SSP

POLICÍA FEDERAL

Centro Nacional de Respuesta a Incidentes Cibernéticos CERT-MX

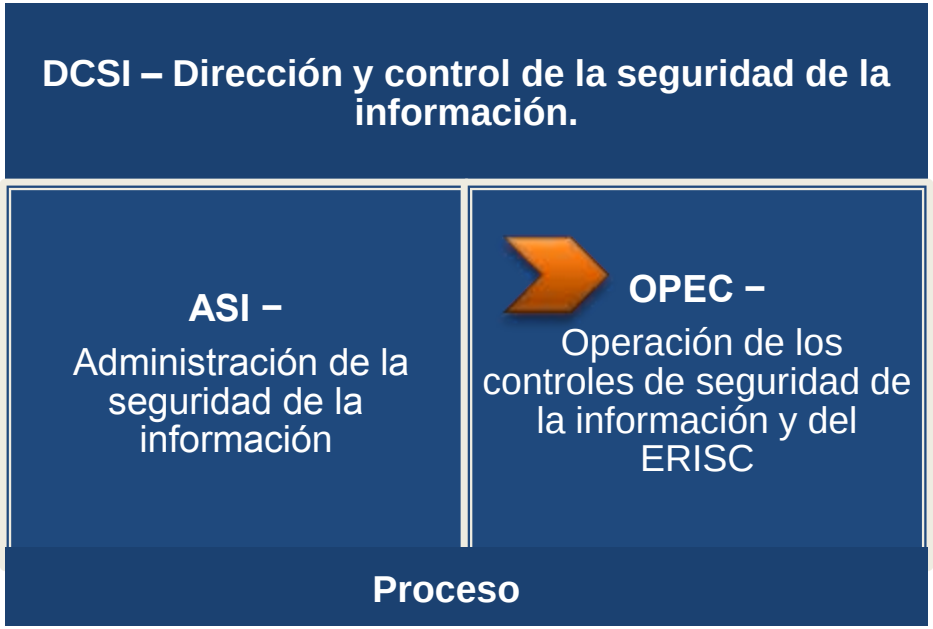
Comisario Eduardo Espina García

División Científica

Coordinación para la Prevención de Delitos Electrónicos

cert-mx@ssp.gob.mx

MAAGTIC SI


DCSI – Dirección y control de la seguridad de la información.
ASI –
Administración de la seguridad de la información
OPEC –
Operación de los controles de seguridad de la información y del ERISC
Proceso

Objetivos del proceso

- Implantar y operar los controles de seguridad de la información.
- Definir y aplicar la planeación para la mitigación de riesgos por incidentes.
- Implantar las mejoras recibidas del proceso ASI-Administración de la seguridad de la información, para el fortalecimiento del SGSI, tanto de sus guías técnicas como de los controles de seguridad de la Información en operación.

OPEC-2

- Elaborar la Guía técnica de atención a incidentes, de acuerdo a la criticidad de los Activos de TIC afectados, considerando al menos los siguientes apartados:
  a) Detección de los Incidentes.
  b) Priorización de los Incidentes.
  c) Investigación técnica de los Incidentes.

OPEC-2

d) Criterios técnicos de contención de los Incidentes, de acuerdo a la criticidad de los Activos de TIC.

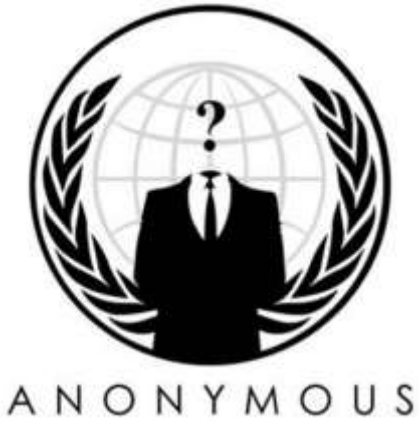
e) Obtención, preservación y destino de los indicios de los Incidentes.

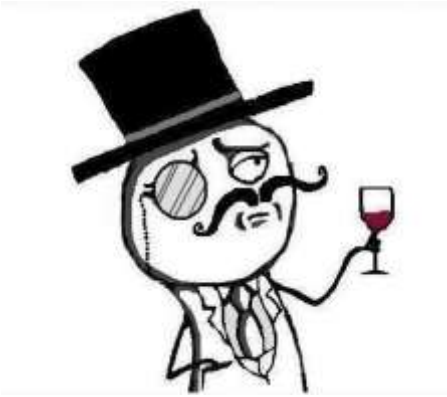
f) Erradicación de los Incidentes.

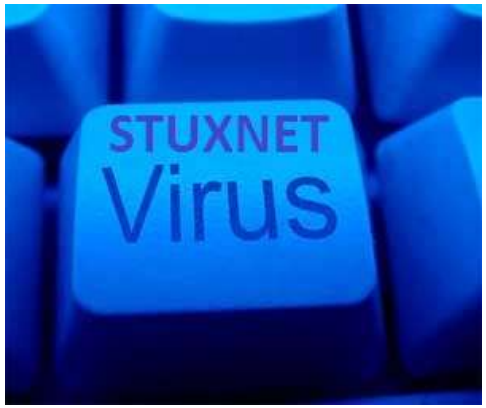
g) Recuperación de la operación.

