# Equipo de Respuesta a Incidente de Seguridad

*Introducción*

## Agenda

- Equipo de Respuesta a Incidentes de Seguridad
  - ¿Qué es el CSIRT?
  - Proceso de establecimiento del CSIRT
- Estudio de caso:
  - CSIRT UTPL
  - CAIS/RNP
  - PeCERT

## Objetivo de esta sección

- Capacitar los participantes sobre los pasos y requerimientos básicos para implantar un CSIRT efectivo.
- Destacar los puntos clave que deben considerarse en este proceso.
- Ayudar a los participantes a entender los varios modelos organizacionales y el nível de servicios que puede ser provisto por un CSIRT.
- Intercambiar experiencias.
- Aprender con los que ya actúan en el área.



## ¿Qué es un CSIRT?

## Qué es un CSIRT?

- CSIRT = *Computer Security Incident Response Team*, o Equipo de Respuesta a Incidentes de Seguridad.
- CERT = *Computer Emergency Response Team*, o Equipo de Respuesta ante Emergencias.
  - Servicio principal: respuesta a incidentes de seguridad.
  - Punto único de contacto para la notificación de incidentes

## Tipos de CSIRT

- Interno
- Coordinación
- Centros de análisis
- Vendors
- Como Servicio

## Ejemplos de CSIRTs









## Proceso de establecimiento del CSIRT

## Consideraciones iniciales

- Cada CSIRT tiene su propia identidad y son diferentes entre sí
- El proceso debe ser adecuado a cada organización
- No existe un procedimiento universal
- Depende de:
  - Las necesidades y requisitos
  - La misión y objetivos
  - Los recursos disponibles
- Lo que presentaremos es un guía que será adaptado a su institución.

## Importante

- El apoyo y participación de la administración son fundamentales
  - ¡Primera etapa del proceso!
- El CSIRT debe apoyar la misión/objetivos de la organización.
- Utilice un enfoque orientado a proyectos.
- Mantenga la comunicación con las partes interesadas durante todo el proceso
  - Siempre obtenga *feedback*
- Comience pequeño y crezca de a pocos
- Use lo que existe, ¡si fuera apropiado!

# GT CSIRT – LA-3: Checklist

## Checklist para la implementación de un CSIRT

| | |
|---|---|
| **Institución:** | |
| **Fecha:** | |
| **Responsables por la verificación:** | |
| **Tipo del CSIRT:** | |
| **Participantes:** | |

| Fase 1: Sensibilización y análisis de contexto | | | | | |
|---|---|---|---|---|---|
| **Código** | **Pregunta** | **Si** | **No** | **No es aplicable** | **Comentarios** |
| **1** | **Sensibilización de las partes interesadas** | | | | |
| 1.1 | Definición de los objetivos del CSIRT | | | | |
| 1.2 | Identificación de las partes interesadas y participantes | | | | |
| 1.3 | Alineamiento con la direción y obtención del apoyo para implementar el CSIRT | | | | |
| 1.4 | Análisis FODA | | | | |
| **Fase 2: Planeamiento** | | | | | |
| **Código** | **Pregunta** | **Si** | **No** | **No es aplicable** | **Comentarios** |
| **2** | **Definiciones básicas** | | | | |
| 2.1 | Misión y visión | | | | |
| 2.2 | Nombre | | | | |
| 2.3 | Clientes atendidos | | | | |
| 2.4 | Servicios para cada cliente atendido | | | | |
| 2.5 | Modelo de ingresos para financiar los servicios | | | | |
| **3** | **Aspectos organizacionales** | | | | |
| 3.1 | Modelo organizacional del CSIRT | | | | |
| 3.2 | Autoridad del CSIRT | | | | |
| 3.3 | Estrucutura organizacional | | | | |
| **4** | **Personal** | | | | |

# Etapas

Fase 1: Sensibilización y análisis de contexto

Fase 2: Planeamiento

Fase 3: Implementación

Fase 4: Operación

Fase 5: Mejora continua

Fase 6: Establecimiento de alianzas

## Sensibilización y análisis de contexto

*Fase 1*

## Sensibilización y análisis de contexto

- Definición de los objetivos del CSIRT
- Identificación de las partes interesadas y participantes
- Alineamiento con la gerencia y obtención del apoyo
- Análisis FODA
  - F = Fuerzas
  - O = Oportunidades
  - D = Debilidades
  - A = Amenazas

