AECI

Asociación Ecuatoriana de Ciberseguridad

Secuestro Digital, lo conoces

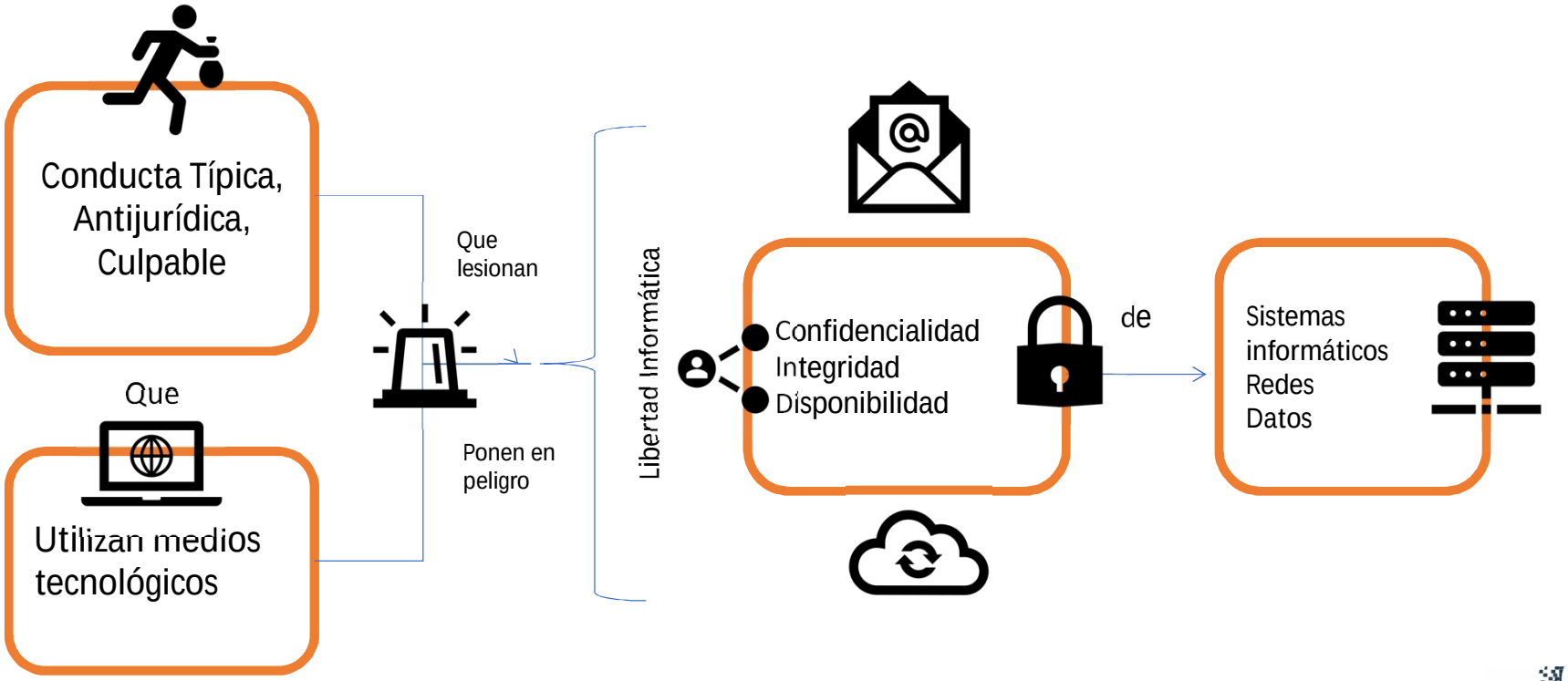
Asociación Ecuatoriana de Ciberseguridad

