



Tema:

Nuevos desafíos de la seguridad en la banca ecuatoriana y la reducción de las brechas de ciberseguridad a través de la implementación de un CSIRT financiero.

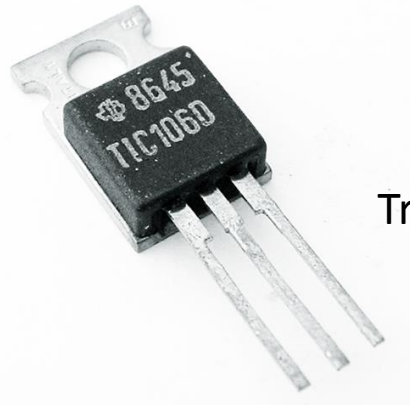
“CREANDO UN MUNDO DIGITAL MÁS SEGURO”



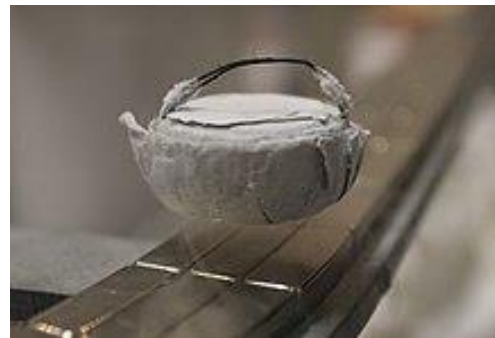
- Jhon Bardeen

CIBERSEGURIDAD - SEGURIDAD DIGITAL

“
*La ciencia es un esfuerzo de colaboración.
Los resultados combinados de **varias**
personas que trabajan juntas es a menudo
mucho más eficaz de lo que podría ser el
de un científico que trabaja solo.*
”



Transistor
-1956-



Superconductividad
-1972-

Agenda



1. Objetivos de la presentación.
2. Nuevos **desafíos de seguridad** en el sector financiero mundial.
3. Entender qué es un **CSIRT** y cómo opera.
4. Reducción de las **brechas de ciberseguridad**.
5. **Ventajas de contar** con un CSIRT como aliado

1.- Objetivos



Comprender los riesgos de ciberseguridad en el sector financiero.

Identificar posibles soluciones para minimizar o evitar el impacto de la materialización de riesgos.

Entender cuáles son las ventajas de contar con un CSIRT, que valor me agrega.

Analizar los campos de acción de un CSIRT.



Agenda seguimiento

1. ~~Objetivos de la presentación.~~
2. Nuevos **desafíos de seguridad** en el sector financiero mundial.

2.- Desafíos de Ciberseguridad

Crimen organizado, en los ataques al sector financiero

- Crecen robos a cajeros electrónicos, acusa empresa ciber forense; Phishing, rebasado; predominan agresiones a entidades del sector



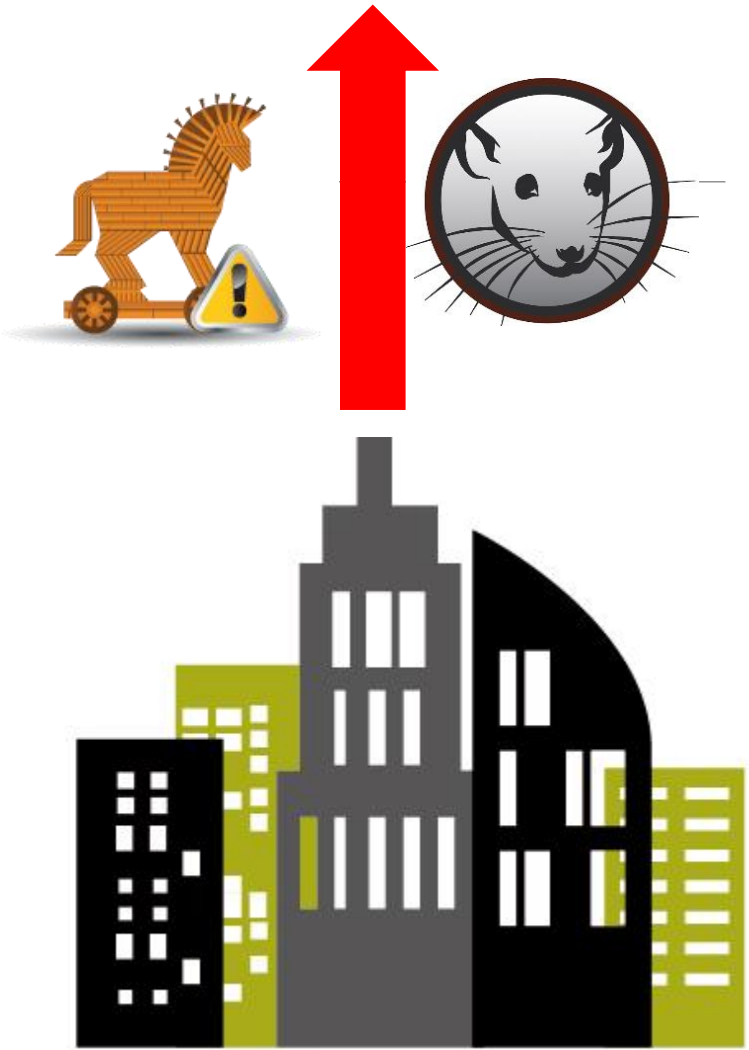
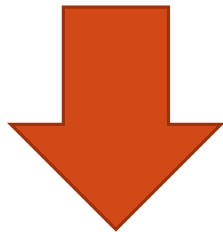
2.- Desafíos de Ciberseguridad

