



# Experiencias en la creación de CSIRT en Iberoamérica

Carlos Doce Reyes

Director

MCSec

# Ponente: Carlos Doce Reyes

- Ingeniero Informático – Universidad Politécnica de Catalunya
- MSc. Network Centred Computing - University of Reading
- Master en tecnologías de seguridad informática – UPC-esCERT
- CISA, CISM – ISACA
- FIH y AIH – Carnegie Mellon University, SEI
- ITIL Foundations v3, ITIL Service Manager v2 – EXIN
- CEH – ECCouncil
- FCNSA, FCNSP – Fortinet
- DFUC, DFSC y DFAC – Damballa
- LogRhythm
- Profesor de Análisis Forense – Universitat Oberta de Catalunya

## Audiencia Objetivo

Charla orientada a organizaciones que estén valorando crear un CSIRT, organizaciones que actualmente gestionan incidentes de forma informal o equipos de respuesta a incidentes con poco tiempo de existencia.

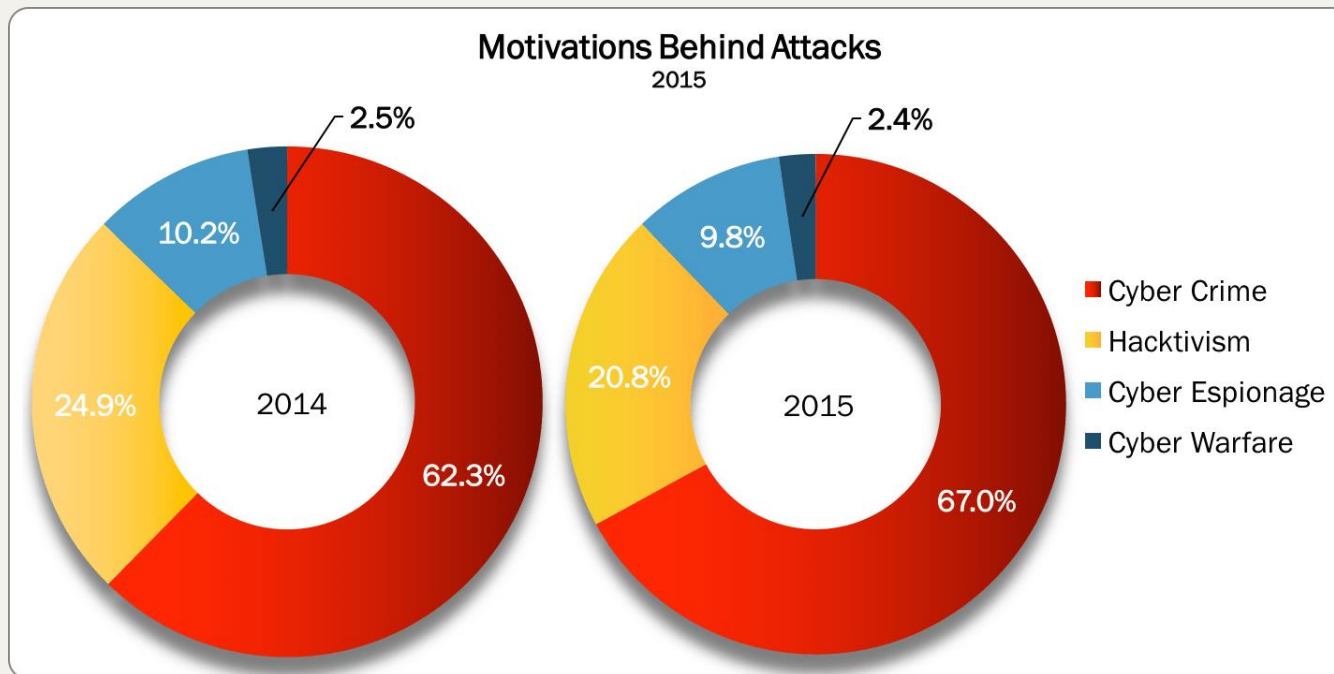
# Índice

- Introducción
- Estado del arte de los ataques
- Creación de un CSIRT

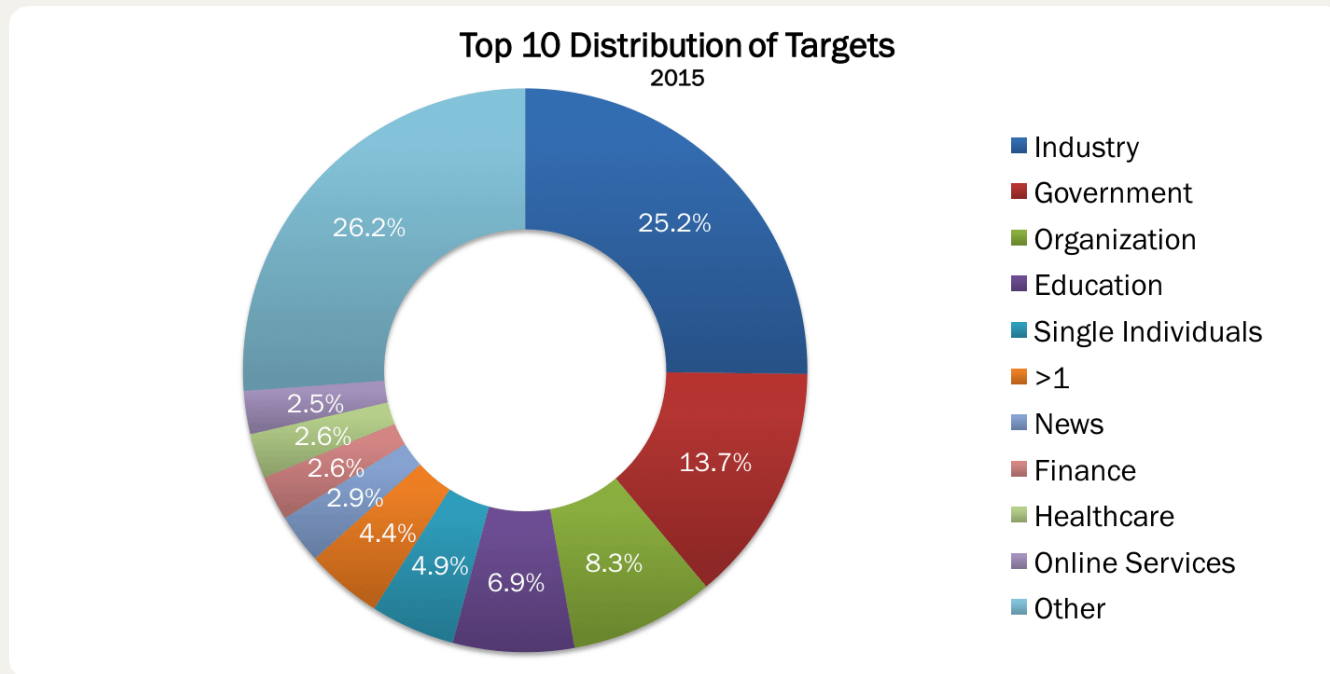
# Introducción

- La tecnología moderna y la constante conexión a Internet por parte de la sociedad moderna ha permitido un crecimiento enorme de los servicios que se ofertan en la red.
- Los criminales cibernéticos están descubriendo nuevas formas cada vez más complejas de aprovechar las redes para sus propósitos maliciosos.
- En los últimos años las amenazas a la seguridad han evolucionado hasta convertirse en complejos sistemas diseñados para robar información mediante una vasta variedad de vectores de ataque.
- El creciente uso de la encriptación resulta en que cada vez sea más difícil detectar los ataques.