Ransomware y COIP

Dr. Santiago Acurio Del Pino

Asociación Ecuatoriana de Ciberseguridad

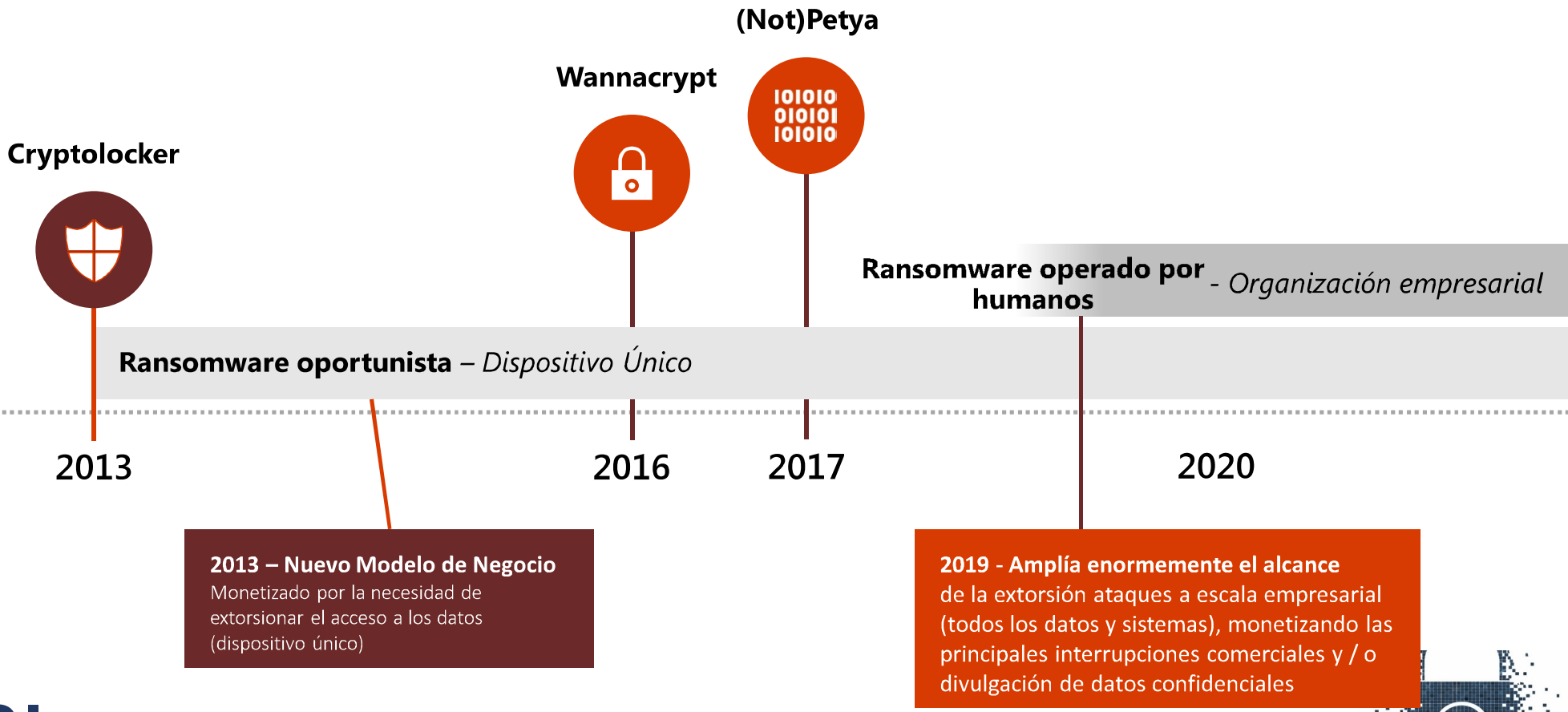
Delito Informático



AECI

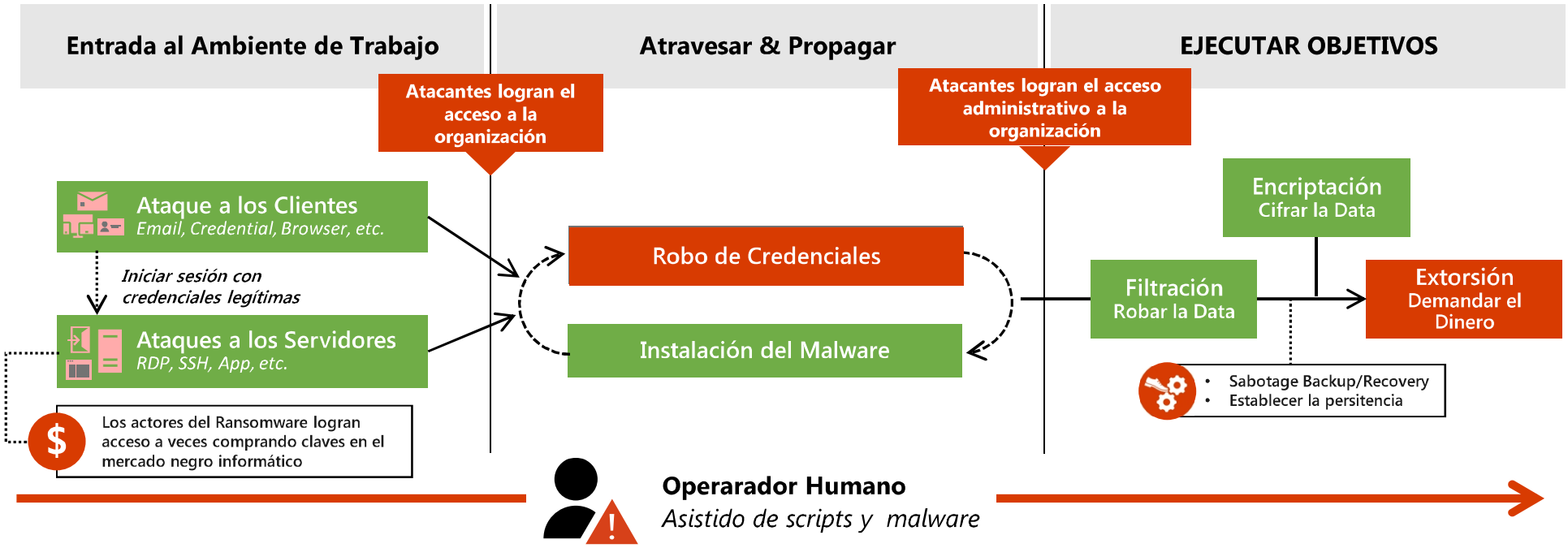
Asociación Ecuatoriana de Ciberseguridad

Evolución de los Modelos de Ransomware



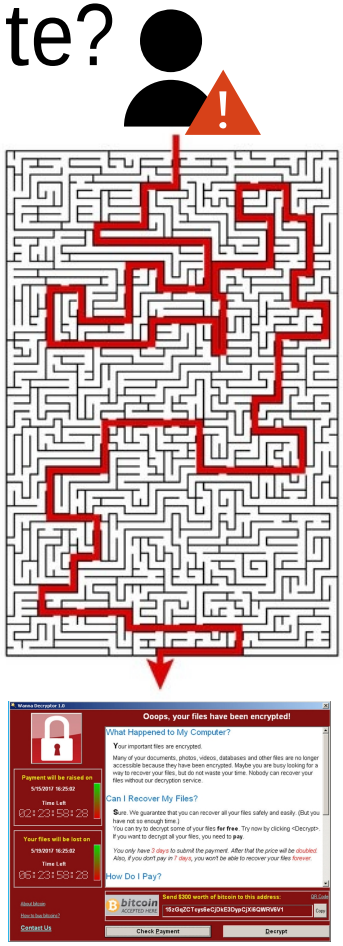
AECI

Cómo funciona – Ransomware operado por humanos



¿Qué hace que el ransomware operado por humanos sea diferente?