Sector Financiero

1. Phishing,
2. Malware bancario,
3. Ataques a móviles,
4. POS (Puntos de venta),
5. ATM (Cajeros automáticos).



2.- Ataques a entidades financieras



2.- Ataques informáticos



Agentes de la Amenaza



Métodos de Ataque



Vulnerabilidades

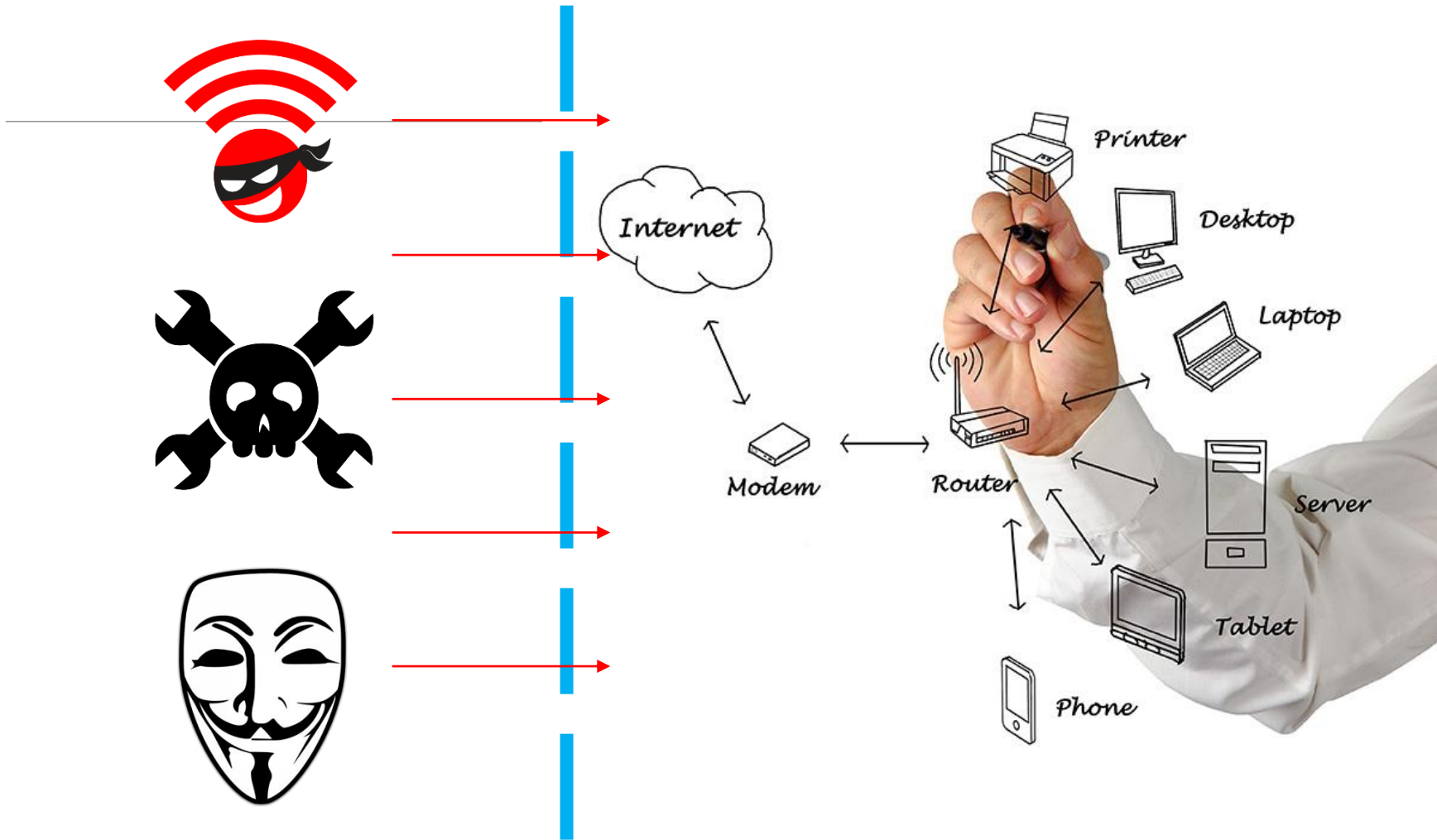


Medidas

2.- Ataques informáticos

	2013	2014	2015	2016
Vulnerabilidades				
Empleados descuidados o desinformados	53%	57%	44%	55%
Controles de seguridad o arquitectura de información desactualizados	51%	52%	34%	48%
Acceso no autorizado	34%	34%	32%	54%
Amenazas				
<i>Malware</i>	41%	34%	43%	52%
Suplantación de identidad (<i>Phishing</i>)	39%	39%	44%	51%
Ataques cibernéticos para robar información financiera	46%	51%	33%	45%
Ataques cibernéticos para robar <i>IPs</i> o datos	41%	44%	30%	42%
Ataque internos	28%	31%	27%	33%

2.- Riesgo financiero



2.- Situación actual (Sector financiero)



capacidad de respuesta

Escaza o nula



Escasez de CSIRTs
y personal
capacitado



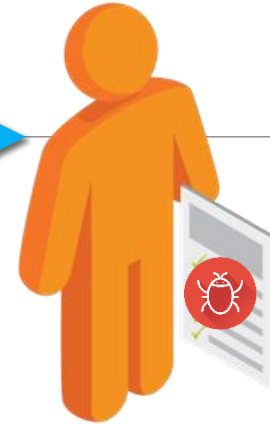
Número creciente de organizaciones - Usuarios



2.- Situación actual (Sector financiero)



