



GT-CSIRT: Grupo de Trabajo de RedCLARA CSIRT

Tratamiento de Incidentes de Seguridad: Una visión práctica

Apoyo: Centro de Atendimento a Incidentes de Segurança (CAIS/RNP)

Carla Freitas
Frederico Costa
Rildo Souza
Liliana Solha

16a Reunión Técnica de RedCLARA
04-06 de Julio, 2012
Lima, Perú




CLARA

This project is funded by the European Union A project implemented by CLARA



Derechos de autor© 2009 CAIS/RNP - Centro de Atención a los Incidentes de Seguridad de la Red Nacional de Enseñanza e Investigación de Brasil – RNP. Todos los derechos reservados.

La reproducción total o parcial de este material está totalmente prohibida, así como su uso para cualquier propósito, comercial u otro.





CLARA



Equipo de Respuesta a Incidente de Seguridad

Introducción



The slide features a decorative header with a globe and blue gradient. The main content is centered, displaying the title and subtitle. The footer contains logos for alice2, European Union, and CLARA.



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



The slide features a decorative header with a globe and blue gradient. The main content is a bulleted agenda. The footer contains logos for alice2, European Union, and CLARA.



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 nivel 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

The slide displays a collection of logos for various Computer Security Incident Response Teams (CSIRTs). The logos include: GSI-PR (Centro de Segurança da Informação e Comunicação); CertMX México (Centro de Investigación en Seguridad de la Información); CLCERT (Centro de Logos de Certificación); CAIS (Centro de Análisis de Incidentes de Seguridad); CSIRT-UTPL (Centro de Seguridad de la Información de la Universidad Tecnológica del Perú); CERT (CERT's Secure Coding Video Series); ebay; TEAM CYMRU (Cyprus); alice2 (Alianza Latinoamericana de Expertos); CLARA (Centro de Logos de Análisis de Respuesta a Incidentes de Seguridad).

Proceso de establecimiento del CSIRT

The slide displays logos for alice2 and CLARA, which are part of the process of establishing a 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, isi 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 dirección 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	Estructura 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



The slide features a decorative header with a globe and a blue gradient. The main content is the title "Sensibilización y análisis de contexto" in a bold blue font, followed by "Fase 1" in a smaller, italicized blue font. The footer contains logos for "alice2" (with the tagline "Análisis Lógico Inconveniente Con Europa"), "CSIRT", the European Union flag, and "CLARA".



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



The slide features a decorative header with a globe and a blue gradient. The main content is the title "Sensibilización y análisis de contexto" in a bold white font. Below the title is a bulleted list of four main items, with the last item having a sub-list. The footer contains logos for "alice2" (with the tagline "Análisis Lógico Inconveniente Con Europa"), "CSIRT", the European Union flag, and "CLARA".

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

The screenshot shows the 'FIRST.org / FIRST Members / Alphabetical list' page. On the left, there is a section titled 'Members around the world' with a world map and the text: 'View the distribution of FIRST Teams around the world, per country (Macromedia Flash Plugin is required)'. The main content is a table listing various CERT teams and their countries.

Team Name	Country
AAB GCIRT	NL
ABN AMRO Global CERT	NL
AboveSecCERT	CA
ACOnet-CERT	AT
Adobe PSIRT	US
ADPCERT	AE
aeCERT	AE
AFCERT	US
Apple	US
AiCERT	AR
ASEC	KR
AT&T	US
AusCERT	AU
BAC-SIRT	US
BCERT	US
Bell IPCR	CA
BELNET CERT	BE
BFK	DE
BIRT	CA
BMO ISIRT	CA

Planificación *Fase 2*

The slide features a blue header with a globe icon and the title 'Planificación Fase 2'. At the bottom, there are four logos: 'alice2' (Alianza Latinoamericana de Centros de Emergencias de Internet), 'IPTS' (Internet Public Trust Services), the European Union flag, and 'CLARA' (Coordinated Liaison and Assistance Response Agency).



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 distribuido?