- Ransomware operado por Humanos, usa múltiples técnicas, tales como
  - Troyanos bancarios
  - Desactivar el Antivirus
  - Robo de credenciales
  - Golpe de cobalto
  - Reconocimiento de red
  - Puertas traseras adicionales
  - Registros claros
  - Exfiltración de datos
  - Dispositivo de rescate



Los ataques no son ataques preprogramados, los operadores ajustan según sea necesario

Apuntar deliberadamente a activos críticos

Pagar el rescate no elimina al atacante

Se enfocan en sistemas críticos y trabajadores de primera línea

Asociación Ecuatoriana de Ciberseguridad

AECI

Ransomware básico Vs Operado por Humanos

Asociación Ecuatoriana de Ciberseguridad

Ransomware Básico Oportunista

- Objetivos **individuales**
- Ataques **preprogramados** que son el mejor esfuerzo
- **Cifrado** de datos oportunista
- Es **poco probable** que cause **una interrupción catastrófica** del negocio
- La defensa exitosa es **la remediación** de malware

Ransomware operado por Humanos

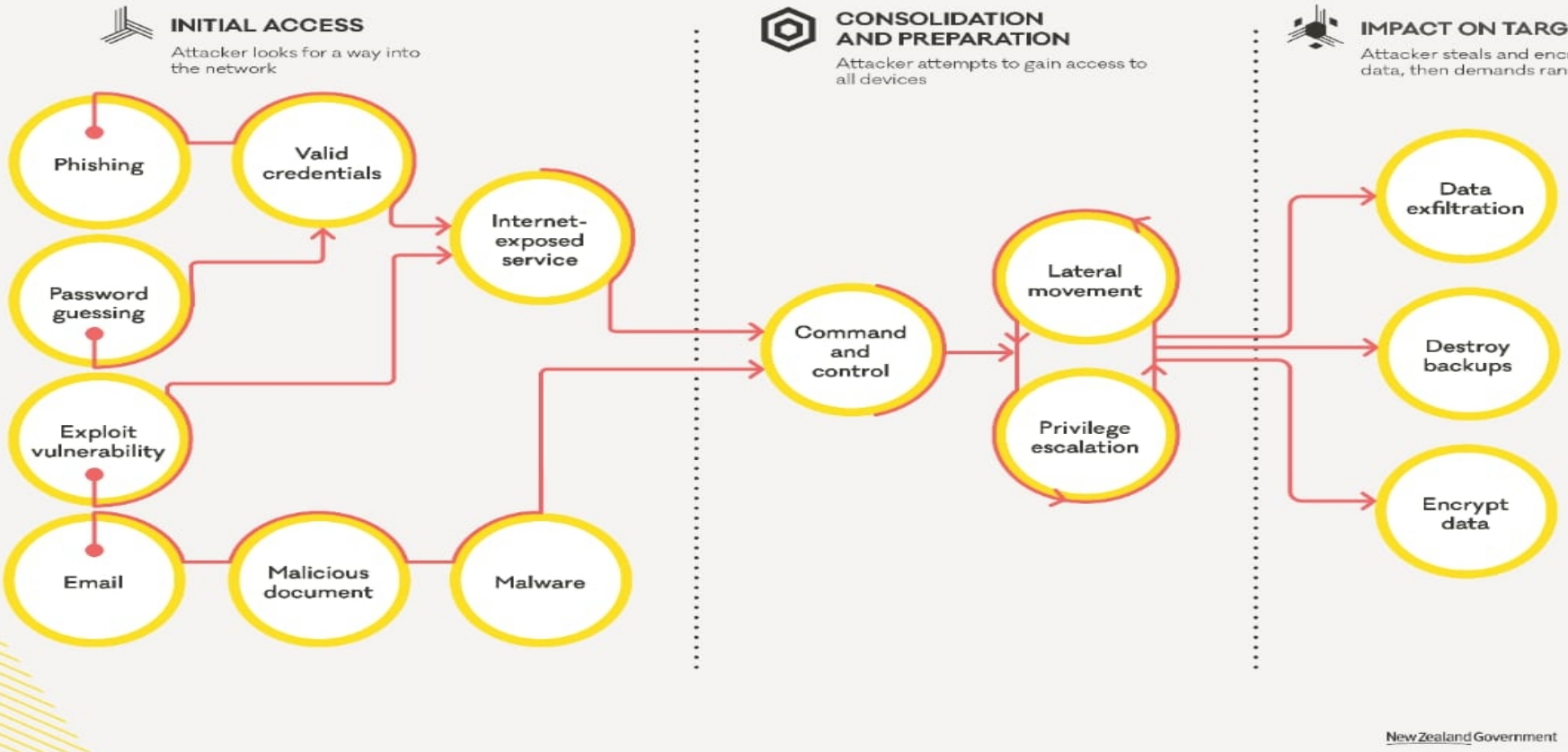
- Se dirige a **toda la empresa**
- Ataques **personalizados** impulsados por una determinada inteligencia humana
- **Cifrado** de datos calculado / **Fuga** de datos
- **Garantizado** para **causar una interrupción del negocio catastrófica y visible**
- La defensa exitosa es el **desalojo** del adversario.

AECI

LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.