# Motivación de los ciberataques



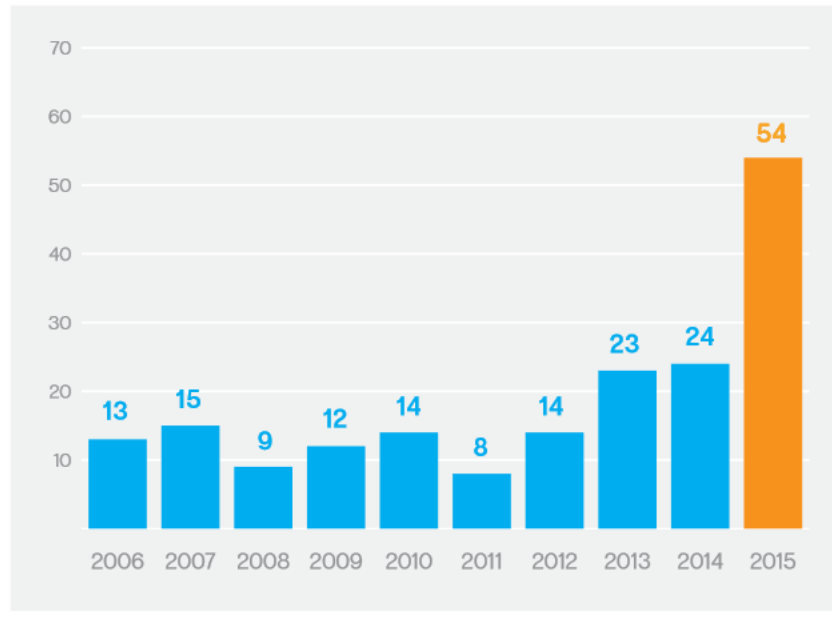
# Distribución de los ciberataques



# 0-day en 2015

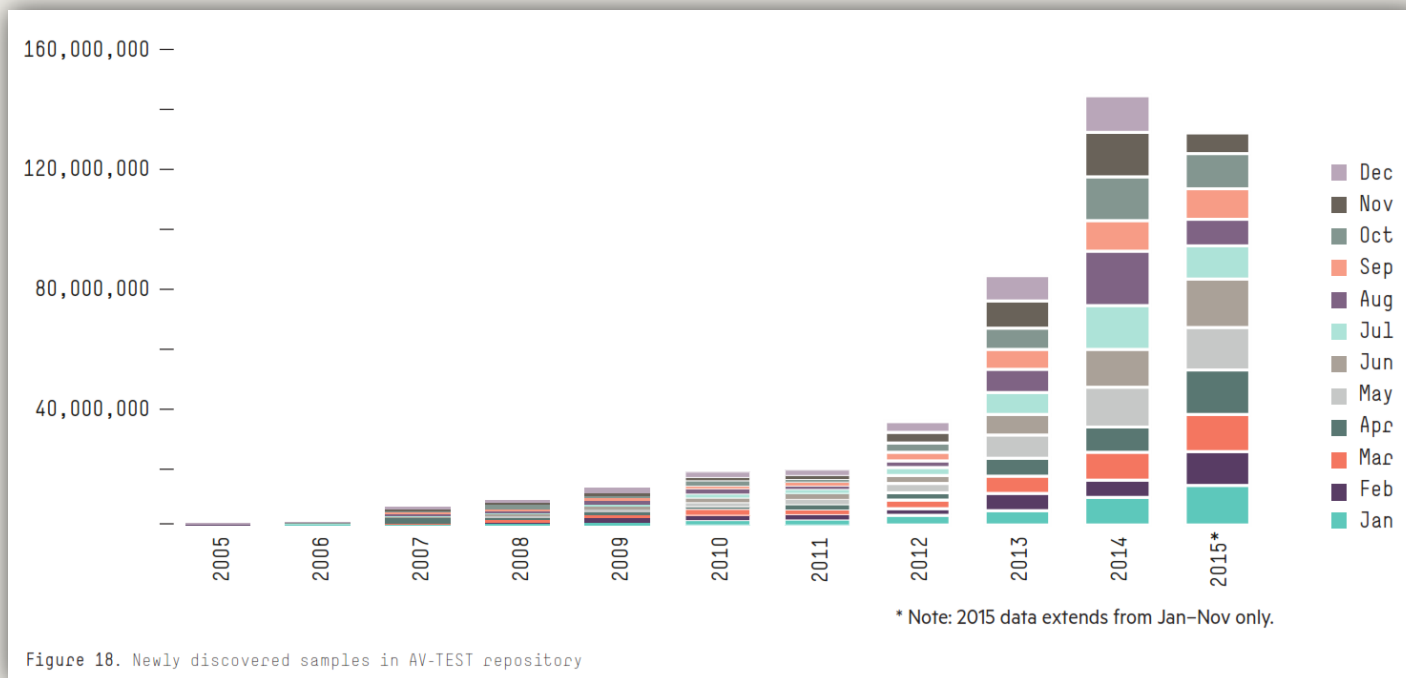
## Zero-Day Vulnerabilities, Annual Total

- ▶ The highest number of zero-day vulnerabilities was disclosed in 2015, evidence of the maturing market for research in this area.





