AECI

Asociación Ecuatoriana de Ciberseguridad

“MANEJO Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD”

Asociación Ecuatoriana
de Ciberseguridad

AGENDA

- ¿Qué es un incidente?
- ¿Qué dicen las “buenas prácticas”?
- ¿Qué camino debemos seguir?
- Entonces, vamos por la gestión!

AECI

Presentación

Asociación Ecuatoriana de Ciberseguridad

Jorge C. Guerrón Eras.
SECURITY INFORMATION & GRC **SENIOR ADVISOR**

10 años de experiencia específica desarrollando diferentes actividades en sub ramas de la seguridad de la Información, como Auditor, Oficial de Seguridad de la Información, Perito Informático Forense, Ingeniero Preventa y actualmente desarrollo actividades como Consultor Senior en Seguridad de la Información, involucrado en el desarrollo satisfactorio de proyectos en Ecuador, Colombia, Brasil, Puerto Rico, USA, España.

Ingeniero en Sistemas formado específicamente, Máster en Seguridad de las Tecnologías de la Información y de las Comunicaciones - UOC-UAB-URV, Diplomado en Seguridad de Aplicaciones Web y Bases de Datos – UOC, Diplomado en Gobierno de TI, Auditoría y Seguridad de los Sistemas de Información - Centro de Innovación Tecnológica de la Fundación Rosario, Argentina, Diplomado Enseñanza-Aprendizaje efectivo en la Educación Superior.

CISM Certified Information Security Manager® An ISACA® Certification

CDPSE Certified Data Privacy Solutions Engineer™ An ISACA® Certification

IRCA

Banca, Economía Popular y Solidaria, Retail, Seguros, Petróleo y Gas, Educación, Call Center, Telecomunicaciones, Desarrollo de SW, Salud, Sector Público (Gobierno)

COBIT® 5 AN ISACA® FRAMEWORK

ITIL® Foundation V3

IT RISK FUNDAMENTALS An ISACA Certificate

@toquilla_hat

https://www.linkedin.com/in/jorgeguerroneras

AECI

Asociación Ecuatoriana
de Ciberseguridad

¿Qué es un incidente?

AECI

Asociación Ecuatoriana de Ciberseguridad

¿Qué nos dicen las “buenas prácticas”?

ITIL®

Incidente se refiere a una interrupción no planificada de un servicio, o reducción en la calidad de un servicio

El propósito de gestión de incidentes es minimizar el impacto negativo de los incidentes mediante la restauración del funcionamiento normal del servicio lo más rápido posible

AECI

Asociación Ecuatoriana de Ciberseguridad

¿Qué nos dicen las “buenas prácticas”?

COBIT 2019

DSS02: Proporcionar una respuesta oportuna y efectiva a las solicitudes de los usuarios y la resolución de todos los tipos de incidentes. Restaurar el servicio normal, registrar y completar las solicitudes de usuario; y registrar, investigar, diagnosticar, escalar y resolver los incidentes.

Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidencias de los usuarios. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio. Resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes.

AECI

Asociación Ecuatoriana de Ciberseguridad

¿Qué nos dicen las “buenas prácticas”?

NIST

Un ***evento*** es cualquier ocurrencia observable en un sistema o red.

Un ***incidente*** de seguridad informática es una violación o amenaza inminente de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas de seguridad estándar

AECI

Asociación Ecuatoriana de Ciberseguridad

¿Qué nos dicen las “buenas prácticas”?

