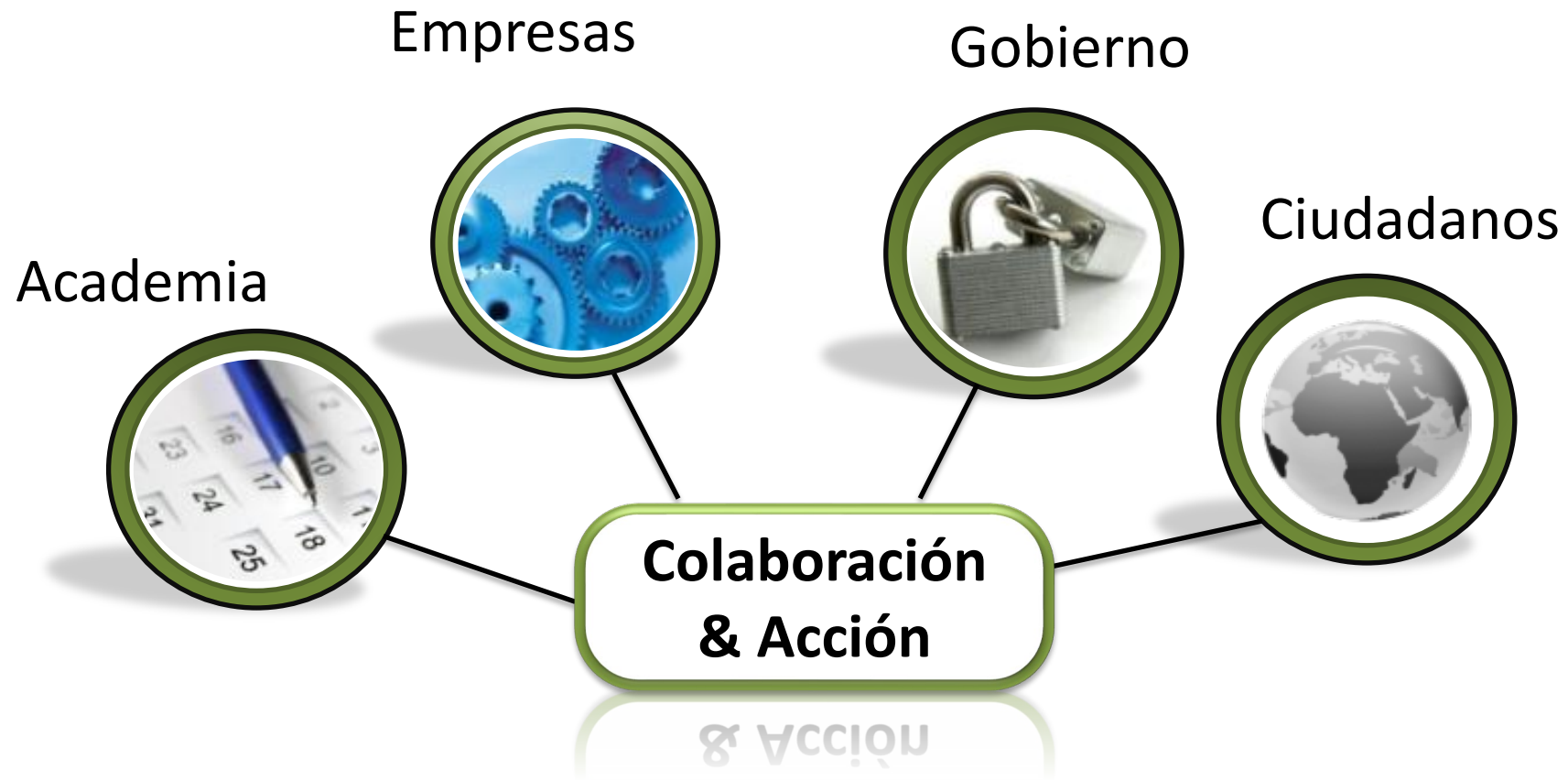
**MAYOR
APERTURA**

**MAYOR
SUPERFICIE**

**MAYOR
EXPOSICIÓN**

Basado en: Trendmicro (2020) The new norm. Trend Micro Security Predictions for 2020. Trendmicro Research. De: <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2020>

SOLUCIÓN AL PROBLEMA



Mientras el crimen es organizado, nosotros no lo estamos

PREGUNTAS



Muchas GRACIAS !