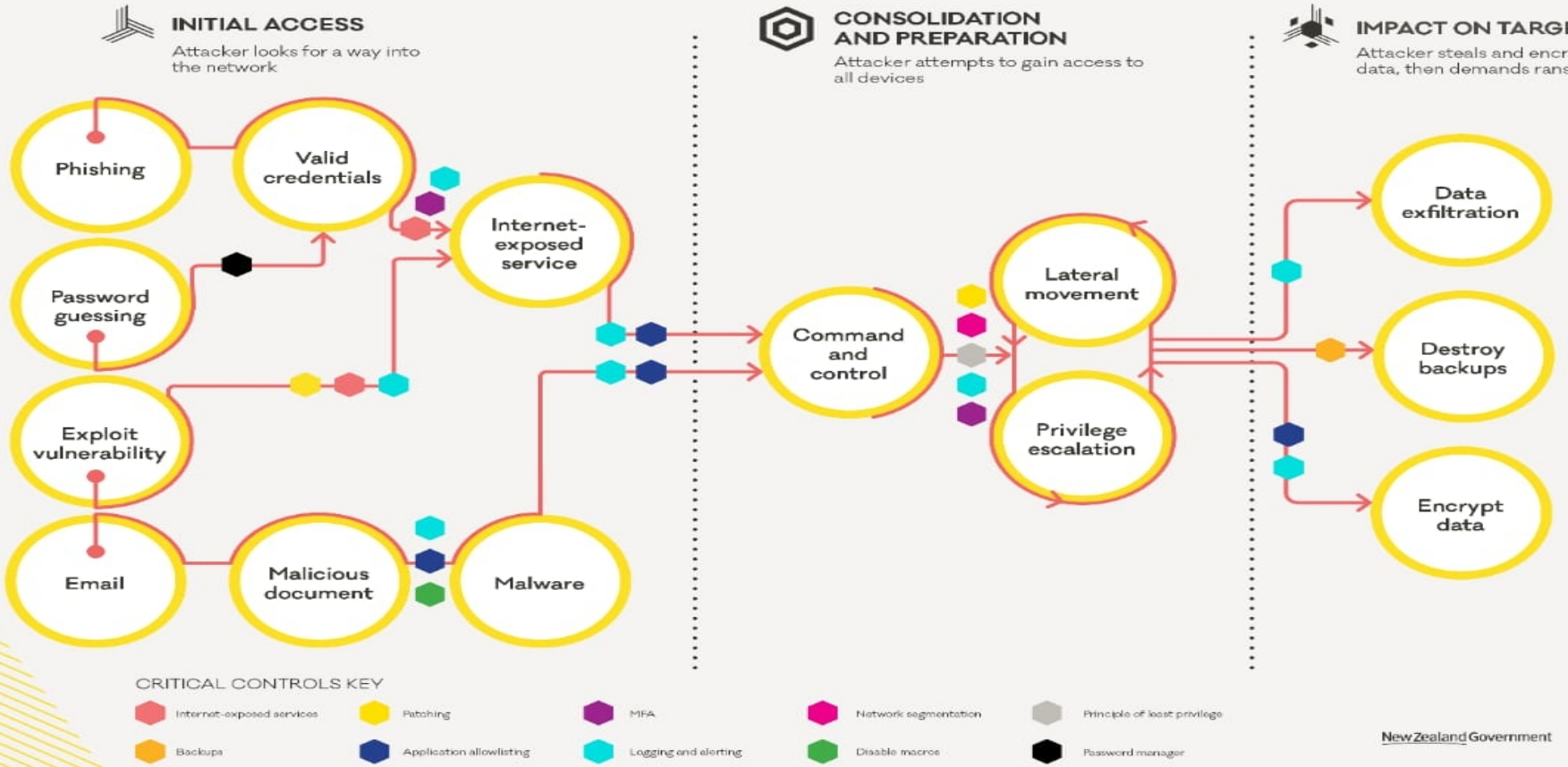
New Zealand Government

AECI

LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.



New Zealand Government

AECI

Que dice el COIP

- **Art. 20.- Concurso real de infracciones.-** Cuando a una persona le son atribuibles varios delitos autónomos e independientes se acumularán las penas hasta un máximo del doble de la pena más grave, sin que por ninguna razón exceda los cuarenta años.
- **Art. 185.- Extorsión.-** La persona que, con el propósito de obtener provecho personal o para un tercero, obligue a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o el de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.
- La sanción será **de cinco a siete años** si se verifican alguna de las siguientes circunstancias:

5. Si se comete total o parcialmente desde el extranjero.

- **Art. 232.- Ataque a la integridad de sistemas informáticos.-** La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de **tres a cinco años**.
- Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

- Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, **la pena será de cinco a siete años** de privación de libertad.

Asociación Ecuatoriana de Ciberseguridad

AECI

Que dice el COIP

Asociación Ecuatoriana de Ciberseguridad

- Phishing & Pharming (Art. 230.2 COIP)
- Acceso no Autorizado a Sistemas de Información (Art. 234 COIP)
- Ataque a la Integridad de Sistemas Informáticos (Art. 232 COIP)
- Extorsión (Art. 185 COIP)
- Revelación Ilegal de Base de Datos (Art. 229 COIP)