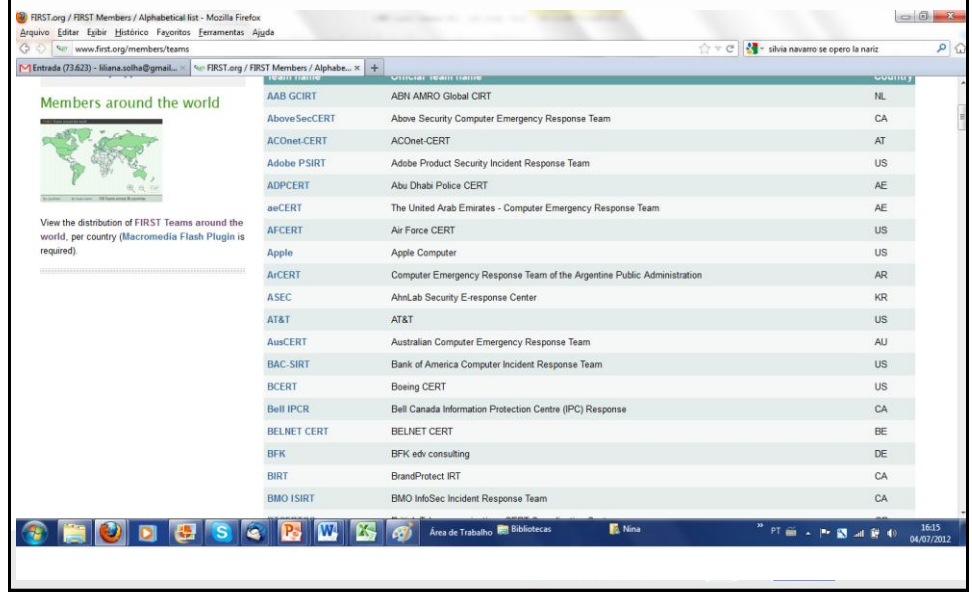
## Brainstorming

- ¿Cómo el CSIRT puede ayudar en el quehacer de la organización?
- ¿Por qué implementar un CSIRT?
- ¿Qué debe cambiar en la organización para que éste sea implementado?
- ¿Qué personas deben estar involucradas?
- ¿Cuáles son las instituciones/personas/áreas interesadas?
- ¿Cómo obtener el apoyo de la gerencia?
- ¿Cuáles son las necesidades de los interesados?
- ¿Cuáles son los activos críticos que deben ser protegidos?

## Aprendiendo con los demás

- Navegue en los sites de otros CSIRTs
- Converse con otros CSIRTS
  - Visitas
  - Participación en eventos: FIRST, COLARIS
- Lea la documentación existente:
  - CERT/CC
  - ENISA
  - AMPARO

# Aprendiendo con los demás




## Planificación

*Fase 2*

## Planificación

- Objetivo:
  - Definiciones básicas (factores claves)
  - Aspectos organizacionales
  - Personal
  - Infraestructura
  - Evaluación del CSIRT
  - Planificaciones

**¡La participación de la administración es fundamental!**

## Planificación

- Objetivo:
  - **Definiciones básicas (factores claves)**
  - Aspectos organizacionales
  - Personal
  - Infraestructura
  - Evaluación del CSIRT
  - Planificaciones

**En su opinión, ¿Cuáles serían los factores claves?**

## Factores claves

- Nombre
  - Uso común de siglas
- *Constituency*
  - ¿Quiénes son los clientes?
- Misión
  - ¿Qué hace el CSIRT? ¿Cuál es su objetivo?
- Servicios
  - ¿Cómo cumplir con lo establecido en la misión? ¿Qué se le ofrece a los clientes? ¿Qué tipo de incidentes son tratados?

## Factores claves

- Financiamiento de las operaciones
  - Inscripción
  - Servicios pagados
  - Financiado por el gobierno
  - Financiado por la misma institución
  - Consorcio
- Localización
- Tipo de CSIRTs
- ¿Centralizado o distribuído?