ISO/IEC 27001

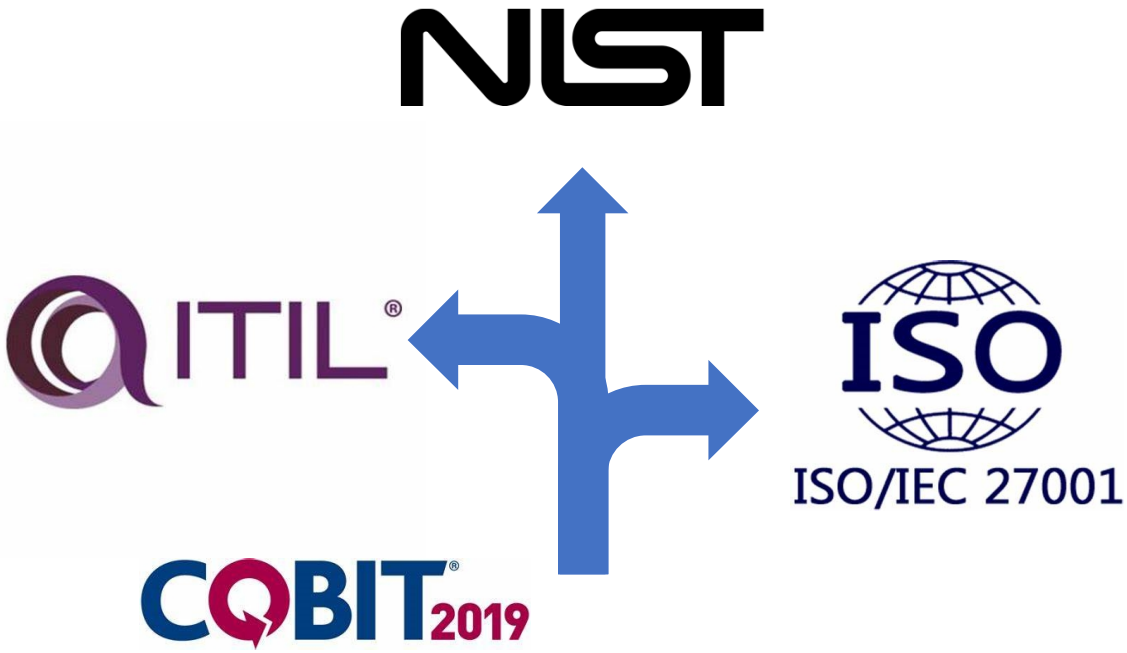
A.16.1 Gestión de incidentes de seguridad de la información y mejoras.

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

AECI

Asociación Ecuatoriana de Ciberseguridad

¿Qué camino debemos seguir?



AECI

Asociación Ecuatoriana de Ciberseguridad

Entonces, vamos por la gestión!