Delitos de Acción Pública

FGE
FISCALÍA GENERAL DEL ESTADO
ECUADOR

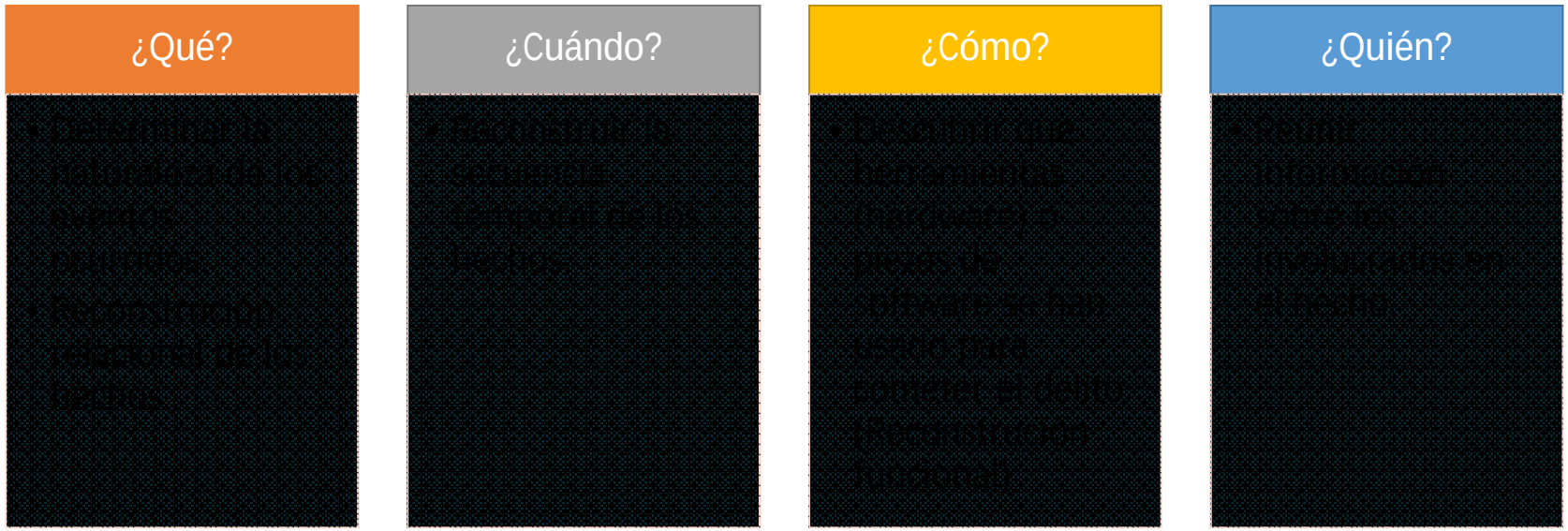
La noticia criminal llega por denuncia o de oficio

Investigación Previa

- Es reservada
- Se buscan los elementos de convicción
- Se cuenta con el apoyo de la Policía Judicial
- Criminalística
- Peritos especializados

AECI

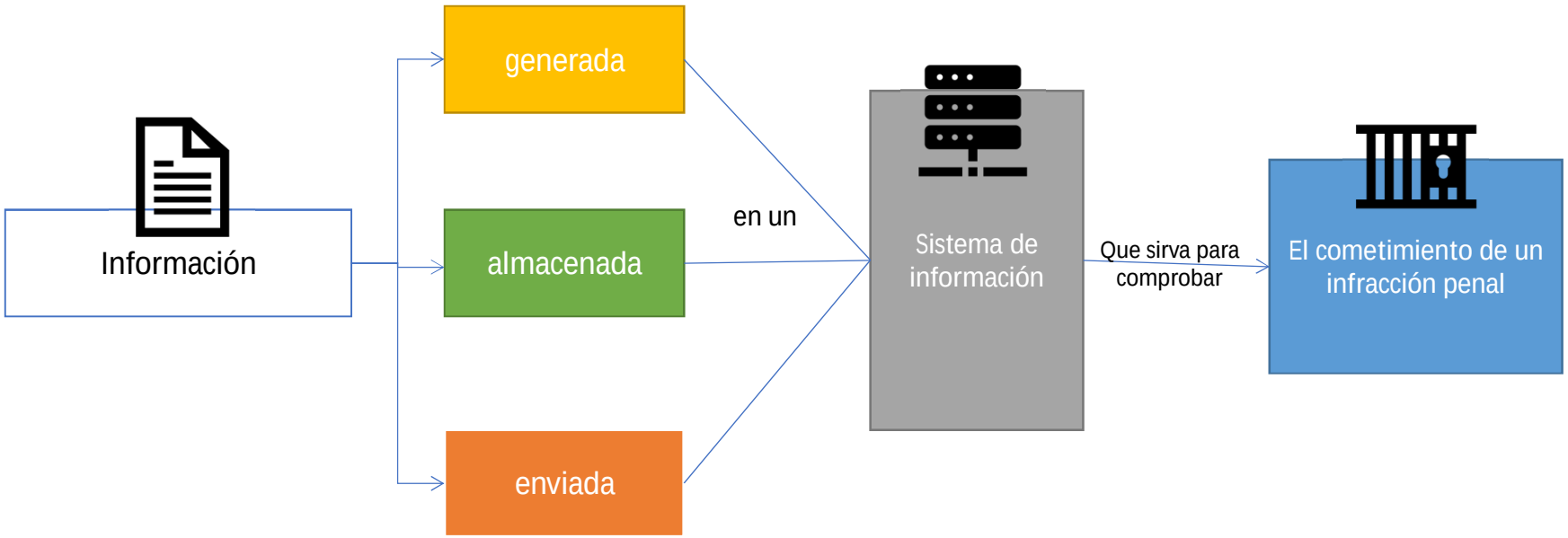
¿Qué nos preguntamos dentro de una investigación?



AECI

Asociación Ecuatoriana de Ciberseguridad

Que buscamos: Evidencia Digital



AECI

Asociación Ecuatoriana de Ciberseguridad

Clases de Evidencia Digital

En medios volátiles

- Registros internos de los dispositivos
- Memoria física
- Memoria caché
- Registro de estado de la red
- Contenido del portapapeles
- Registros de procesos en ejecución

En medios persistentes

- Discos duros internos y externos.
- Dispositivos de almacenamiento externos.
- Dispositivos de conectividad internos y externos.

AECI

Asociación Ecuatoriana de Ciberseguridad

¿Qué hacemos en la escena del delito?