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	Pre-response type service	Security quality service
<ul style="list-style-type: none"> • Alerts and warnings • Incident handling <ul style="list-style-type: none"> - Incident analysis - On-site incident response - Incident response support - Incident response study • Vulnerability handling <ul style="list-style-type: none"> - Vulnerability analysis - Vulnerability response - Vulnerability response study • Artifact handling <ul style="list-style-type: none"> - Artifact analysis - Artifact response - Artifact response study 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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



alice2   CLARA

Planificación

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

alice2   CLARA

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

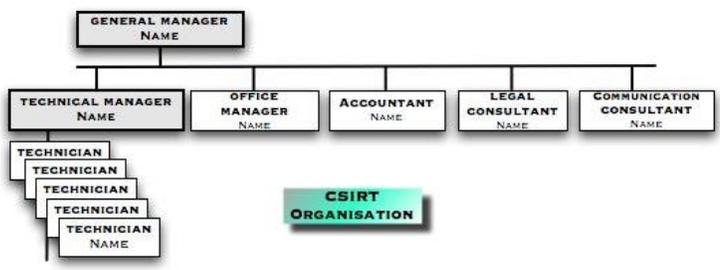





CLARA

Modelos

Fuente: ENISA

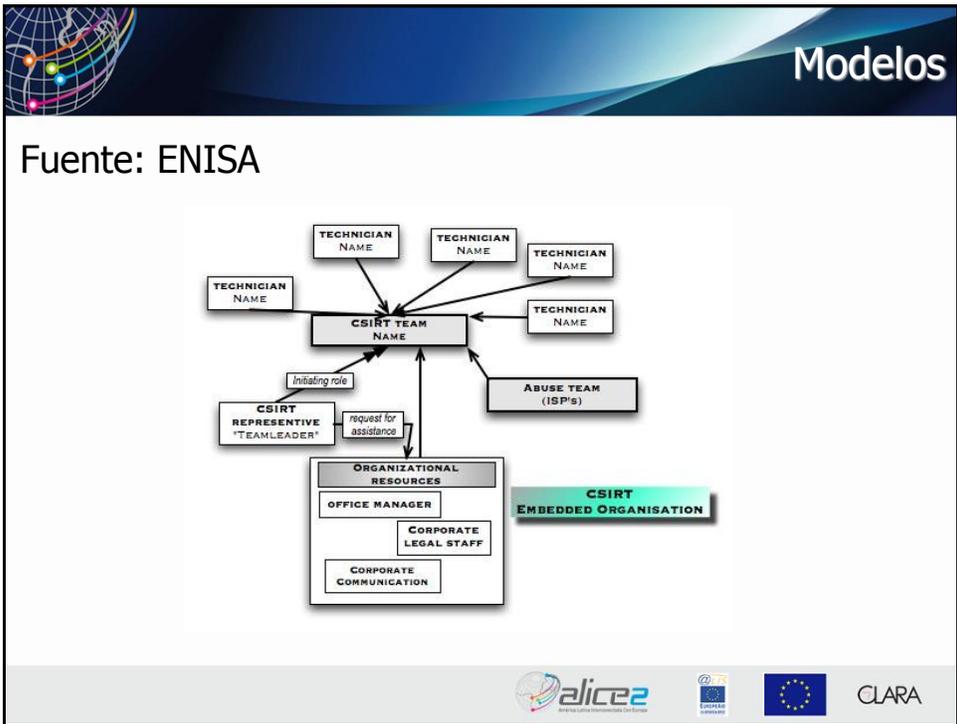
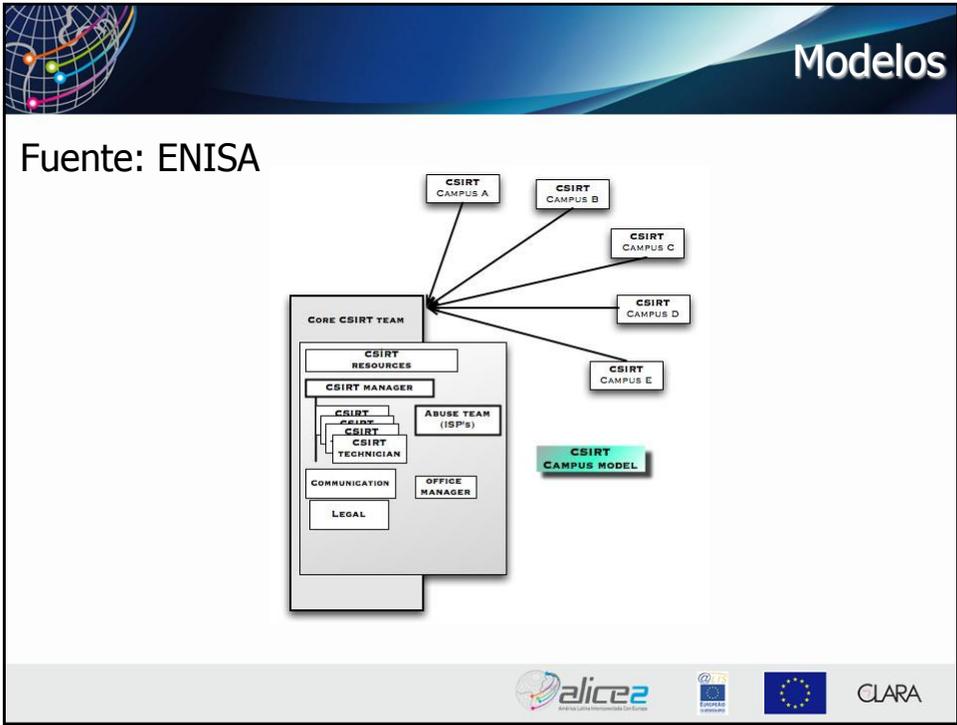