AECI

Asociación Ecuatoriana de Ciberseguridad

Preparación

1. Compromiso Alta Gerencia

2. Gestión del Riesgo

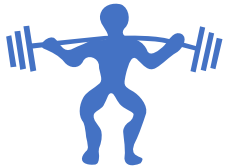
3. Gestión del Respaldos

4. Guía para atención

5. Medio de comunicación

6. Caja de herramientas

7. Selección del Equipo



8. Hardening

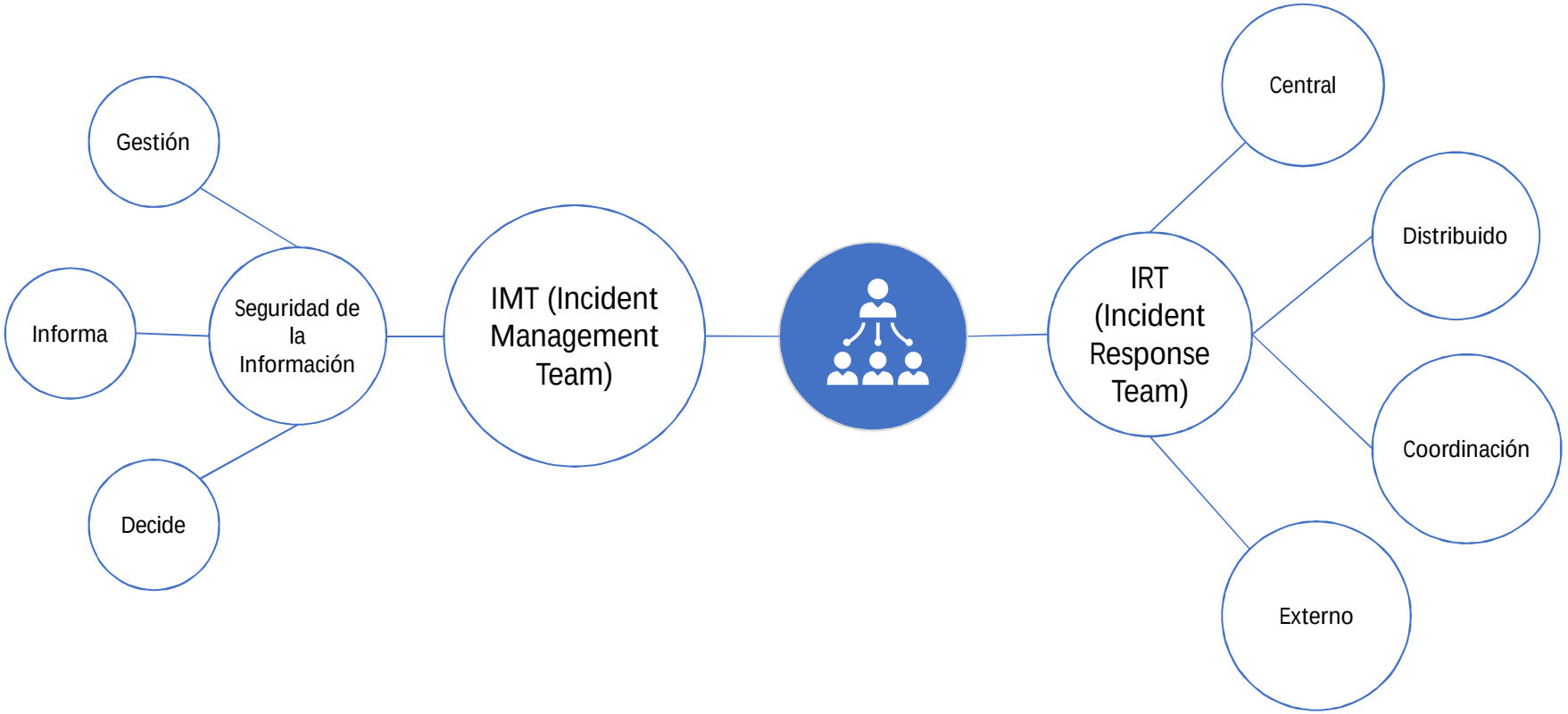
AECI

Preparación

Asociación Ecuatoriana de Ciberseguridad

AECI

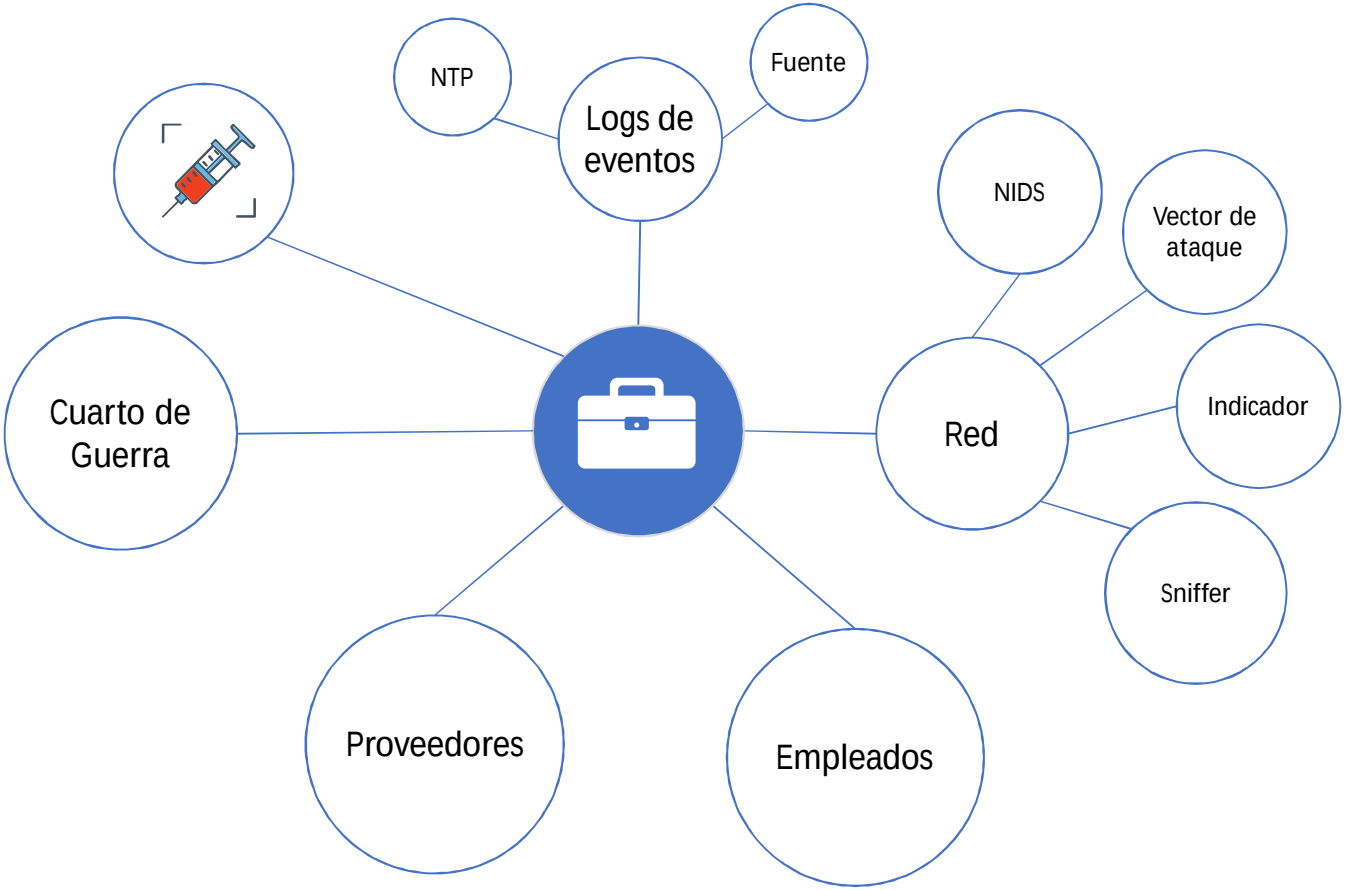