tener un plan
respuesta a incidentes



Creciente número
de amenazas





~~Problema~~

Solución

Agenda seguimiento

1. ~~Objetivos de la presentación.~~
2. ~~Nuevos desafíos de seguridad en el sector financiero mundial.~~
3. Entender qué es un **CSIRT** y cómo opera.

3.- ¿Qué es un CSIRT?



CSIRT

*EQUIPO DE RESPUESTA A
INCIDENTES DE SEGURIDAD
DE LA INFORMACIÓN*

Grupo de **expertos** en Ciberseguridad



Procedimientos y políticas predefinidas.

Incidentes de **seguridad informática**

Bomberos – salvar vidas



Paramédicos – Salvar Vidas



CSIRT – Salvar los Activos



Colaboración - Apoyo



Crear - Confianza



Cuando los segundos importan



¿Para que un CSIRT?



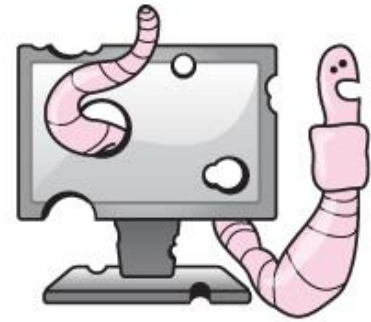
Para apoyar el negocio





“Creando un mundo digital más seguro”

3.- CSIRT - Nacimiento



En el año **1988**, el Internet se ve afectado por un **gusano** y deja fuera de servicio a muchos sistemas informáticos.

Se define una **estrategia global** para mejorar respuesta a incidentes de seguridad informática.

La agencia **DARPA** crea el **CERT/CC** en el SEI de la Carnegie Mellon University.