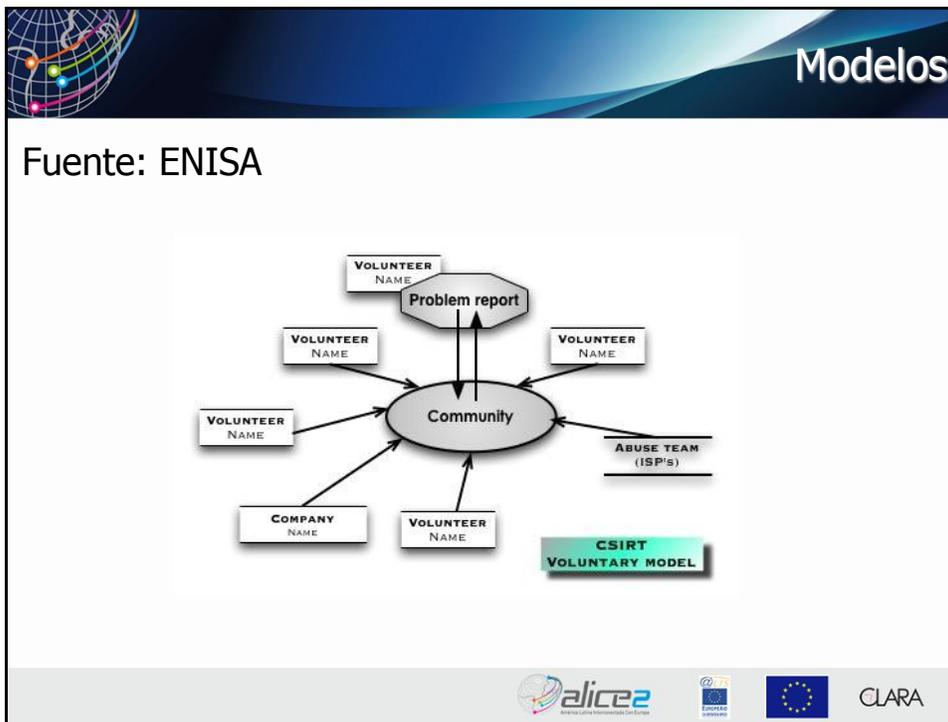
```

graph TD
    GM[GENERAL MANAGER NAME] --- TM[TECHNICAL MANAGER NAME]
    GM --- OM[OFFICE MANAGER NAME]
    GM --- AC[ACCOUNTANT NAME]
    GM --- LC[LEGAL CONSULTANT NAME]
    GM --- CC[COMMUNICATION CONSULTANT NAME]
    TM --- T1[TECHNICIAN]
    TM --- T2[TECHNICIAN]
    TM --- T3[TECHNICIAN]
    TM --- T4[TECHNICIAN]
    subgraph CSIRT_ORG [CSIRT ORGANISATION]
    end
  