# Crecimiento de Malware a través de los años

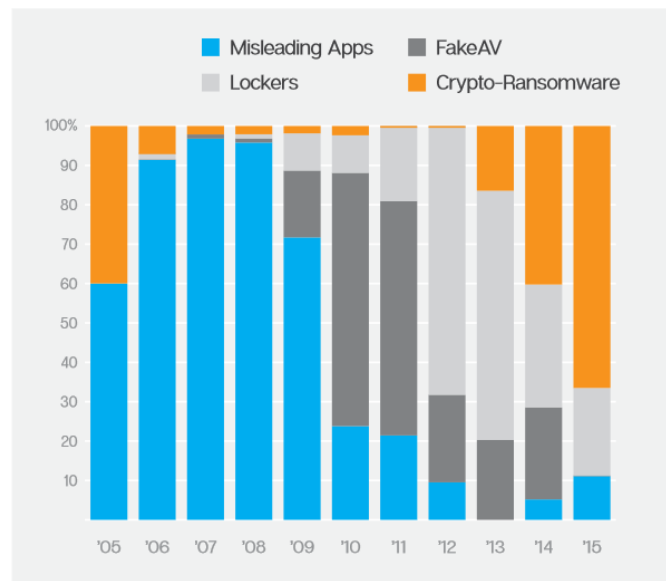


# Malware en 2016

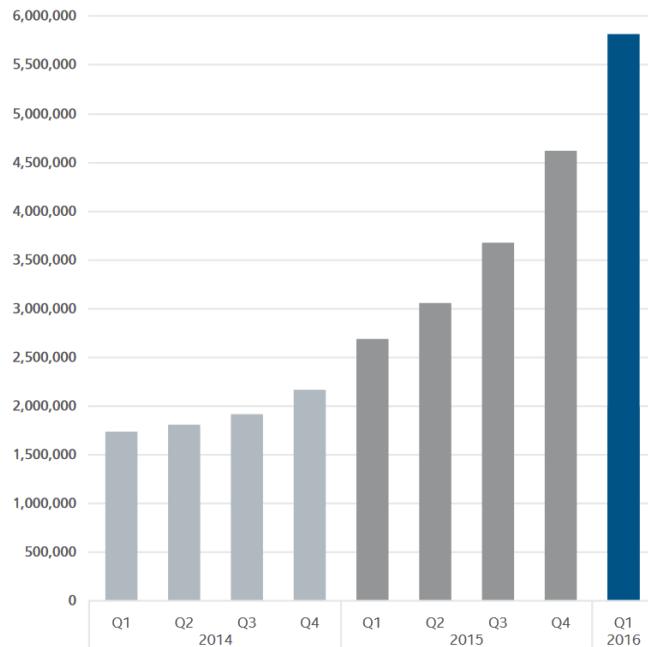
## Crecimiento de Ransomware

### Growing Dominance of Crypto-Ransomware

- Percentage of new families of misleading apps, fake security software (Fake AV), locker ransomware and crypto ransomware identified between 2005 and 2015.














### Total Ransomware



Source: McAfee Labs, 2016.

# Top 10 de Fuga de datos

## Top 10 breaches

 myspace	359,420,698	MySpace accounts
	164,611,595	LinkedIn accounts
	152,445,165	Adobe accounts
	112,005,531	Badoo accounts  
	93,338,602	VK accounts
	68,648,009	Dropbox accounts
<b>tumblr:</b>	65,469,298	tumblr accounts
	49,467,477	iMesh accounts
	40,767,652	Fling accounts 
<b>lost.fm</b>	37,217,682	Last.fm accounts



Perimeter security > Endpoint security > Breach Detection... "The Last Line of Defense"