Preparación



Asociación Ecuatoriana de Ciberseguridad

AECI

Detección y Análisis



Asociación Ecuatoriana de Ciberseguridad

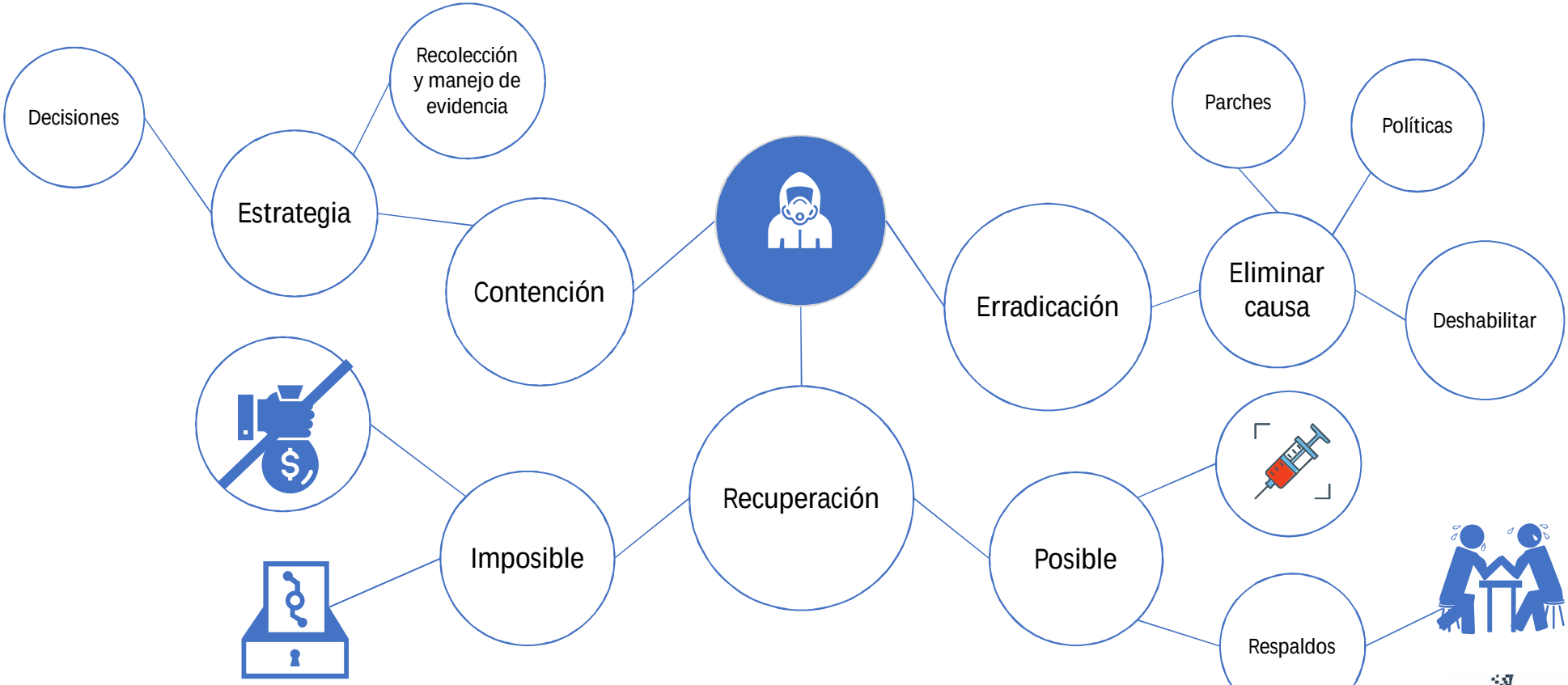
AECI

Asociación Ecuatoriana de Ciberseguridad

Contención, Erradicación y Recuperación

AECI

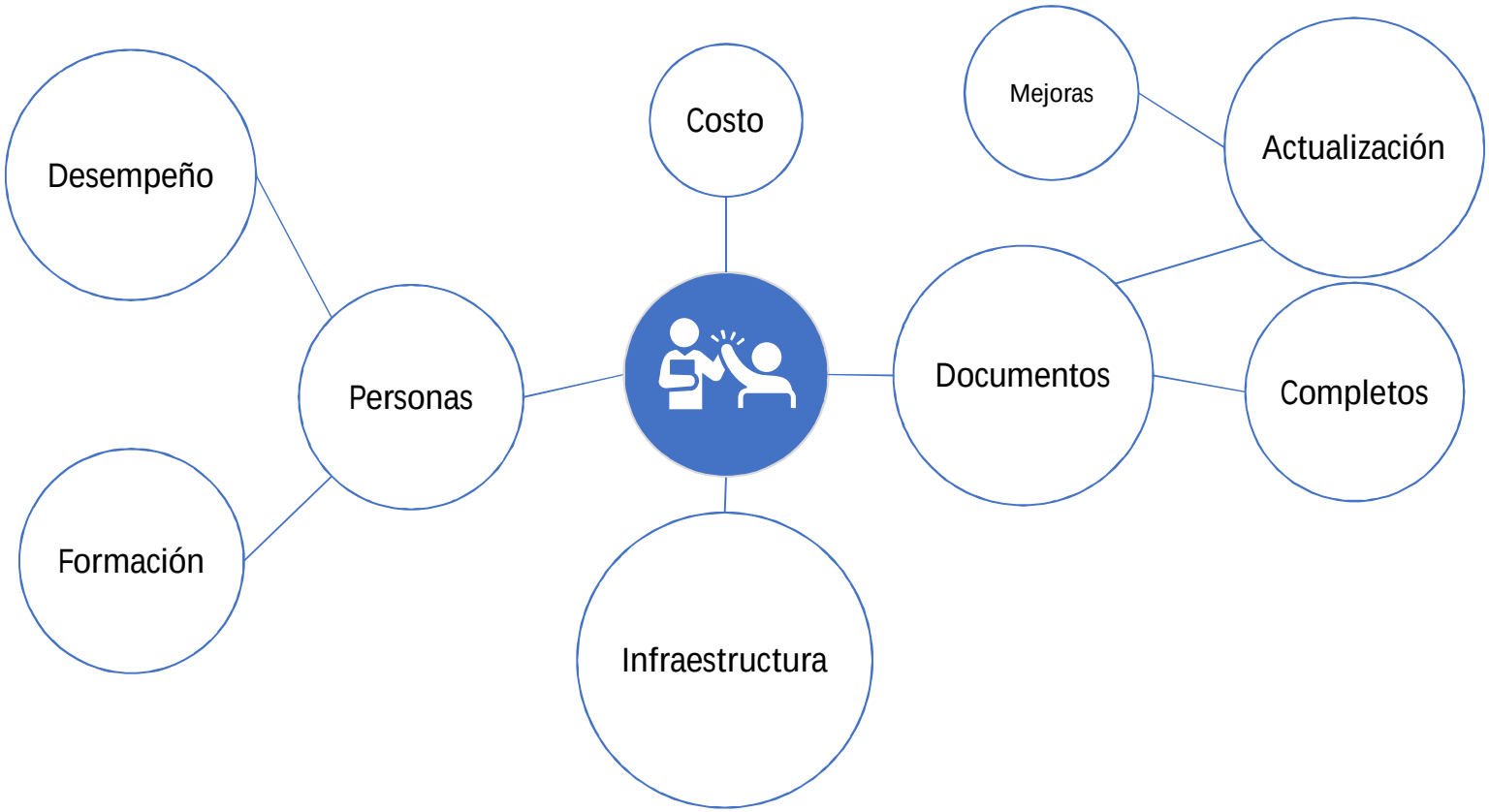
Contención, Erradicación y Recuperación



Asociación Ecuatoriana de Ciberseguridad

AECI

Actividades Post-incidente



Asociación Ecuatoriana de Ciberseguridad

AECI

Asociación Ecuatoriana de Ciberseguridad

Actividades Post-incidente

Art. 10 .- Principios

Calidad y Exactitud

Seguridad de datos personales

Responsabilidad proactiva y demostrada

Art. 17 .- Derecho a la portabilidad

AECI

Asociación Ecuatoriana de Ciberseguridad

Actividades Post-incidente

Art. 37 .- Seguridad de datos personales

Verificación, evaluación y valoración continua → **Medias de control**

Medias de control:
- **Anonimización**
  Seudononimización
  Cifrado
- **Mantener CIA**
- **Resiliencia** → **Técnica**, **Física**, **Administrativa**, **Jurídica**

Mitigación adecuada de riesgos

AECI

Actividades Post-incidente

Art. 38 .- Medidas de seguridad en el ámbito del sector público

EGSI v2 → **incluir** → **Medidas para los casos de tratamiento de datos personales**

