Equipos de respuesta a incidentes. Experiencias y retos

Rubén Aquino Luna

Subdirección de Seguridad de la Información UNAM-CERT

Dirección de Telecomunicaciones

Subdirección de Seguridad de la Información
UNAM-CERT

DGTIC

Seguridad de la información / UNAM-CERT

- Equipo de Seguridad en Cómputo
- Área de Seguridad en Cómputo
- Departamento de Seguridad en Cómputo
- UNAM-CERT
- Subdirección de Seguridad de la Información

DGTIC

Seguridad de la información / UNAM-CERT

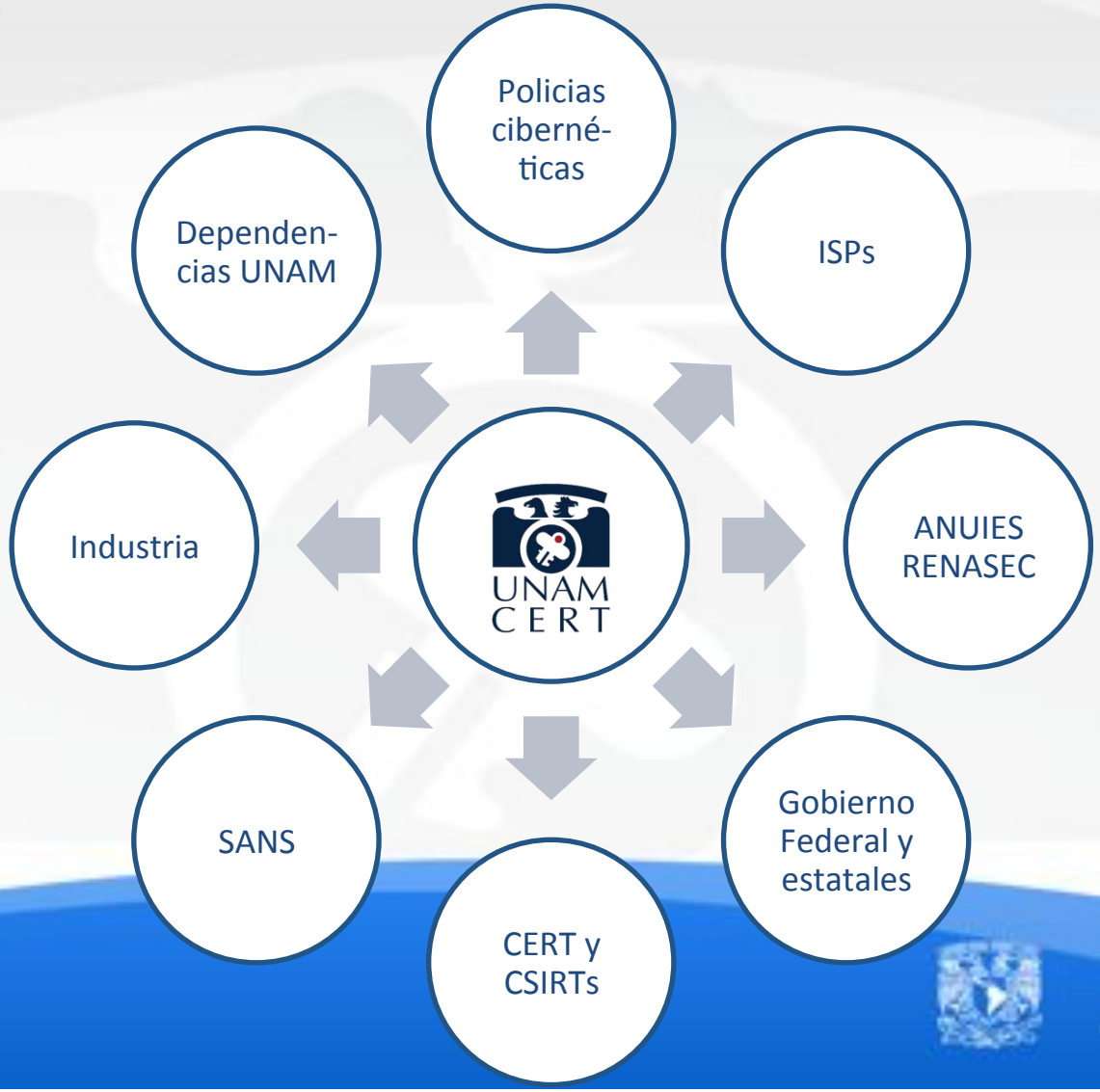
- Casi 20 años desde que se formó el ESC.
- Incremento en impacto en nuestra circunscripción
- Colaboración al interior y exterior
- Mejor entendimiento de la función de un equipo de respuesta.