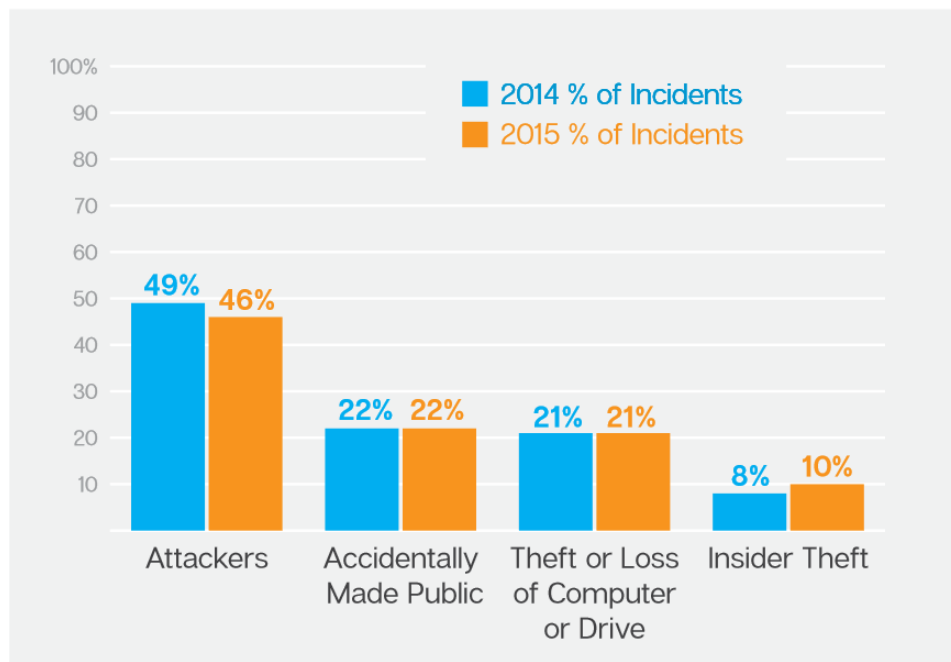
**66%** of breaches remain undetected for months

**87%** of breaches are discovered by external parties

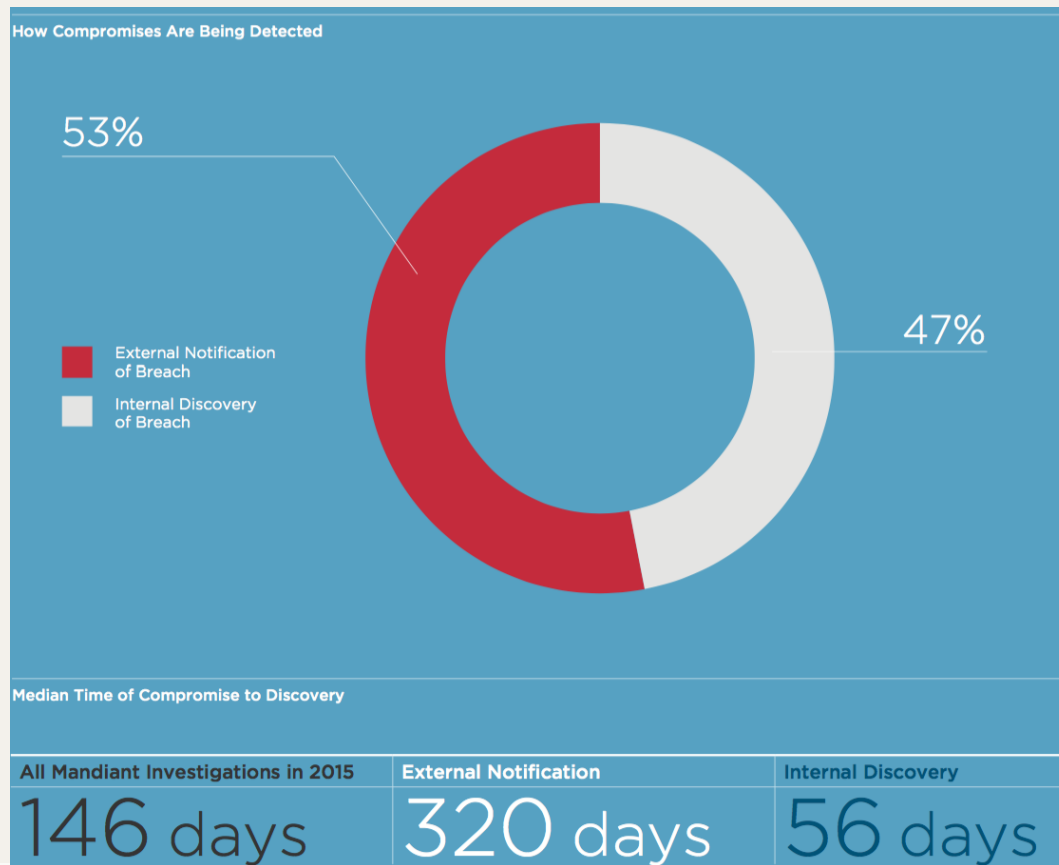
# Incidentes: Causas

## Top Causes of Data Breach by Incidents

- The proportion of incidents involving insider theft grew from less than one percent in 2014 to 10 percent in 2015.