## Costos de un CSIRT

- Algunos elementos que deben ser considerados:
  - Herramientas
  - Equipo
  - Teléfono, celular, etc.
  - Certificado Digital
  - Alquiler de sala
  - Mecanismos de seguridad física

## Ejemplos de misión

- CAIS/RNP (CSIRT de Coordinación):
  - *"O CAIS – Centro de Atendimento a Incidentes de Segurança atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes".*
- CERTuy (CSIRT de Gobierno):
  - *"Proteger los activos de información críticos del Estado y promover el conocimiento en seguridad de la información de manera de prevenir y responder a incidentes de seguridad."*

## Servicios de un CSIRT

**Post-response type service**

- Alerts and warnings
- Incident handling
  - Incident analysis
  - On-site incident response
  - Incident response support
  - Incident response study
- Vulnerability handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response study
- Artifact handling
  - Artifact analysis
  - Artifact response
  - Artifact response study

**Pre-response type service**

- Announce
- Technology trend survey
- Security survey or screening
- Setting up / maintenance of security tools, applications, infrastructures, and services
- Security tool development
- Intrusion detection service
- Provisioning of security-related information

**Security quality service**

- Risk analysis
- Business continuity and disaster recovery plan
- Security audit or screening
- Security consulting
- Awareness enhancement
- Education/training
- Product evaluation or certification

Fuente: CERT/CC

## Servicios de un CSIRT

- Para cada servicio, hay que definir:
  - Modo de operación
  - Horario de atención
  - Políticas y procedimientos
    - SANS Security Policy Project
    - ISO/IEC 27002
  - Nivel de servicio

## Práctica

- Ejercicio 1


## Planificación

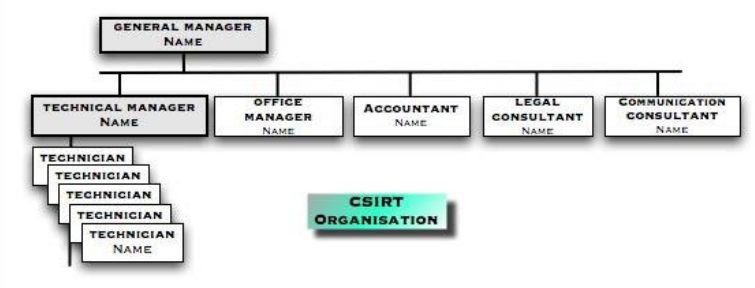
- Objetivo:
  - Definiciones básicas (factores claves)
  - **Aspectos organizacionales**
  - Personal
  - Infraestructura
  - Evaluación del CSIRT
  - Planificaciones

## Aspectos organizacionales

- ¿Dónde está ubicado el CSIRT dentro de la organización?
- ¿A quién le reporta el CSIRT?
- ¿Cómo interactuará el CSIRT con las demás áreas tecnológicas de la organización? ¿Y con el área jurídica?
- Modelo organizacional: ¿Cómo el CSIRT operará?
- ¿Cómo es la autoridad del CSIRT?
  - Completa
  - Compartida
  - Sin autoridad

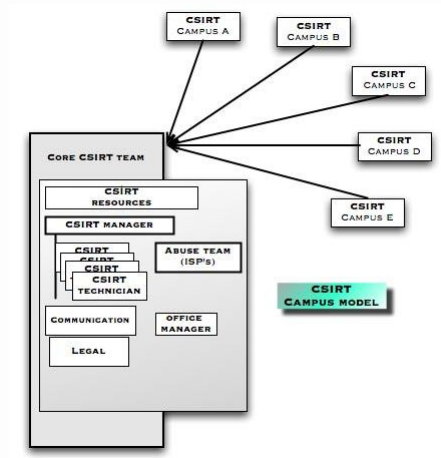
## Modelos

Fuente: ENISA



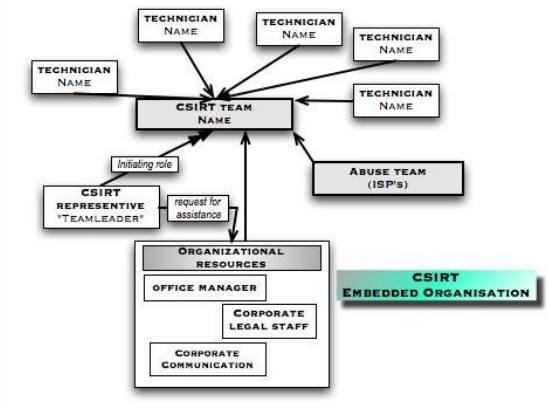
## Modelos

Fuente: ENISA




## Modelos

Fuente: ENISA



## Modelos

Fuente: ENISA


## Práctica

- Ejercicios 2 y 3

## Planificación

- Objetivo:
  - Definiciones básicas (factores claves)
  - Aspectos organizacionales
  - **Personal**
  - Infraestructura
  - Evaluación del CSIRT
  - Planificaciones

## Equipo

- Funciones y responsabilidades del CSIRT
- Perfiles requeridos y conocimientos necesarios
  - Comunicación, técnico, respuesta a incidentes, etc.
- Estrategia para la conformación del equipo
  - ¿Ya existen esos perfiles en la organización? ¿O será necesario contratar? O el equipo será capacitado?
- ¿Cuántas personas debe tener el CSIRT?
  - Depende de factores como: servicios, cantidad de clientes atendidos, SLA, etc.