Asegurar la escena

- Evitar la modificación o destrucción de evidencias digitales.
- Códigos de Integridad

Identificar evidencias

- Identificar los sistemas de información que contengan información relevante
- Evidencia Volátil o Persistente

Recolectar evidencias

- Minimizar el impacto en la evidencia original.
- Cadena de Custodia sobre los dispositivos de almacenamiento

El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de **técnicas digitales forenses**.
Art. 500.1 del COIP

AECI

Asociación Ecuatoriana de Ciberseguridad

Infraestructura Crítica Pública o Privada

- Cuando la evidencia digital se encuentre almacenada en sistemas de información pertenecientes a la **infraestructura critica** del sector público o privado, se realizará su recolección, en **el lugar y en tiempo real**, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido. Art. 500.2 COIP

AECI

Durante la recolección de evidencias

Capturar imágenes precisas.

Realizar notas detalladas, fechas, horarios.

Minimizar cambios y agentes externos.

Priorizar la recolección, antes del análisis.

Recoger la información según el orden de volatilidad.

Cada dispositivo puede ser recogida de manera diferente.

AECI

Asociación Ecuatoriana de Ciberseguridad

Qué buscamos en la escena del delito

Registros almacenados en el equipo de tecnología informática

- Correos electrónicos.
- Archivos de aplicaciones de ofimática.
- Imágenes,
- Documentos,
- Mensajes de datos, etc.

Registros generados por los equipos de tecnología informática

- Registros de auditoría.
- Registros de transacciones.
- Registros de eventos, etc.

Registros parcialmente generados y almacenados en los equipos de tecnología informática

- Hojas de cálculo .
- Consultas especializadas en bases de datos.
- Vistas parciales de datos, etc.

AECI

Que hacemos después en el Laboratorio Forense

Asociación Ecuatoriana de Ciberseguridad

Cuando es evidencia no volátil ni que pertenezca a la infraestructura crítica

Preservar evidencias

- Documentación detallada de los procedimientos realizados sobre las evidencias.

Analizar evidencias

- Seguir metodología forense especializada y las herramientas adecuadas.

Presentar resultados

- Los resultados deben presentarse de forma concreta, clara y ordenada.

AECI

Asociación Ecuatoriana de Ciberseguridad

Conclusiones

1. La modalidad de malware conocida como Ransomware está tipificada en el Código Orgánico Integral Penal.
2. Puede existir una concurrencia real de infracciones, por tanto se puede acumular la pena
3. Las infracciones comprendidas en el Ransomware son de acción pública (denuncia a la Fiscalía).
4. Para recuperar y preservar la evidencia digital se lo debe hacer utilizando técnicas digitales forenses, y siguiendo el trámite legal

AECI

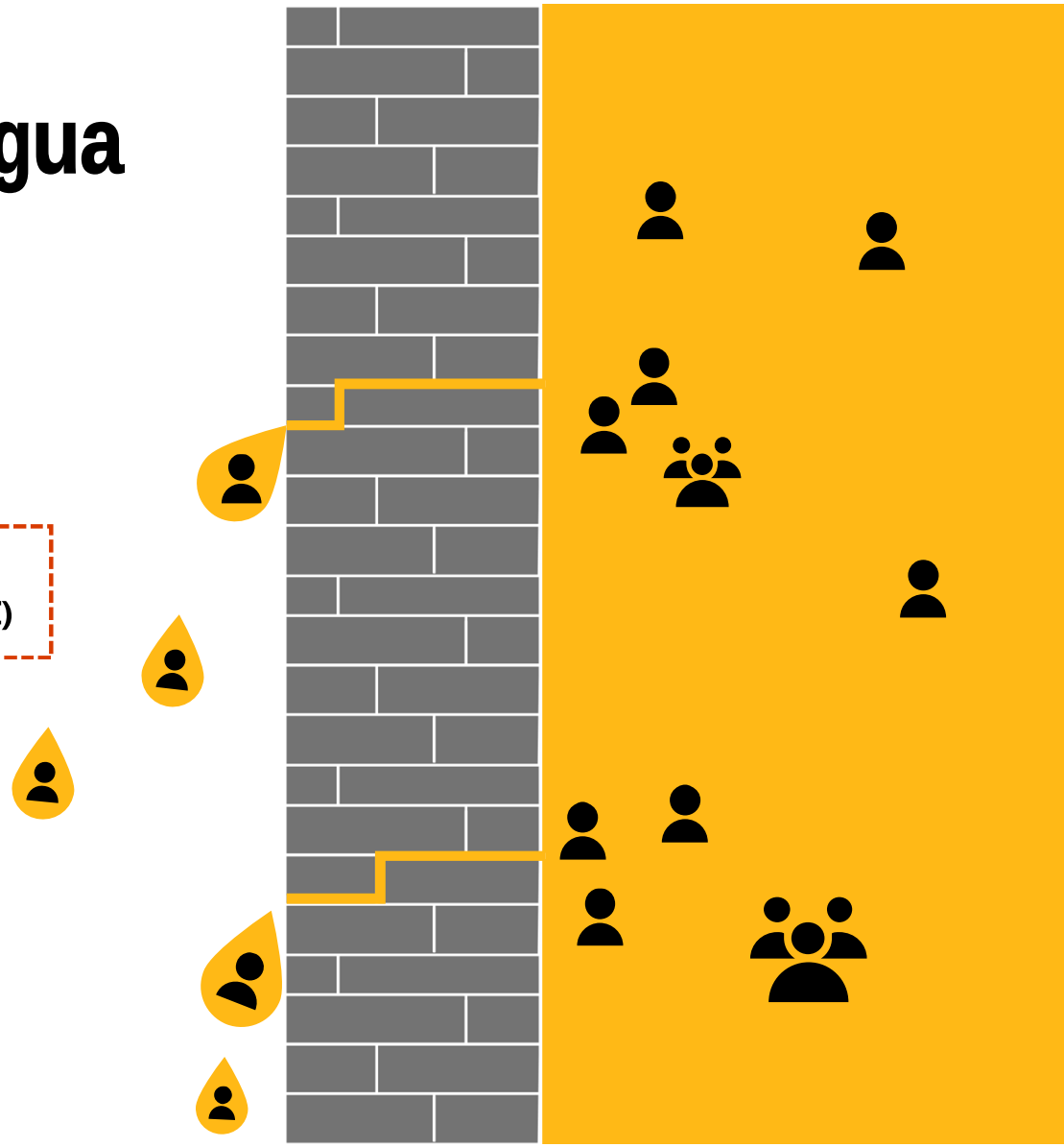
Los atacantes son como agua

Los atacantes toman el camino de menor resistencia para lograr los objetivos

Caminos / métodos establecidos

Nuevas aperturas más fáciles

Los atacantes solo se molestan cuando se vuelven buenos y cuando tienen un **Retorno de la Inversión (RI)**