# Incidentes: Detección



# ¿Cómo responden la mayoría de organizaciones?



## ¿Y las preparadas?





## CSIRT – Objetivos Estratégicos

- Prevenir los ataques cibernéticos contra las redes y sistemas y los entes gestores de infraestructuras críticas
- Reducir las vulnerabilidades ante ataques cibernéticos
- Minimizar los daños y tiempos de recuperación ante ataques cibernéticos

# CSIRT con los que he colaborado



# Características de los CSIRT

## Con qué contaban todos

- Financiación / sponsor
- RFC 2350
  - Misión, visión y objetivos
  - Comunidad (constituency) y autoridad bien definida
  - Servicios definidos\*
  - Claves PGP
- FIRST / Trusted Introducer\*
- Personal técnico formado
- Canales de comunicación (web, email, teléfono, etc.)

## Características especiales

- SLA/OLA
- Cuadros de mando
- Laboratorio forense
- Abogado/periodista/...
- Nivel de recursos
- Planes de formación
- Servicios

# Servicios CSIRT

## Reactive Services



- + Alerts and Warnings
- + Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- + Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- + Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

## Proactive Services



- ⦿ Announcements
- ⦿ Technology Watch
- ⦿ Security Audit or Assessments
- ⦿ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- ⦿ Development of Security Tools
- ⦿ Intrusion Detection Services
- ⦿ Security-Related Information Dissemination

## Security Quality Management Services



- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

# Servicios de los CSIRT

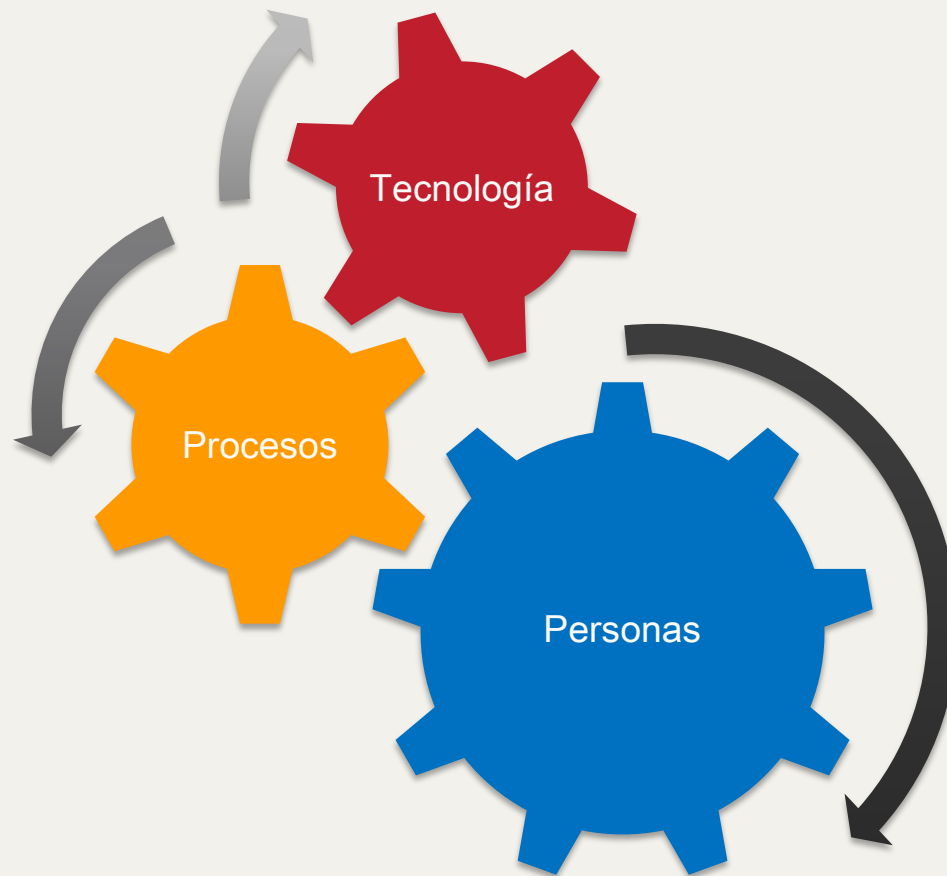
## Con que contaban todos

- Atención de consultas
- Gestión de incidentes
- Alertas a su comunidad
- Awareness
- Formación a terceros
- Respuesta a incidentes remota

