Talking about CSIRT's…

Fast Track

- Introducing CSIRT
- About CSIRT-NQN

OWASP

The Open Web Application Security Project

About me

OWASP
The Open Web Application Security Project

Lic. Victor Figueroa
Dirección de Ciberseguridad
SMGP |OPTIC | Neuquén

CSIRT-NQN

OPTIC
Oficina Provincial de Tecnologías de la Información y la Comunicación

https://csirt-nqn.neuquen.gov.ar

GOBIERNO DE LA PROVINCIA DEL NEUQUÉN

NEUQUÉN PROVINCIA

- **Maestría Universitaria en Seguridad Informática**
- **Diplomado en Delitos Informáticos**
- **Diplomado en Informática Forense**
- **Licenciado en Informática**
- **Analista en Computación**

Mail: vfigueroa@neuquen.gov.ar

Tel: +54 299 449-5882

OWASP
The Open Web Application Security Project

Fast Track

- **Introducing CSIRT**
  - Defining Incident Response Team
  - Standars & Frameworks
  - Setting up Incident Response Team
- **About CSIRT-NQN**
  - Review SMGP/OPTIC
  - Review CSIRT-NQN
  - Home Task: MITRE CALDERA

OWASP
The Open Web Application Security Project

CSIRT :: Computer Security Incident Response Team

Equipo de Respuesta a Incidentes de Seguridad Informática. Es un centro de respuesta a incidentes de seguridad responsable del desarrollo de medidas preventivas y reactivas relacionadas a la Seguridad Informática, en el contexto de una organización.

Antecedentes

*El 2 de noviembre de 1988, **Morris** fue el primer malware autorreplicable que infectó a aproximadamente 6.000 de los 60.000 Servidores conectados a la internet…*

OWASP
The Open Web Application Security Project

Standars & Frameworks

FIRST CSIRT Framework

ENISA CSIRT Setting Up Guide

SP-800-61 Rev. 2 CS Incident Handling Guide
NIST Cybersecurity Framework

Guías CCN-STIC

Setting up Incident Response Team

- Composición del Equipo
- Definición de Servicios brindados
- Definición de Clientes (constituency) atendidos
- Capacitación y Especialización
- Definición de Metodología de Respuesta
- Obtención de Herramientas
- Vinculación y Colaboración