```




CLARA





Práctica

- Ejercicios 2 y 3

A circular timer icon with a blue and red face. The text "20min" is displayed in the center of the clock face.

alice2
Alianza Latinoamericana de Centros de Respuesta a Incidentes de Seguridad Informática

@IPS
European Incident Response

CLARA



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 red
 - 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



alice2   CLARA

Planificación

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

alice2   CLARA



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







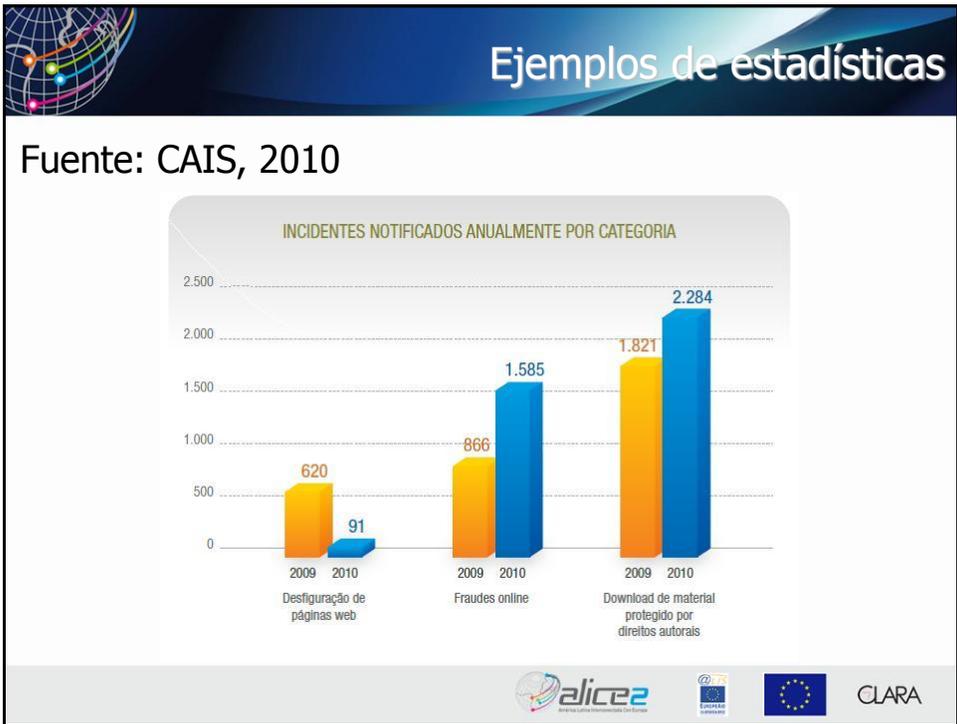
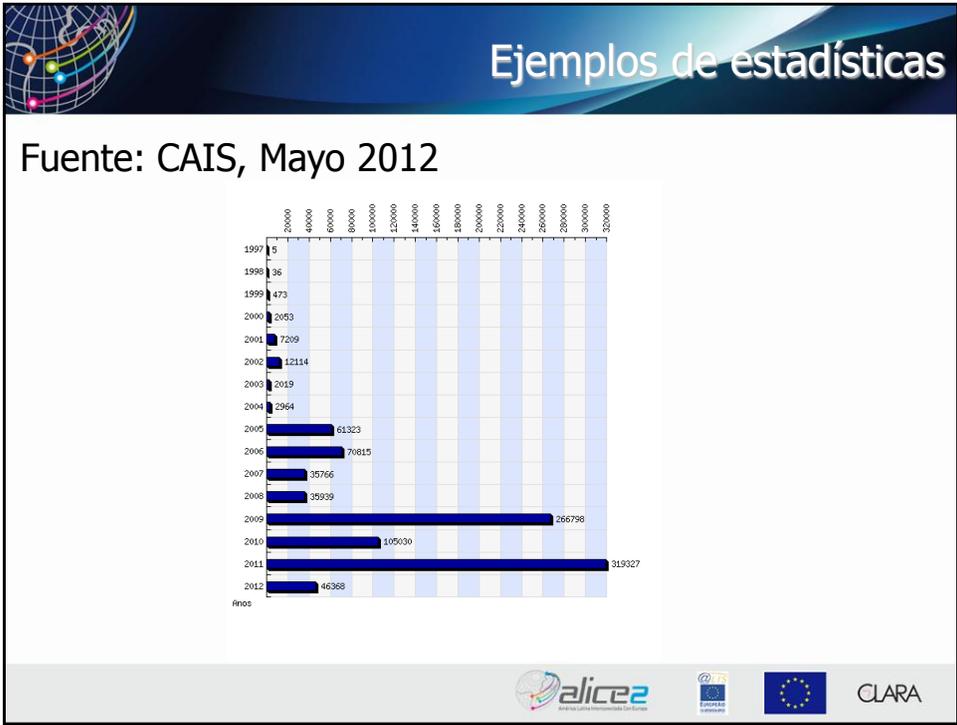
Ejemplo de indicadores