Seguridad de la información / UNAM-CERT

- Servicios
- Proyectos internos, externos
- Difusión y capacitación
- Colaboración

DGTIC

Colaboración



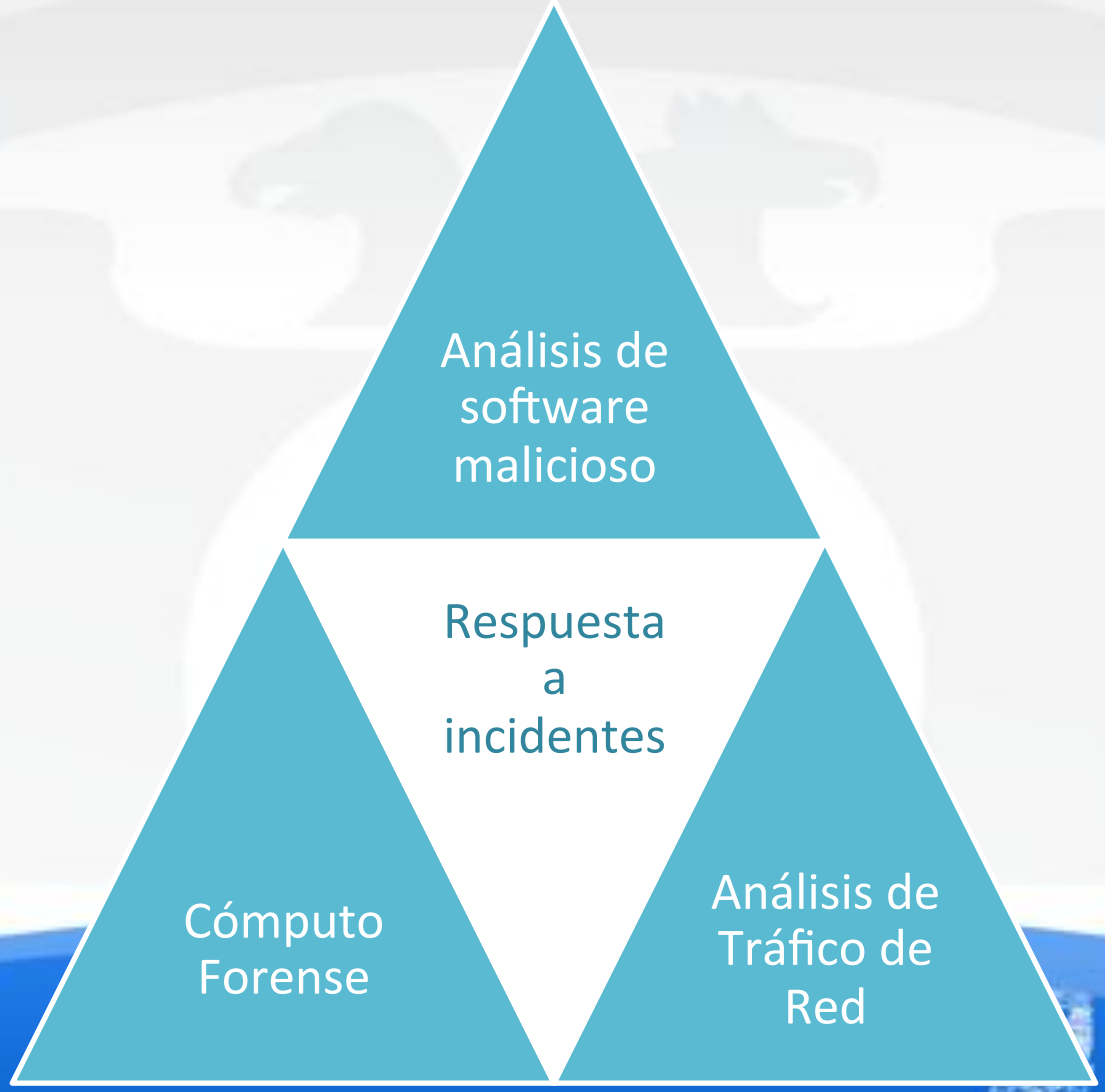
DGTIC

Respuesta a incidentes de seguridad de la información

- Objetivo: Detectar y gestionar los incidentes de seguridad informática en RedUNAM y organizaciones externas

DGTIC

Respuesta a incidentes de seguridad de la información



DGTIC

Evaluación de tecnología

- Evaluar soluciones de seguridad de la información para proporcionar elementos en la toma de decisiones sobre soluciones de seguridad informática como:
  - Antivirus
  - Antispam
  - IPS
  - Firewalls

Revisión/auditorías de seguridad

- Revisar el estado actual de una organización respecto a la seguridad de sus activos de información, acorde a las mejores prácticas internacionales en la materia.

Pentest (Pruebas de penetración)

- Detectar y clasificar vulnerabilidades para minimizar el riesgo de que los activos de información sean afectados por amenazas de seguridad informática. Ingresos económicos para DGTIC.

Asesorías en seguridad de la información

- Apoyar en el diseño e implementación de soluciones de seguridad de la información.