## Papeles en un CSIRT

- Gerente
- Analista de Hotline/Helpdesk
- Incident Handlers
- Vulnerability Handlers
- Analista de malware
- Especialista en plataformas
- Escritor técnico
- Otros

**Cuidado** con los papeles críticos sin backup!

## Práctica

- Ejercicio 4

## Planificación

- Objetivo:
  - Definiciones básicas (factores claves)
  - Aspectos organizacionales
  - Personal
  - **Infraestructura**
  - Evaluación del CSIRT
  - Planificaciones

## Infraestructura

- Incluye:
  - Ubicación de los servidores
  - Salas de trabajo
  - Notebooks y estaciones de trabajo
  - Servidores
  - Red
  - Sistemas
  - Herramientas de trabajo
  - Banco de datos
  - Celular, tablets, teléfonos, etc.

## Herramientas

- Hardware y software
  - Servidores
  - Equipos de rede
  - Estaciones de trabajo
- Definición de cómo la infraestructura del CSIRT será protegida y monitoreada
- ¡Evalúe todas las herramientas antes de utilizarlas!

## Herramientas

- Software de encriptación de mensajes
- Herramientas de tratamiento de incidentes
- Búsqueda de información de contacto
- Copias de seguridad
- Sistema de seguimiento de incidentes
- Correo electrónico seguro
- Sistemas de Comunicaciones Seguras (SSH, SSL, VPN)
- Software antivirus
- CRM

## Práctica

- Ejercicio 5


## Planificación

- Objetivo:
  - Definiciones básicas (factores claves)
  - Aspectos organizacionales
  - Personal
  - Infraestructura
  - **Evaluación del CSIRT**
  - Planificaciones

## Evaluación del CSIRT

- Definir los indicadores y los criterios de medición
- Definir los parámetros de control de calidad
- Definir los métodos para obtener feedback de los clientes
- Definición de las estadísticas

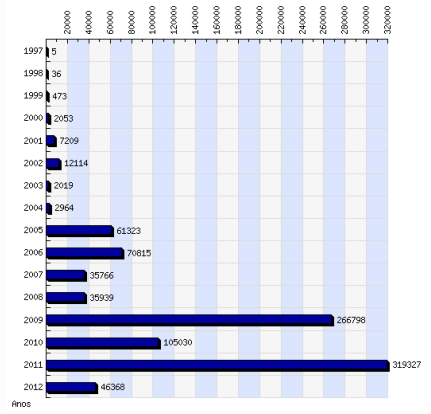
## Ejemplo de indicadores

- Porcentaje de incidentes cerrados dentro de las primeras 24 horas después de notificados
  - Meta: 80%
  - Forma de medición: (Incidentes cerrados en el plazo/Total de incidentes)*100
- Porcentaje de incidentes abiertos sin designación por más de 8 horas
  - Meta: 0
  - Forma de medición: lectura en el sistema de gestión de incidentes

¿Más Ejemplos?

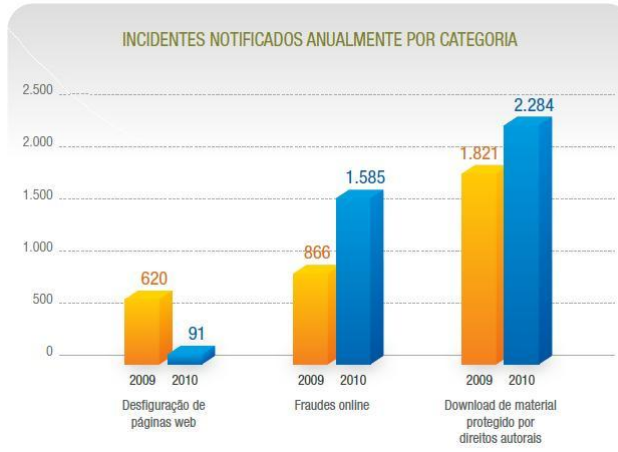
# Ejemplos de estadísticas

Fuente: CAIS, Mayo 2012




# Ejemplos de estadísticas

Fuente: CAIS, 2010



## Ejemplos de estadísticas

- Cantidad de incidentes por año, mes y día
- Cantidad de incidentes por institución
- Cantidad de incidentes por tipo

¿Qué tipo de estadística es interesante externamente?