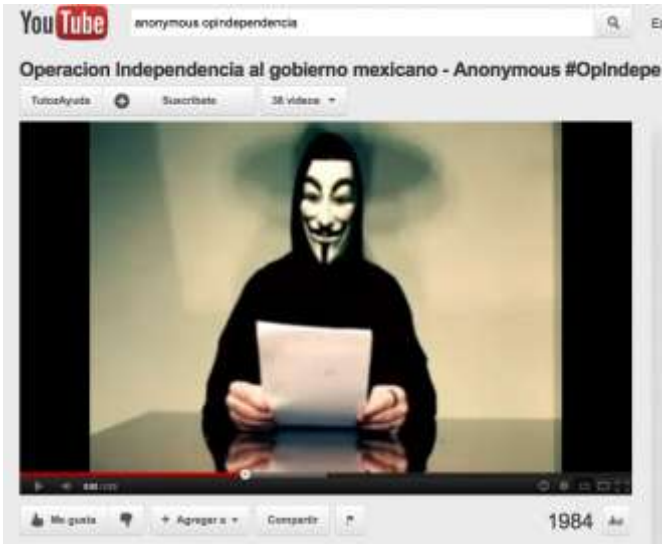
h) Documentación de las lecciones aprendidas.

¿Porqué preocuparse por la seguridad de la información?









¿Qué es el CERT-MX?

- El Centro Nacional de Respuesta a Incidentes Cibernéticos es el organismo acreditado para atender amenazas de ciberseguridad en México.
- Atiende denuncias de ataques a los activos tecnológicos de la infraestructura crítica de México.
- Monitorea la seguridad de la red y los sistemas.
- Coordina la respuesta a incidentes a víctimas de ataques cibernéticos.

Atribuciones - Reglamento de la Ley de la Policía Federal

A partir de la publicación del Reglamento de la Ley de la Policía Federal y de las atribuciones ahí otorgadas, el CERT-MX se establece como "*el organismo encargado de operar el equipo de respuesta a incidentes de seguridad informática en la infraestructura crítica de México, colaborando con los diferentes órdenes de gobierno y actores sociales*."

Misión y Visión

- Proporcionar soporte en la respuesta y defensa en contra de incidentes de seguridad de la información en el dominio .mx e infraestructuras TIC's críticas del país.
- Coadyuvar en los esfuerzos de protección mediante la colaboración e intercambio de información entre instituciones de gobierno estatal y federal, la industria y equipos de respuesta.
- Fortalecer las estrategias de seguridad cibernética de México.

Servicios del CERT-MX

Servicios reactivos, proactivos y de gestión

- Respuesta a incidentes
- Alertas y boletines de seguridad
- Análisis de artefactos
- Análisis forense
- Capacitación y concientización
- Operación 24 x 7, 365 días del año

¿Cómo opera?

Recibe Notificaciones	Realiza Análisis	Disemina y da seguimiento
US-CERT CERT-BR RU-CERT IRIS-CERT UNAM-CERT Shadowserver Honeynet Project Zeus Tracker SpyEye Tracker APWG	¿Es realmente un incidente? ¿Existe relación con eventos anteriores? Normalización Instituciones afectadas Priorización	Identificación de contacto Correo Teléfono Visita en sitio Apertura de incidente Cierre del incidente

¿Cómo fortalece al Estado Mexicano?

- Proporciona respuesta y defensa contra incidentes de seguridad de la información a las instituciones del Estado.
- Facilita la comunicación en los 3 niveles de Gobierno en materia de ciberseguridad.
- Se establece como punto de contacto nacional e internacional para atender las amenazas cibernéticas.
- Previene e investiga ataques perpetrados contra activos tecnológicos críticos del Estado Mexicano.

Atención de incidentes

- Colaboración con los 3 niveles de gobierno
  - SEP, Función Pública
  - PGJDF
  - Gobierno del Estado
    - Jalisco, Guanajuato, Guerrero, Tabasco, Oaxaca
- Instituciones académicas
  - IPN
  - Tecnológico de Monterrey
  - UNAM
- Infraestructura crítica
  - Presidencia de la República
  - SEDENA
  - CFE
  - SAT

CERT-MX – Miembro de FIRST

FIRST
Forum of Incident Response and Security Teams

- El CERT-MX es miembro oficial del FIRST desde Julio del 2011
- FIRST Congrega a los CERTs de más de 50 países
  - Colaboración para la respuesta a incidentes
  - Intercambio de información
    - Tendencias y alertas
    - Actividad maliciosa a nivel mundial
- Incidentes de seguridad informática en México
  - Consolidación del CERT-MX como el punto de contacto a nivel Internacional y Nacional

CERT-MX Colaboración internacional

- Reunión anual de CSIRTs con responsabilidad Nacional
  - Viena, Austria 18-19 de Junio del 2011
  - Participación de los CERTs Nacionales de
    - Estados Unidos
    - China
    - Japón
    - Alemania
    - España
    - Australia
    - Finlandia
    - Polonia
    - Vietnam
    - Malasia
    - Serbia
    - Korea
    - Holanda
    - Bélgica
    - Brasil
    - Uruguay
    - México (CERT-MX)

Respuesta coordinada

ERISC local + CERT MX = Respuesta coordinada

CERT-MX

Contacto

Email: cert-mx@ssp.gob.mx
Reporte phishing: phishing@ssp.gob.mx
Reporte malware: malware@ssp.gob.mx
Tel. 55 11036000 ext. 29147-155