3.- CSIRT - Misión



Investigar

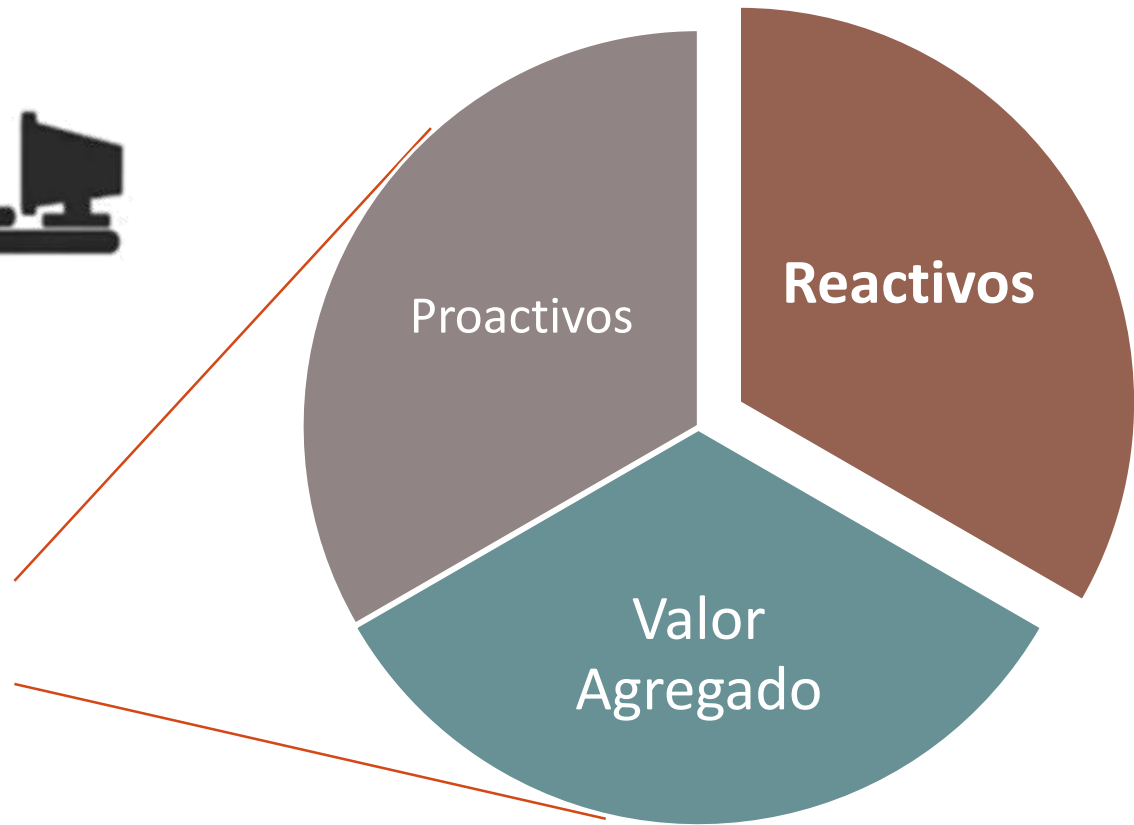
Mitigar

Prevenir

3.- CSIRT - Servicios



Servicios



3.- ¿Qué es un CSIRT?

CSIRT

Computer
Security
Incident
Response
Team

Servicios - PRO

- Análisis de **riesgos**,
- Análisis **forense**
- Gestión de **vulnerabilidades**.
- Planes de **continuidad de negocio**,
- Protección **fuera del firewall**
- Análisis de **malware** y muchas otras áreas.

3.- Tipos de CSIRT

CSIRT Interno Sectorial

- Educativo
- Gubernamental
- Infraestructuras críticas
- **Financiero**

JPMORGAN CHASE & CO.

Bank of America 

Centros de Coordinación (CERT)

- País
- Estado
- Región



Centros de Análisis (investigación)

Comercial (SLA)