AECI

Asociación Ecuatoriana de Ciberseguridad

Actividades Post-incidente

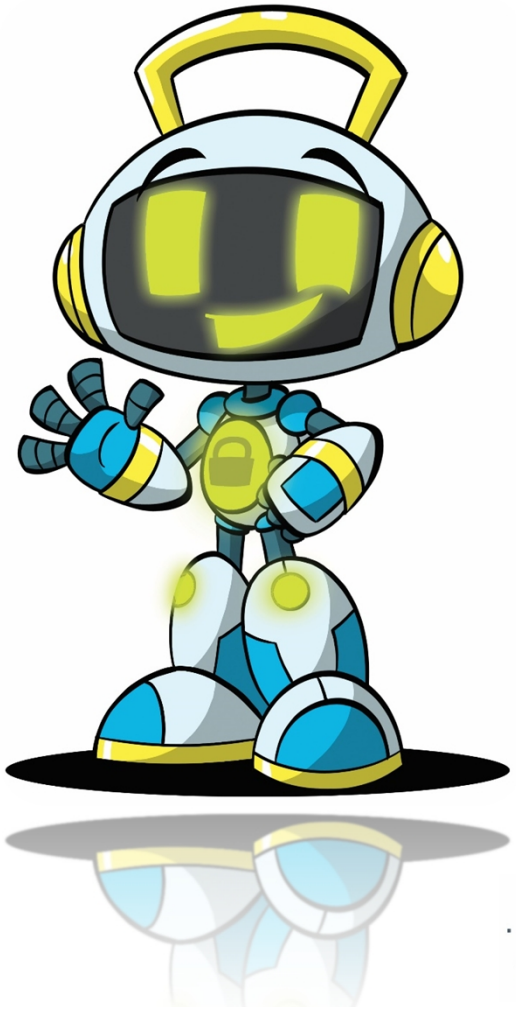
Art. 46 .- Notificación de vulneración de seguridad al titular

Medidas de respuesta → **Consideradas atenuante**

AECI

Asociación Ecuatoriana
de Ciberseguridad

¿CONSULTAS?