## Planificación

- Objetivo:
  - Definiciones básicas (factores claves)
  - Aspectos organizacionales
  - Personal
  - Infraestructura
  - Evaluación del CSIRT
  - **Planificaciones**

## Planificaciones

Momento de planificar la implementación del CSIRT y obtener los recursos necesarios para este fin.

¡Utilice un enfoque orientado a proyectos!

## Implementación
*Fase 3*

## Implementación

- Objetivo: implementar acciones relacionadas con:
  - Personal
  - Documentos
  - Infraestructura
  - Comunicación con el CSIRT

## Implementación

- Objetivo: implementar acciones relacionadas con:
  - **Personal**
  - Documentos
  - Infraestructura
  - Comunicación con el CSIRT

## Personal

- Contratación del equipo
- Desarrollo del plan de capacitación
  - CERT/CC
  - SANS
  - ESR/RNP
  - ISO/IEC 27001 e ISO/IEC 27004
  - ¿Otros?

## Práctica

- Ejercicio 6

## Implementación

- Objetivo: implementar acciones relacionadas con:
  - Personal
  - **Documentos**
  - Infraestructura
  - Comunicación con el CSIRT

## Documentos

- Política de seguridad de la información
- Política de gestión de incidentes de seguridad
  - Clasificación de los incidentes
  - Priorización
  - Nivel de apoyo
- Formatos para el envío de los incidentes
- Non Disclosure Agreement (NDA)
- Service Level Agreement (SLA)