OWASP
The Open Web Application Security Project

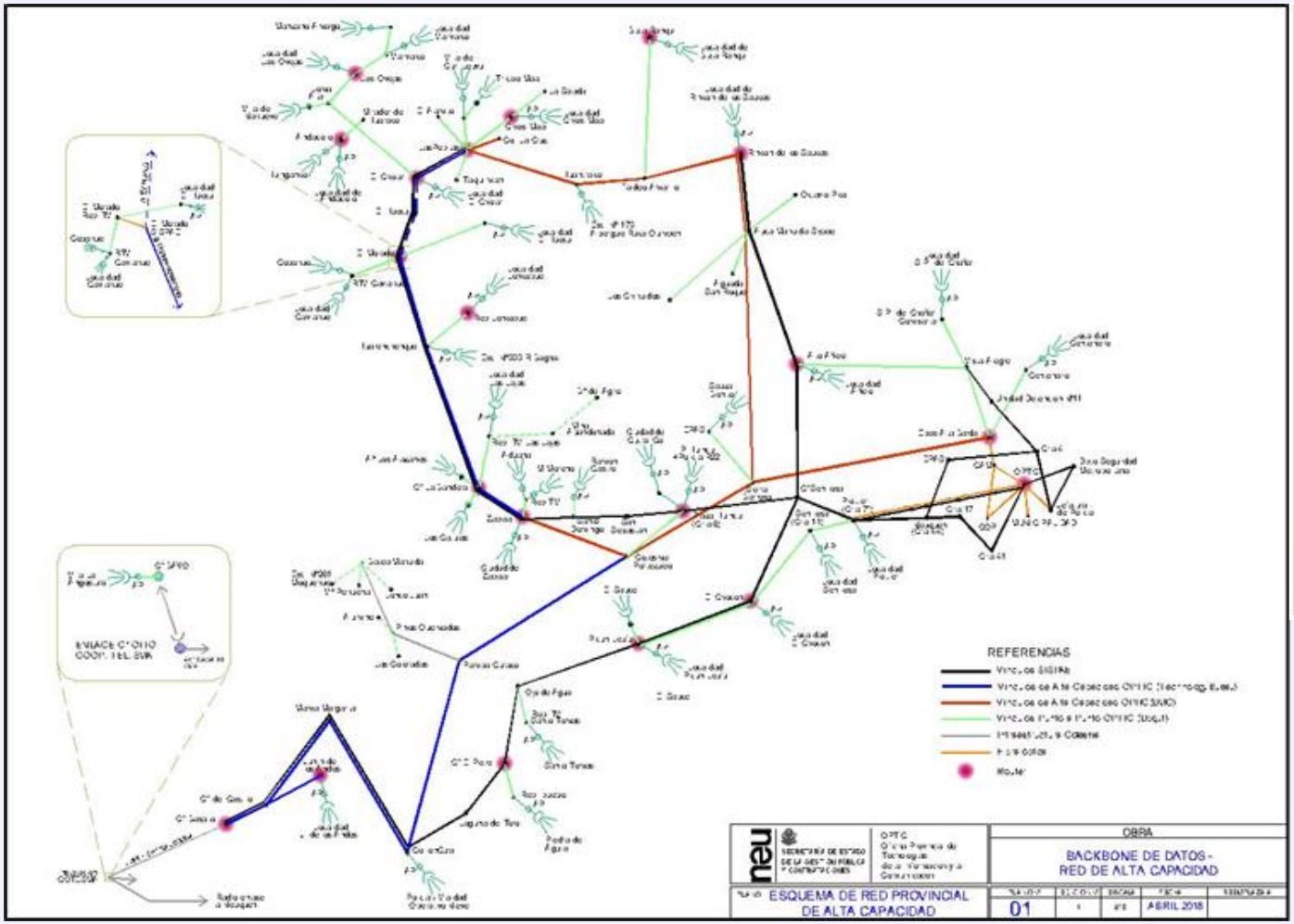
Review SMGP/OPTIC

Secretaría de Modernización de la Gestión Pública

Oficina Provincial de Tecnologías de la Información las y Comunicaciones

OWASP
The Open Web Application Security Project

Review SMGP/OPTIC



OWASP
The Open Web Application Security Project

Review CSIRT-NQN. Composición del Equipo

OPTIC
Oficina Provincial de Tecnologías de la Información y la Comunicación

- Especialista en Infraestructura
- Especialista en Servicios Web
- Especialista en Base de Datos
- Especialista en Redes
- Especialista en Gestión de Requerimientos
- Coordinado x Dirección de Ciberseguridad

OWASP
The Open Web Application Security Project

Review CSIRT-NQN. Composición del Equipo

CSIRT-NQN

- Especialista en Infraestructura
- Especialista en Servicios Web
- Especialista en Base de Datos
- Especialista en Redes
- Especialista en Gestión de Requerimientos
- Coordinado x Dirección de Ciberseguridad

Review CSIRT-NQN :: Servicios brindados

CSIRT-NQN

Reactivos

Alertas y Advertencias

Respuesta a Incidentes

- Apoyo
- Tratamiento
- Análisis

Laboratorio Forense Digital

Review CSIRT-NQN :: Servicios brindados

CSIRT-NQN

Reactivos

- Comunicados
- Observatorio de Tecnologías
- Charlas, Talleres, Eventos Técnicos
- Revisión de Infraestructuras
- Pruebas de Seguridad
- Difusión de Información

OWASP
The Open Web Application Security Project

Review CSIRT-NQN :: Capacitación

lacnic

lacnic warp
Warning Advice and Reporting Point

Taller Amparo

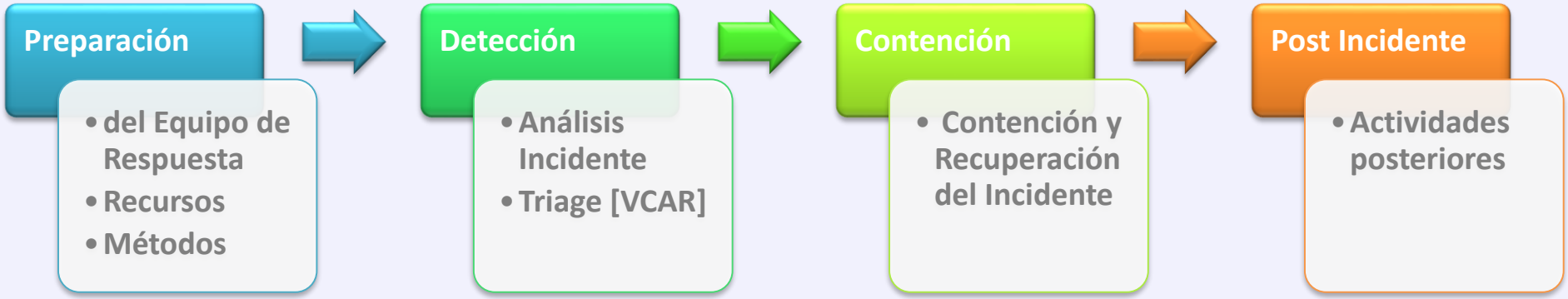
ITU

CYBERDRILL
Ciberseguridad desde
la Patagonia

Seventh Cybersecurity Training
Cyberdrill - Applied Learning for Emergency Response Teams