SWITCH

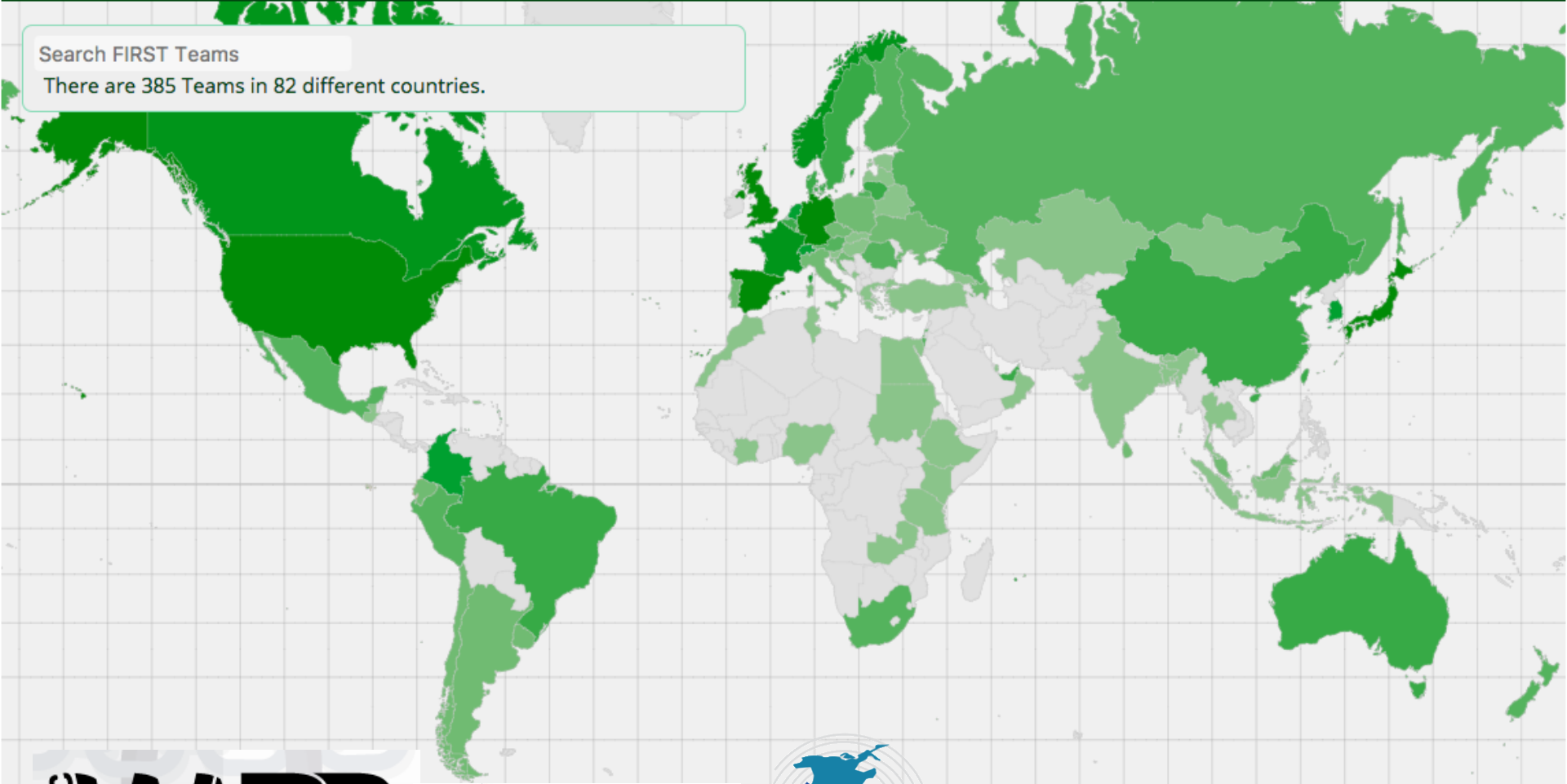


3.- CSIRT en el mundo

FIRST Members around the world

Search FIRST Teams

There are 385 Teams in 82 different countries.



Unifying the Global Response to Cybercrime

Agenda seguimiento

1. ~~Objetivos de la presentación.~~
2. ~~Nuevos desafíos de seguridad en el sector financiero mundial.~~
3. ~~Entender qué es un **CSIRT** y cómo opera.~~
4. Reducción de las **brechas de ciberseguridad.**

4.- Reducción de brechas



4.- CSIRT FINANCIERO



CSIRT: Un modelo de respuesta

Con enfoque organizacional para la gestión de **incidentes de ciberseguridad** en el sector financiero.

Cumplimiento Regulatorio

Resolución JB-2014-3066



2017 ...