- Porcentaje de incidentes cerrados dentro de las primeras 24 horas después de notificados
 - Meta: 80%
 - Forma de medición: $(\text{Incidentes cerrados en el plazo} / \text{Total de incidentes}) * 100$
- 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

- 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?



The slide features a blue header with a globe icon on the left and the title 'Ejemplos de estadísticas'. Below the title is a bulleted list of three statistics. A central orange rounded rectangle contains a question. The footer contains four logos: 'alice2', '@ITS', the European Union flag, and 'CLARA'.

Planificación

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



The slide features a blue header with a globe icon on the left and the title 'Planificación'. Below the title is a bulleted list with a sub-list under 'Objetivo:'. The last item in the sub-list, 'Planificaciones', is highlighted in orange. The footer contains four logos: 'alice2', '@ITS', the European Union flag, and 'CLARA'.



Planificaciones

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

¡Utilice un enfoque orientado a proyectos!



CLARA



Implementación

Fase 3



CLARA



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?



CLARA

Práctica

- Ejercicio 6



CLARA



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

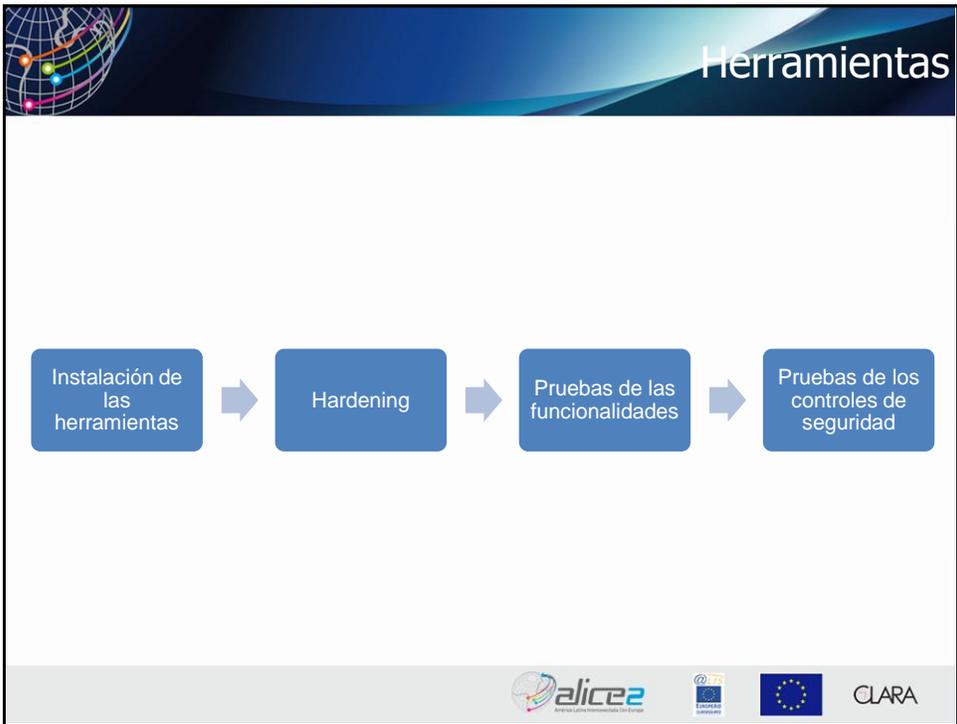
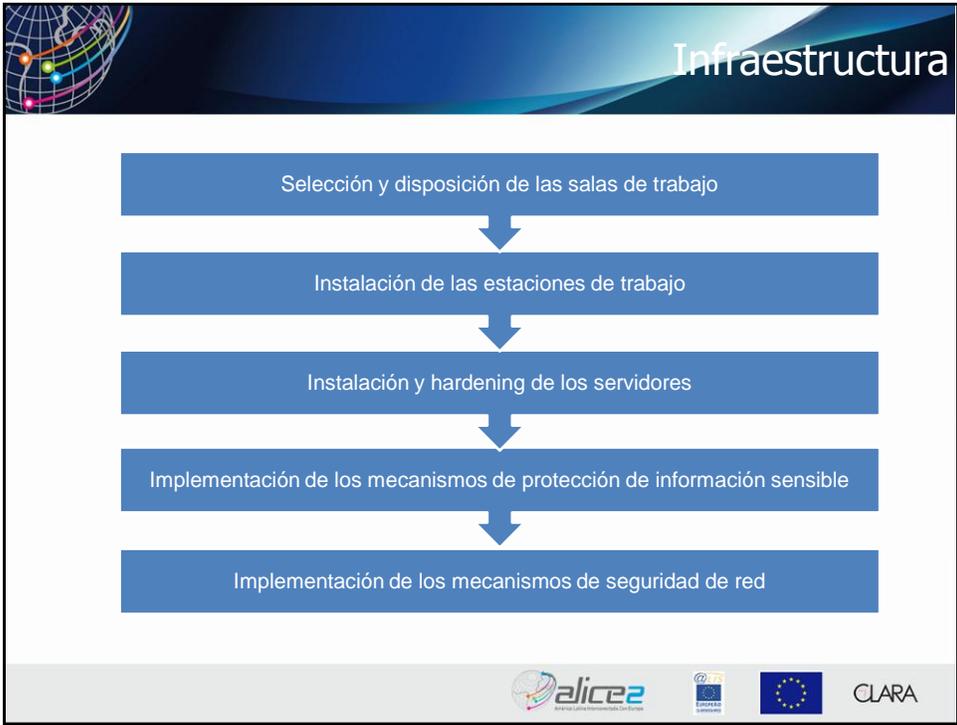
¡Esta lista es una sugerencia!
Puede que otros documentos
sean necesarios.



Implementación

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







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

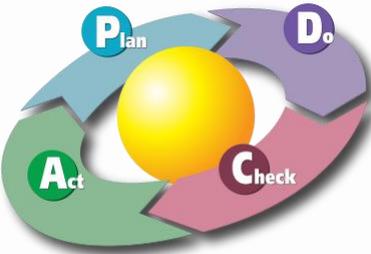
nic-hdl-br: SIC128
person: Security Incidents Response Center
e-mail: cais@cais.rnp.br
created: 20020417
changed: 20050309



CLARA



¿Y ahora?



CLARA



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