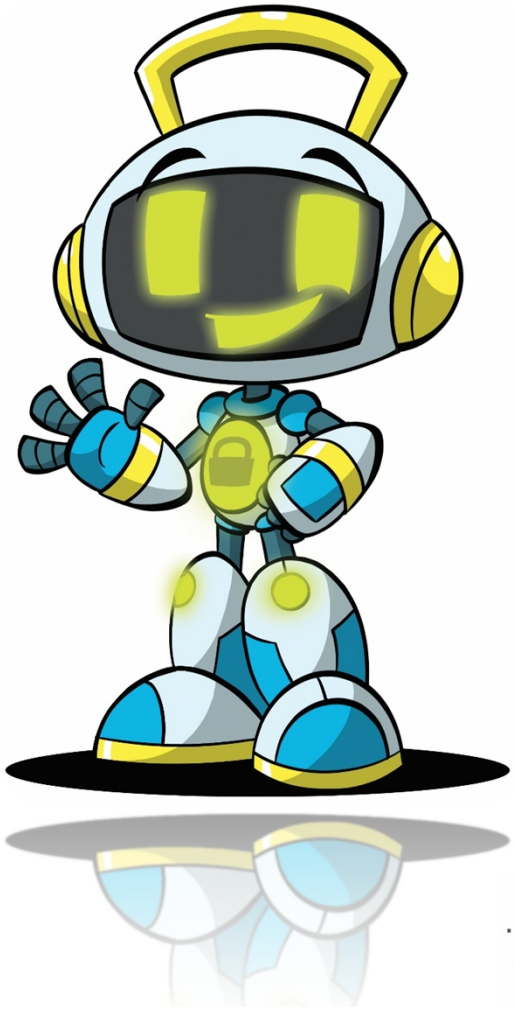
AECI

Asociación Ecuatoriana
de Ciberseguridad

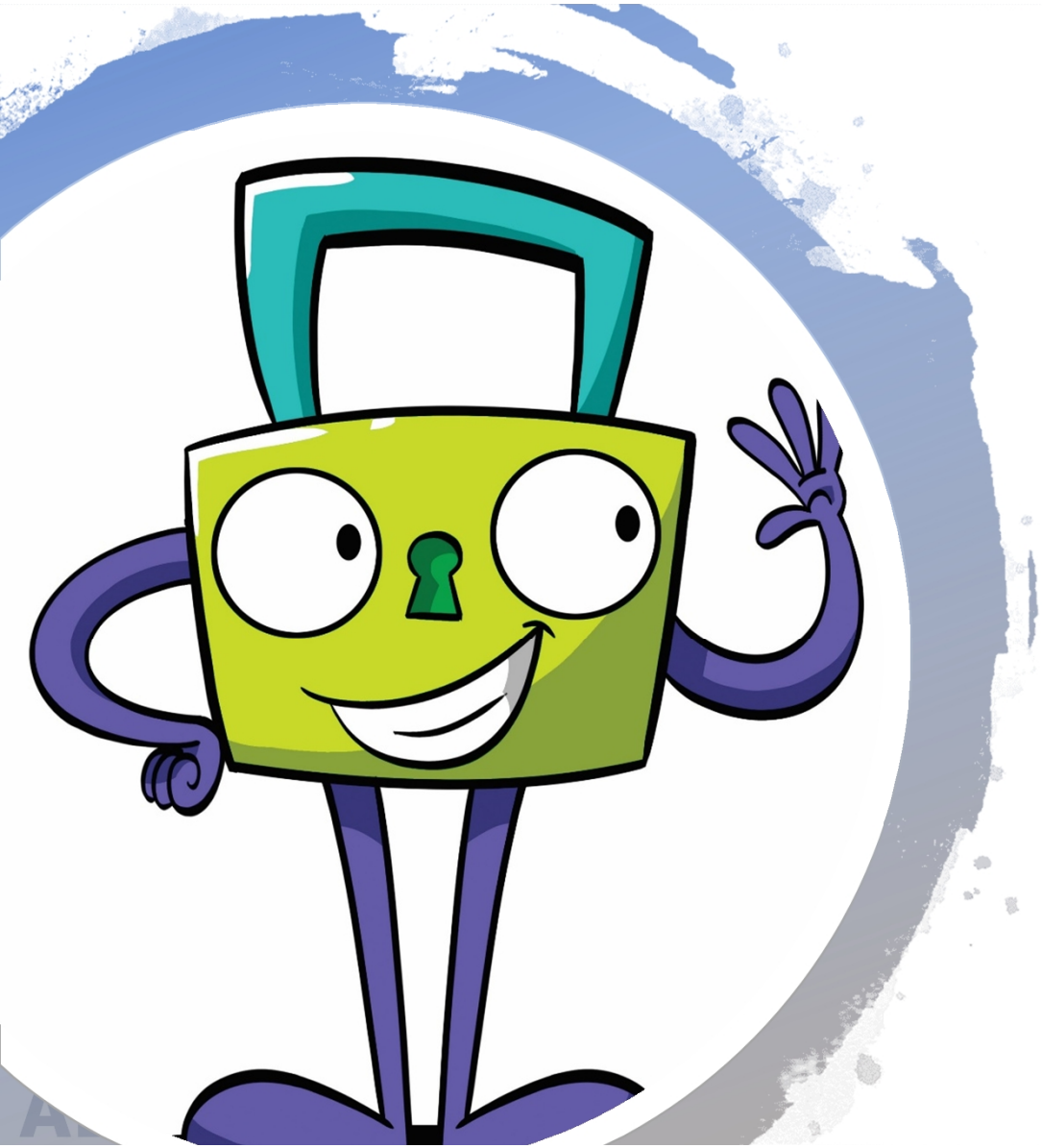
@AECIEcuador

@AECIb

www.linkedin.com/in/aeci/



AECI



¡GRACIAS POR SU TIEMPO!

AECI

Asociación Ecuatoriana de Ciberseguridad

2018 - 2021