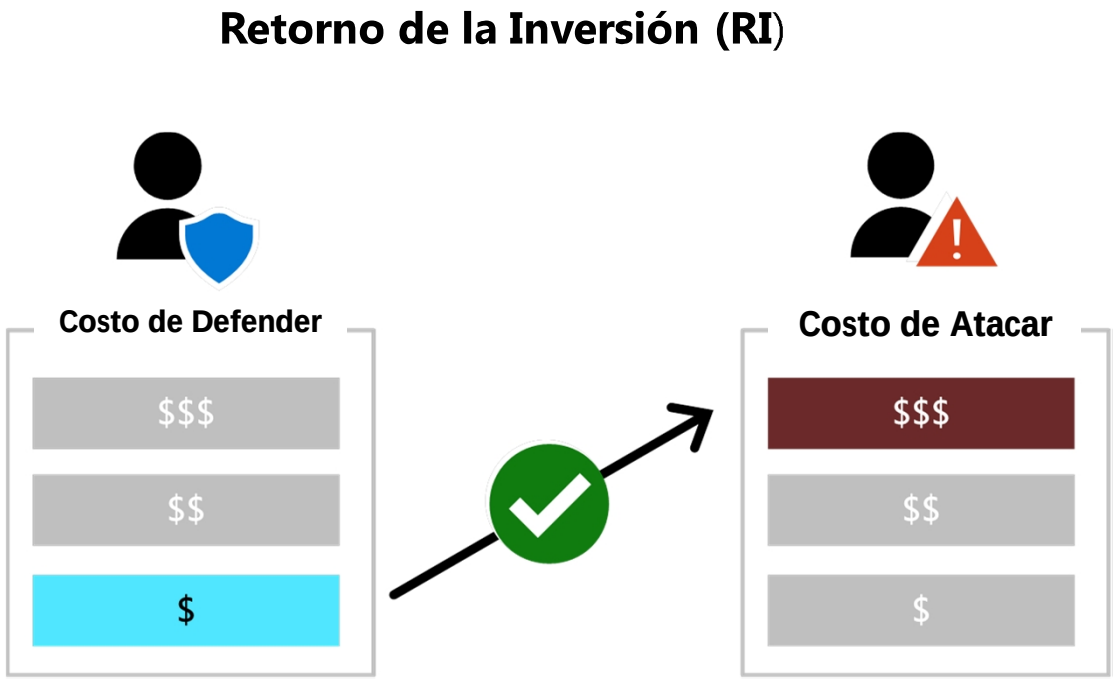
AECI

Objetivo de seguridad: interrumpir a los atacantes

Demore (y a veces detenga) a los atacantes

Busque medios eficientes para interrumpir los ataques

Aumente los costos de los atacantes con la menor cantidad de inversión en recursos

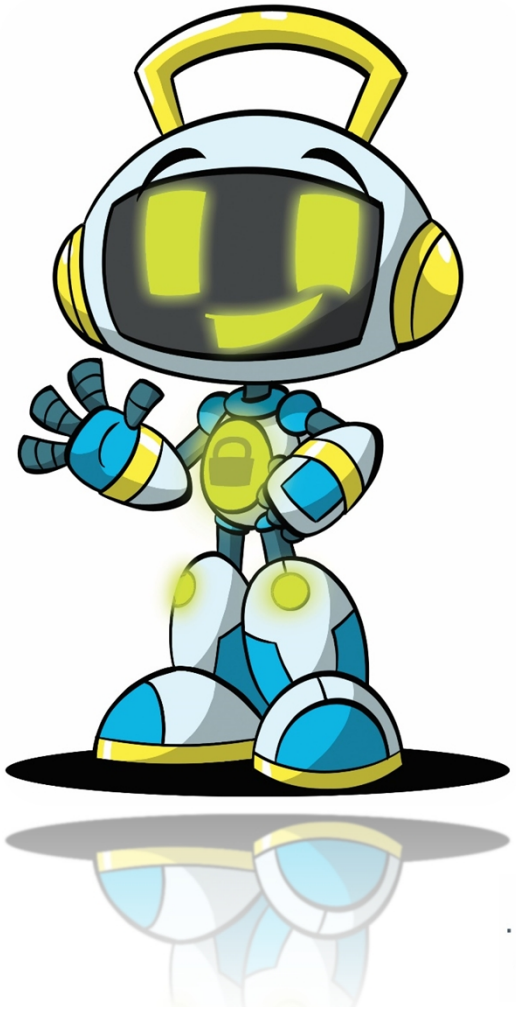


La extorsión (y los ataques destructivos) de ransomware solo funcionan cuando se pierde todo el acceso legítimo a los datos y los sistemas.

AECI

Asociación Ecuatoriana
de Ciberseguridad

¿CONSULTAS?