Big Data

IoT

Banking online

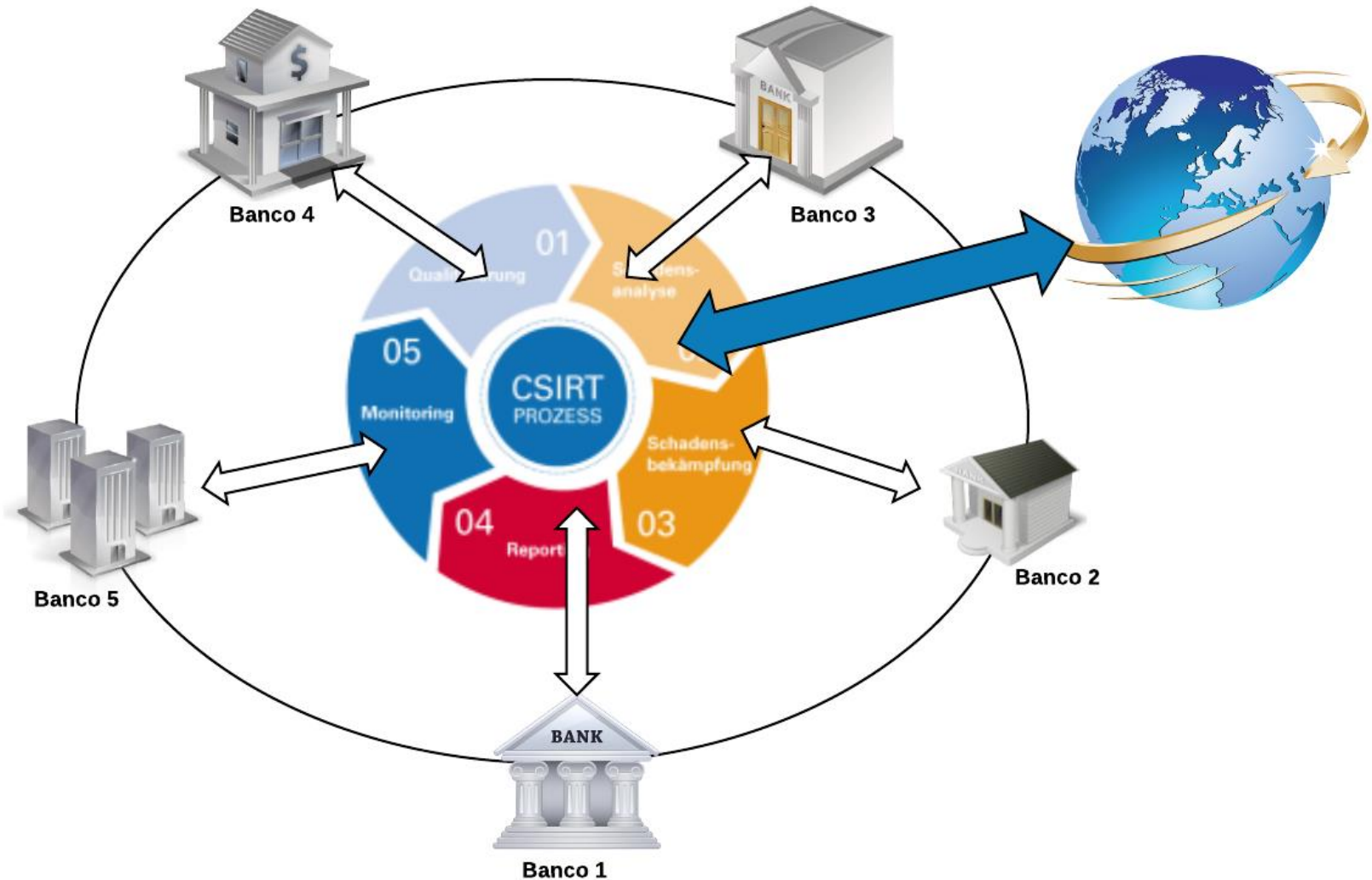
E-commerce

Dinero electrónico

Usuario interno y externo



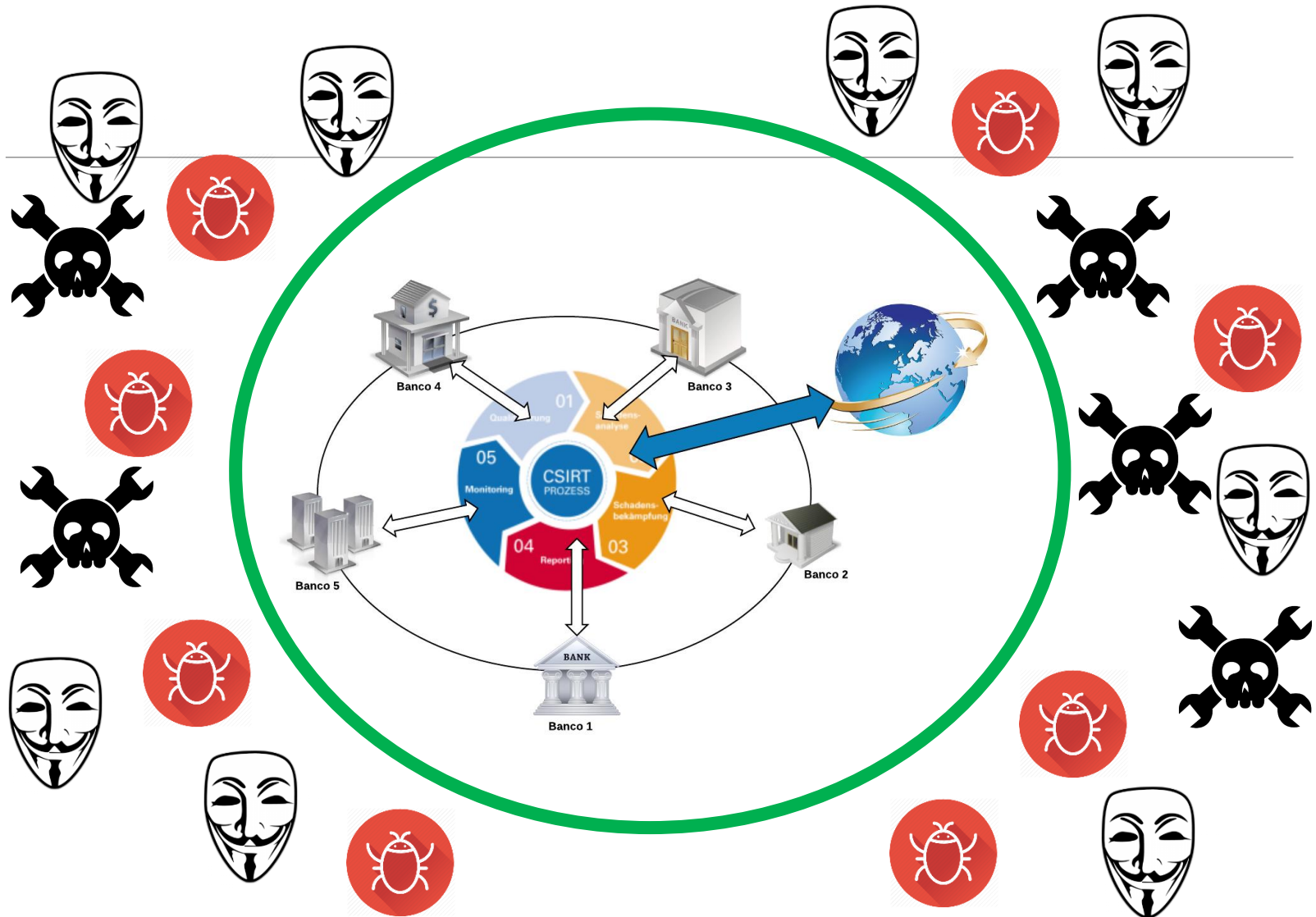
4.- CSIRT FINANCIERO



4.- CSIRT FINANCIERO



4.- CSIRT FINANCIERO



Agenda seguimiento

1. ~~Objetivos de la presentación.~~
2. ~~Nuevos desafíos de seguridad en el sector financiero mundial.~~
3. ~~Entender qué es un **CSIRT** y cómo opera.~~
4. ~~Reducción de las **brechas de ciberseguridad.**~~
5. **Ventajas de contar con un CSIRT como aliado**

5.- CSIRT: Ventajas

Equipo Humano y tecnológico



5.- CSIRT: Ventajas Recuperación



5.- CSIRT: Ventajas

Prevención y planificación





5.- CSIRT: Ventajas

Defensa y protección
de activos **críticos**

5.- CSIRT: Ventajas Concientización y educación



Muchas gracias su atención!!

José María Gómez de la Torre Gómez
jm.gomez@gruporadical.com