## Servicios especiales

- Respuesta a incidentes in-situ
- Gestión de vulnerabilidades
- Análisis forense
- Monitoreo de redes
- Escaneo de vulnerabilidades
- Gestión de artefactos
- Desarrollo de herramientas
- Análisis de riesgos

# ¿Qué se requiere para un CSIRT?



# Lo más básico

## Personas

- Líder
- Legal
- RH
- Marketing
- Pentesters
- Incident Handlers

## Procesos

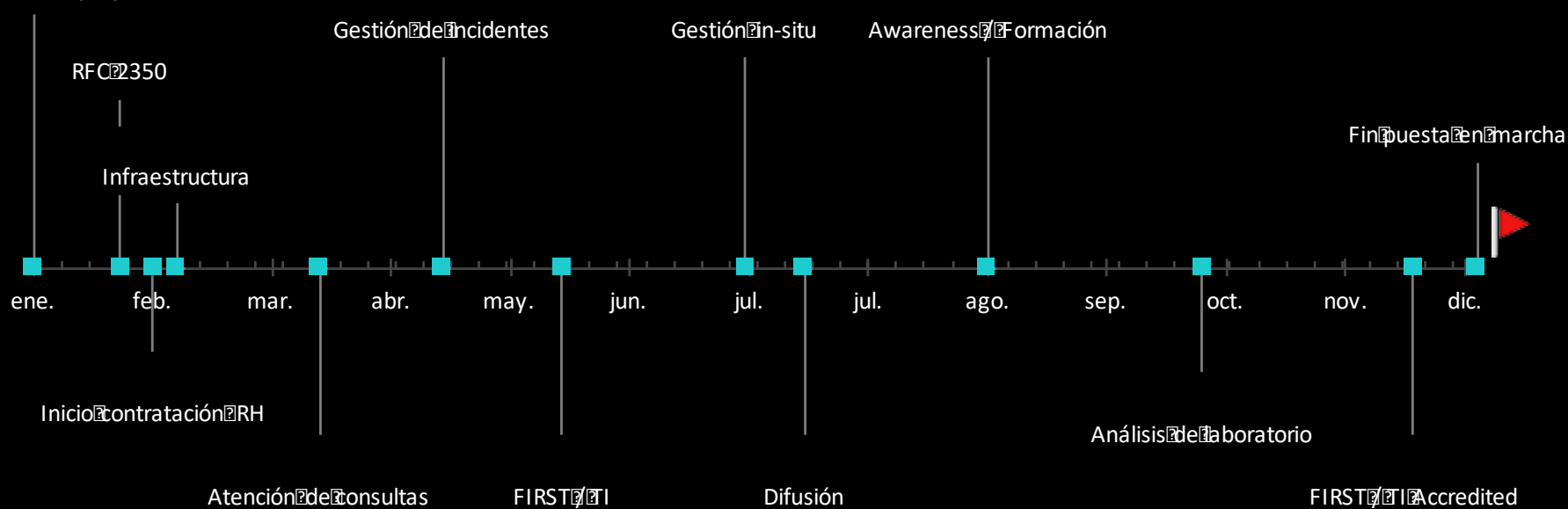
- Modelo conceptual
- Caso de negocio
- Políticas / Normas / Procesos / Guías
- Training

## Tecnologías

- Infraestructura: oficina, mobiliario, impresoras, laptops, servidores, red, etc.
- Protección CSIRT: NGFW, IPS, SIEM, anti-malware, etc.
- Gestión seguridad: ticketing, Office, ...
- Comunidad: email, sondas, etc.
- Análisis: sandbox, forense, IR, etc.

# Cronología

Comienzo del proyecto





# FIRST Full member



# Conclusiones

- La sofisticación de los ataques hace imposible la protección tradicional con mecanismos aislados. Es necesaria una estrategia a nivel de la organización.
- La protección de las infraestructuras críticas depende en gran parte de la seguridad cibernética de sus componentes TIC.
- Es primordial el desarrollo de mecanismos de monitoreo, detección, alerta y respuesta temprana ante incidentes, fallas o ataques de seguridad cibernética → CSIRT.
- Existen muchos modelos para desarrollar esta estrategia, sin embargo no son recetas de cocina, deben adaptarse a la realidad de organización.
- Se requiere personal altamente capacitado y experimentado.

# ¿Preguntas?



Carlos Doce Reyes

carlos@mcsec.com.mx

<https://mx.linkedin.com/in/carlosdocereyes>