AECI

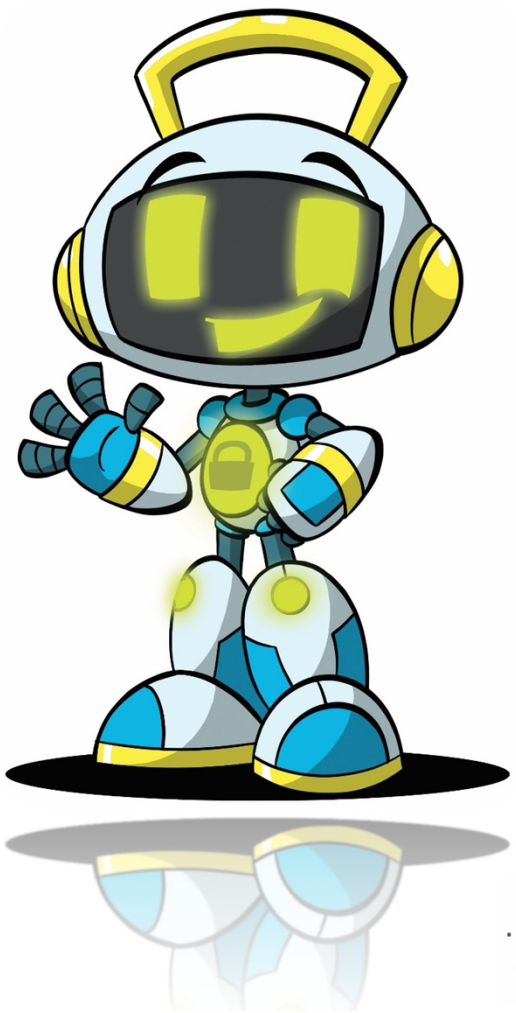
Asociación Ecuatoriana de Ciberseguridad

sacurio@hotmail.com

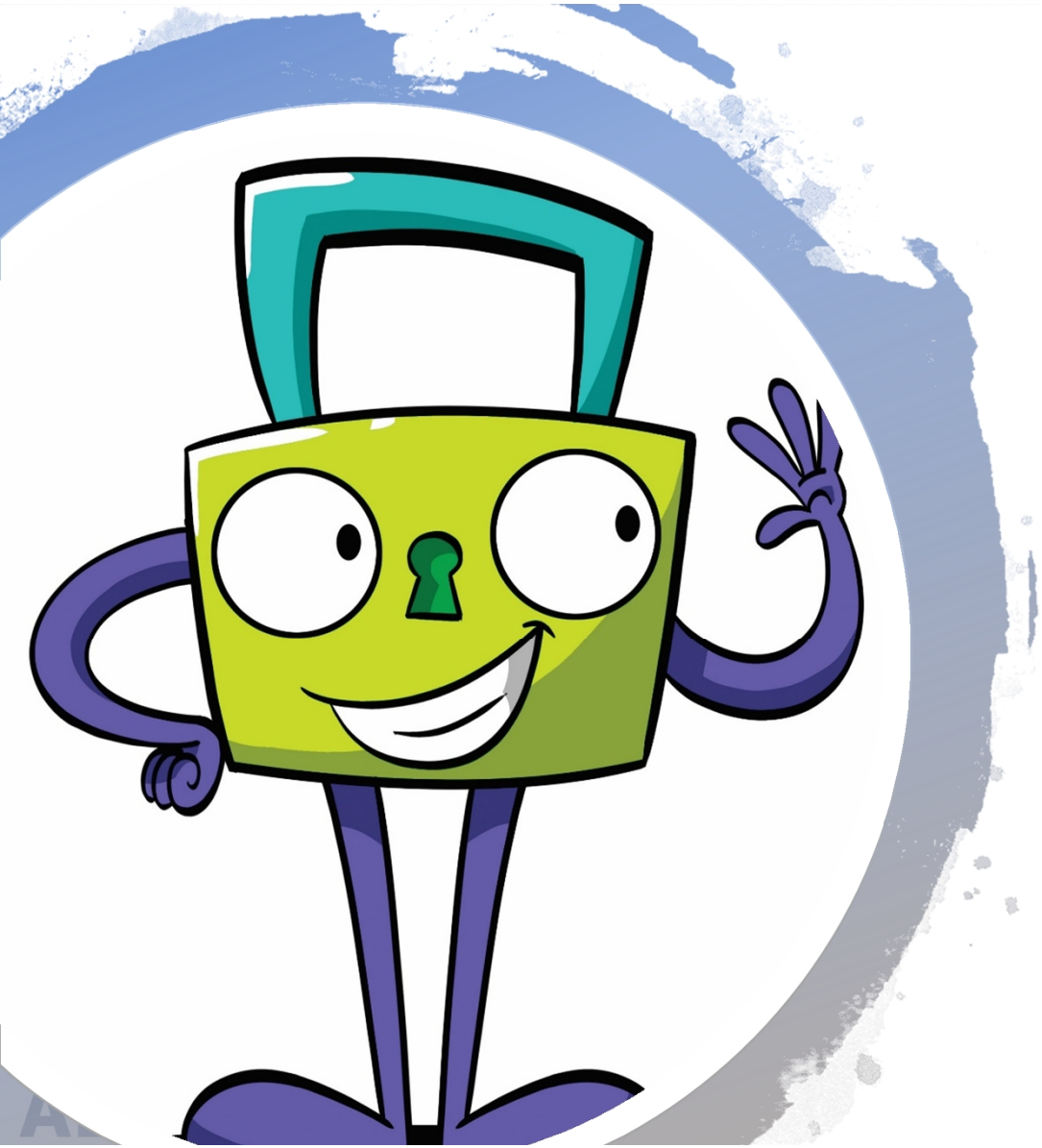
@AECIEcuador

@AECIb

www.linkedin.com/in/aeci/



AECI



¡GRACIAS POR SU TIEMPO!

AECI

Asociación Ecuatoriana de Ciberseguridad

2018 - 2021