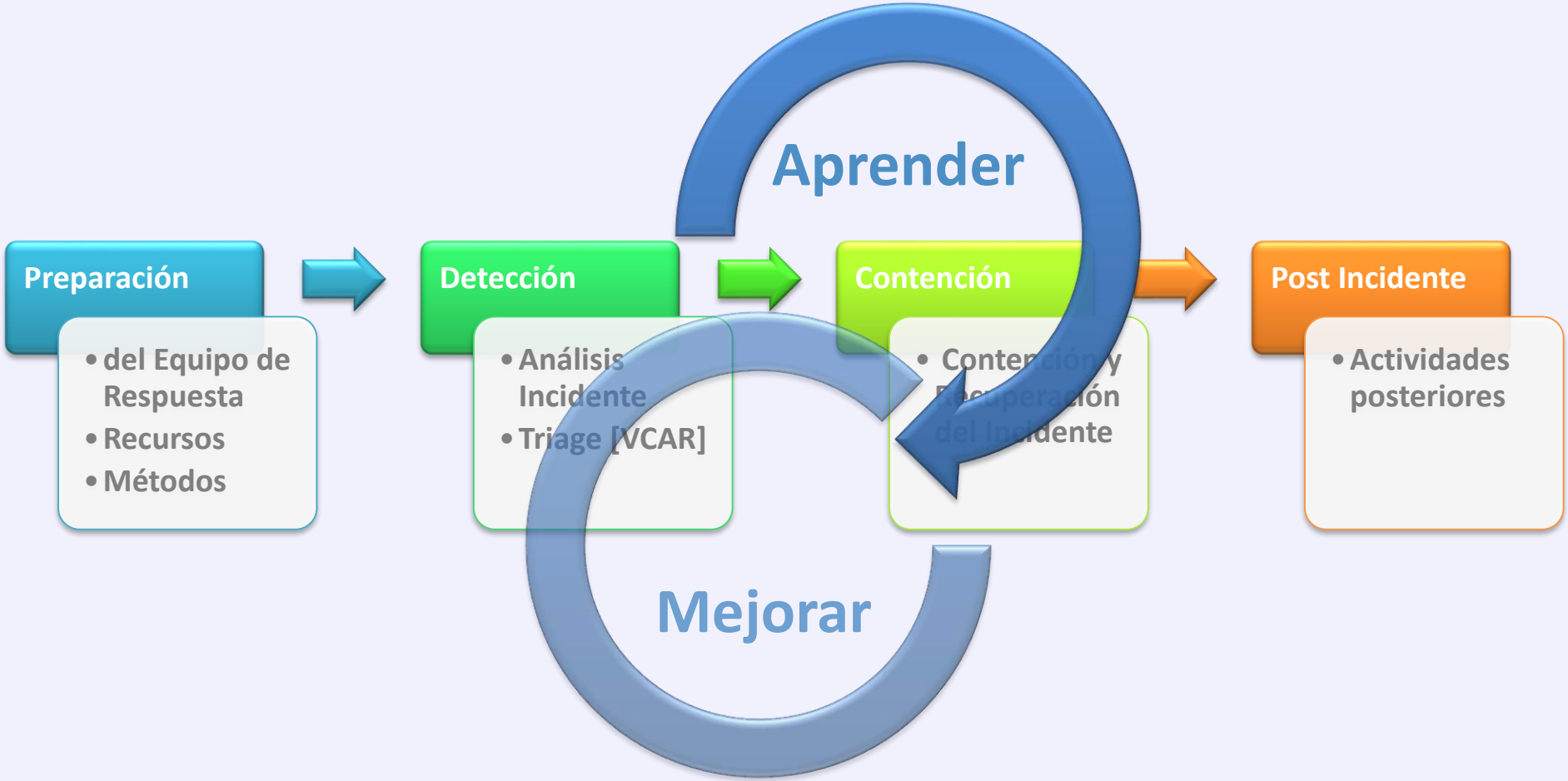
OWASP
The Open Web Application Security Project