Plan de Becarios de Seguridad

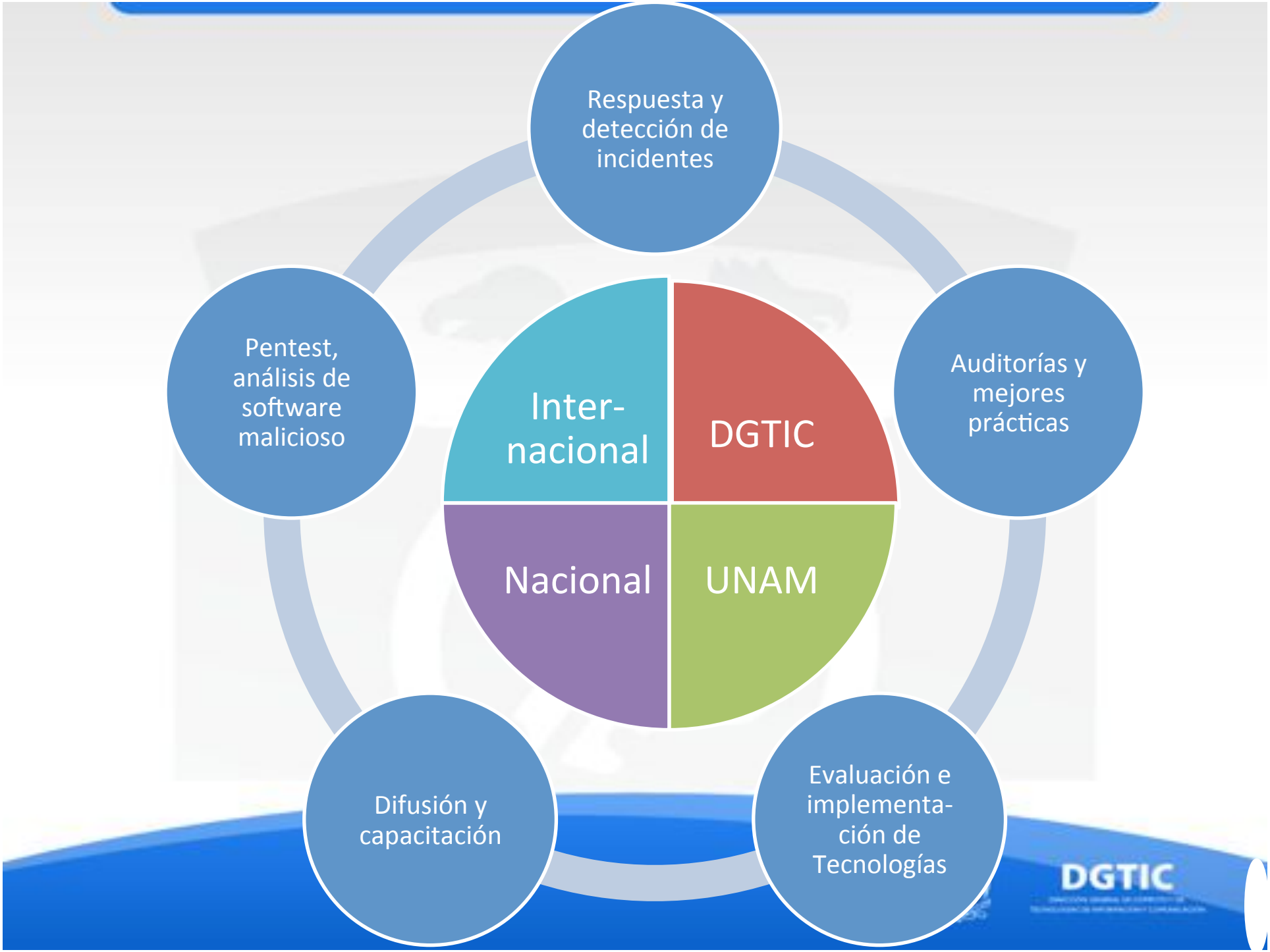
Formar recursos humanos especializados en Seguridad de la Información.

5 Generaciones

60% del personal de la SSI/ UNAM-CERT proviene de un Plan de Becarios

Difusión

DGTIC


Respuesta y detección de incidentes
Auditorías y mejores prácticas
Evaluación e implementa-ción de Tecnologías
Difusión y capacitación
Pentest, análisis de software malicioso
Inter-nacional
DGTIC
Nacional
UNAM
DGTIC

Sistema de Gestión de Seguridad de la Información (SGSI)

- Modelo de trabajo aceptado internacionalmente que reduce los riesgos de seguridad asociados con la operación de TICs.

- Considera las etapas de Establecimiento, Implementación, Operación, Monitoreo, Revisión y Mantenimiento.

Referencias

- www.seguridad.unam.mx
- www.cert.org.mx
- www.malware.unam.mx
- www.honeynet.unam.mx
- revista.seguridad.unam.mx
- tv.seguridad.unam.mx

DGTIC

Retos

- Mas equipos de respuesta
- Colaboración
- Cultura de seguridad de la información
- Sustentabilidad de equipos de respuesta
- Especialistas en seguridad de la información, respuesta a incidentes

DGTIC

Contacto

seguridad@seguridad.unam.mx

incidentes@seguridad.unam.mx

phishing@seguridad.unam.mx

DGTIC