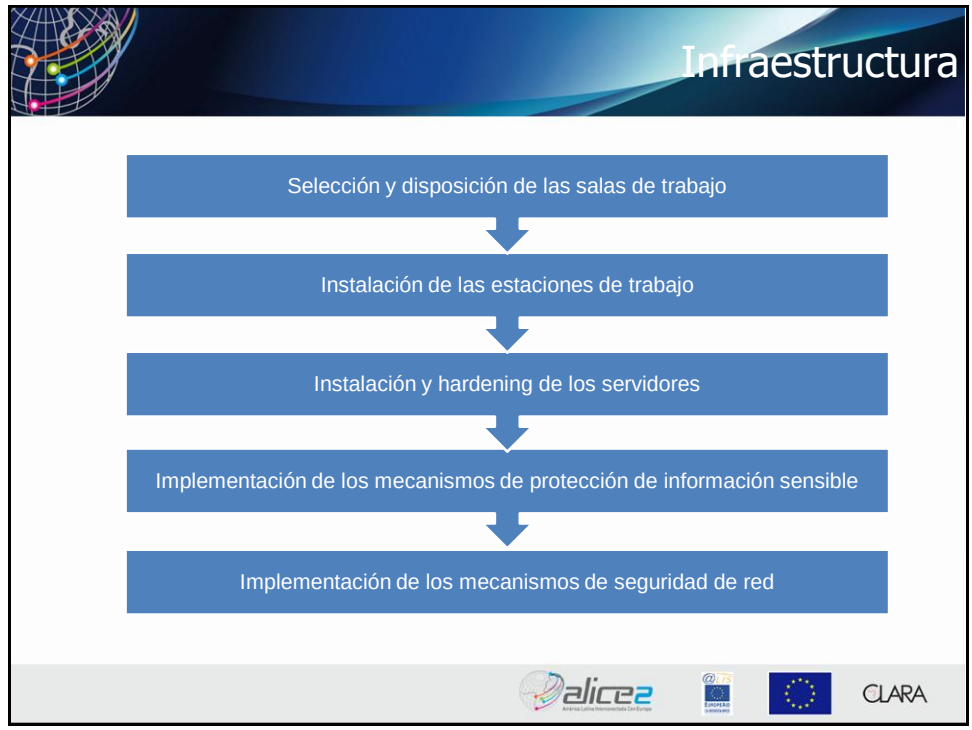
## Documentos

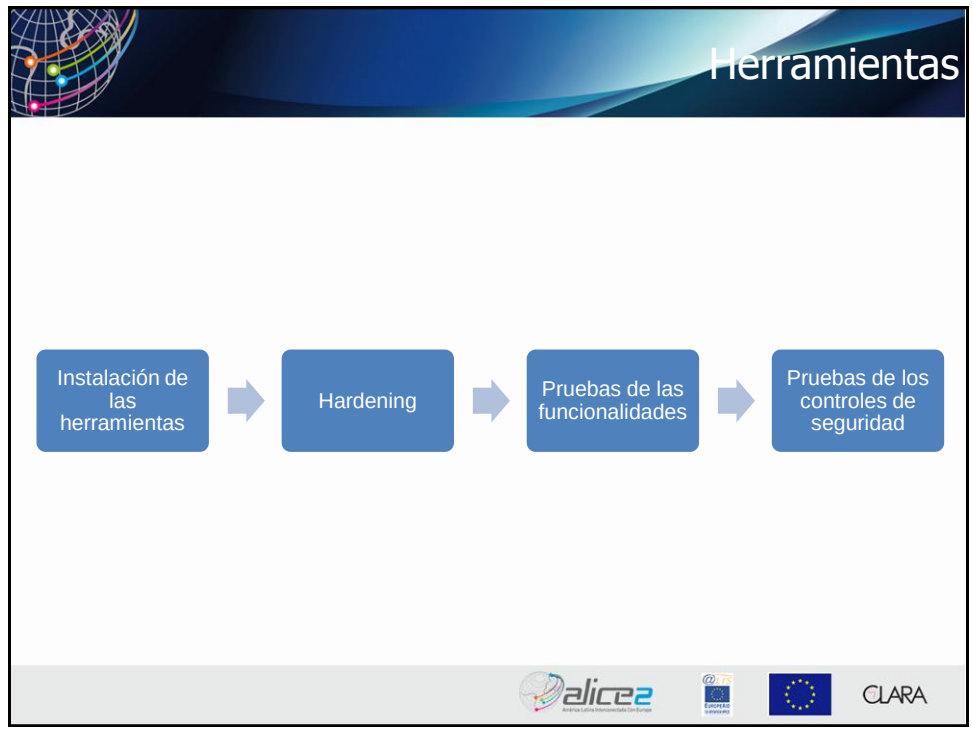
- Plan de continuidad para los servicios críticos
- Procedimientos para ejecución de cada servicio definido
- Procedimientos para la gestión de incidentes
- Procedimientos de reporte de incidentes

¡Esta lista es una sugerencia! Puede que otros documentos sean necesarios.

## Implementación

- Objetivo: implementar acciones relacionadas con:
  - Personal
  - Documentos
  - **Infraestructura**
  - Comunicación con el CSIRT


Infraestructura
Selección y disposición de las salas de trabajo
Instalación de las estaciones de trabajo
Instalación y hardening de los servidores
Implementación de los mecanismos de protección de información sensible
Implementación de los mecanismos de seguridad de red
CLARA


Herramientas
Instalación de las herramientas
Hardening
Pruebas de las funcionalidades
Pruebas de los controles de seguridad
CLARA

## Implementación

- Objetivo: implementar acciones relacionadas con:
  - Personal
  - Documentos
  - Infraestructura
  - **Comunicación con el CSIRT**

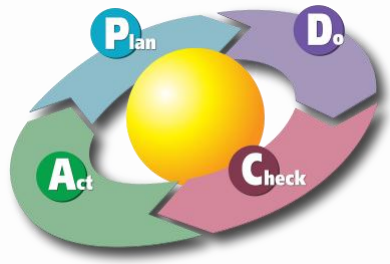
## Comunicación con el CSIRT

- Web-site público
  - /security
- Creación de cuentas y alias para el e-mail del CSIRT
  - abuse@, security@, phishing@
- Creación de las llaves PGP del grupo y de los empleados
- Inclusión del e-mail del grupo en las informaciones del Whois
- Divulgación de las informaciones de contacto a su comunidad

## Comunicación con el CSIRT

nic-hdl-br: SIC128
person: Security Incidents Response Center
e-mail: cais@cais.rnp.br
created: 20020417
changed: 20050309

## ¿Y ahora?



## Lecturas recomendadas

- "Gestión de Incidentes de Seguridad Informática" (AMPARO)
- "A step-by-step approach on how to set up a CSIRT" (ENISA)
- "A basic collection of good practices for running a CSIRT" (ENISA)
- "Creating a Computer Security Incident Response Team: A process for getting started" (CERT/CC)
- "Incident Management Capability Metrics" (CERT/CC)
- "Code of practice for information security management" (ISO 27002)

## Conociendo algunos CSIRTs:

*CSIRT UTPL, CAIS/RNP, y PeCERT*