Review CSIRT-NQN :: Metodología



OWASP
The Open Web Application Security Project

Review CSIRT-NQN :: Metodología

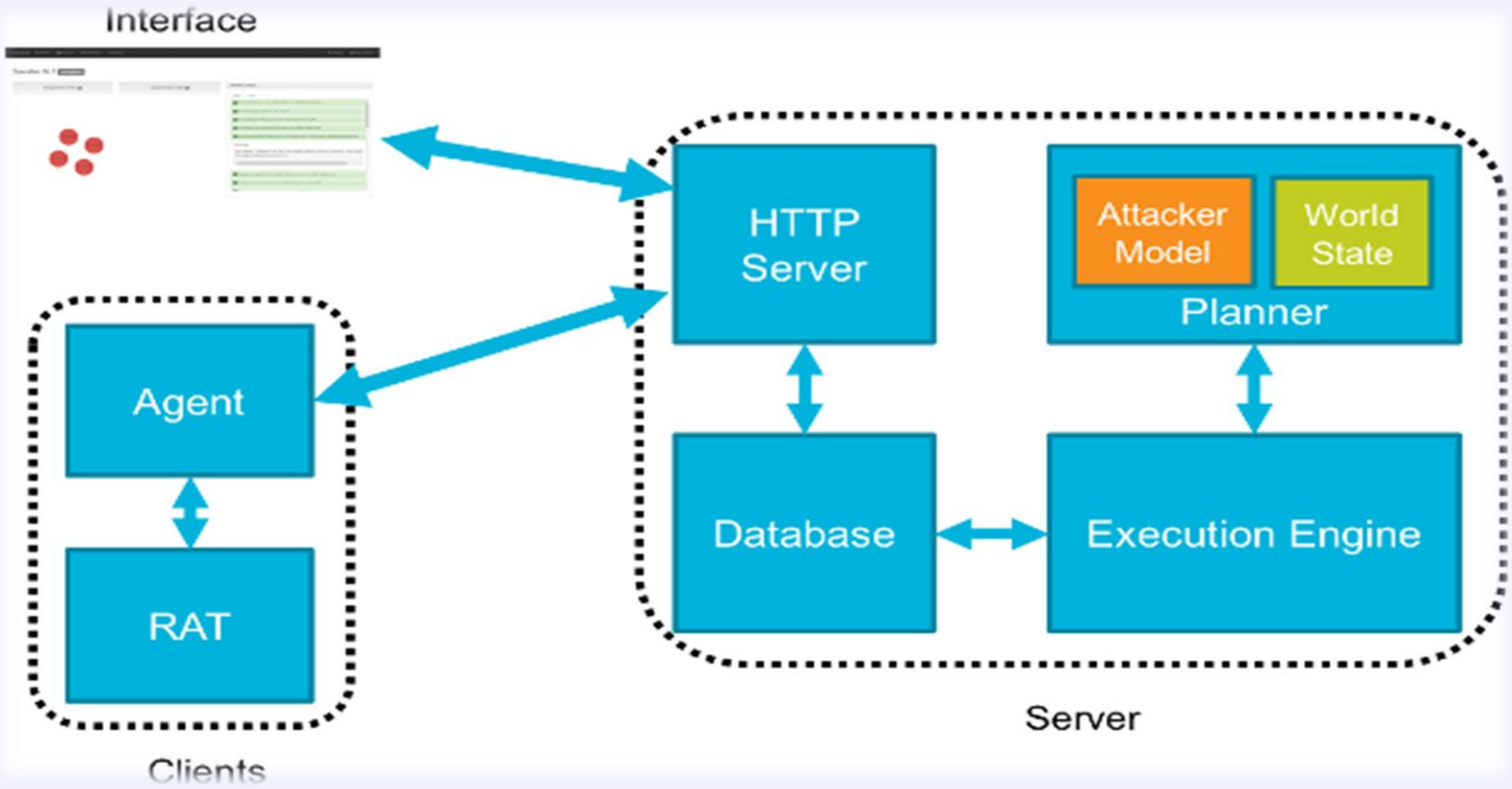


OWASP
The Open Web Application Security Project

Review CSIRT-NQN :: Vinculaciones

OWASP
The Open Web Application Security Project

Home Task: MITRE CALDERA



Fuente: https://www.mitre.org/research/technology-transfer/open-source-software/caldera

OWASP
The Open Web Application Security Project

Talking about CSIRT's…

Espacio para consultas…

OWASP
The Open Web Application Security Project

Talking about CSIRT's…

¡Muchas gracias!

CSIRT-NQN

Seguinos en @CSIRTNQN