



GT-CSIRT: Grupo de Trabajo de RedCLARA CSIRT

Liliana Solha
Coordinadora del GT


15th RedCLARA Technical Meeting
07-08 de Noviembre, 2011
Montevideo, Uruguay



CLARA




This project is funded
by the European Union

A project implemented
by CLARA



Agenda

- Propuesta del GT
- Miembros
- Líneas de acción
- Status
 - Tareas, entregables, cronograma
 - Próximos pasos



CLARA

Propuesta

- GT-CSIRT
 - Consolida acciones del GT-Seg
 - Alcance reducido
- Propuesta focalizada en tres líneas de acción:
 1. Monitoreo de actividad maliciosa
 2. Tratamiento de incidentes de seguridad
 3. Apoyo a la creación de CSIRTs
- Categoría del GT: *Despliegue de un piloto de nueva tecnología/servicio*




 CLARA

Miembros


- Miembros

Institución	NREN	Nombre
INICTEL	RAAP	José Luis Quiroz
INICTEL	RAAP	Javier Richard Quinto
CEDIA	CEDIA	Claudio Chacón
RAU	RAU	Sergio Ramirez
REUNA	REUNA	Claudia Inostroza
CONARE	CONARE	Danny Silva
RNP	RNP	Frederico Costa
RNP	RNP	Carla Freitas
UFRN	RNP	Mário Sérgio
UTPL	CEDIA	Marco Antonio Cevallos

- Asistente: Rildo Souza (RNP)








 CLARA



LA-1: Monitoreo de actividad maliciosa

- Tareas y entregables:
 - [T1] Estructuración del ambiente de monitoreo (piloto).
 - Documentación de instalación y uso de la solución de monitoreo
 - Informe final de ejecución del piloto
 - Término de adhesión para la NREN
 - [T3] Entrenamiento
 - Material del curso
 - Curso hands-on (Taller CLARA-Tec 2012)
 - [T4] Despliegue
 - Cronograma de implantación
 - Estructura implantada en todas las NRENs
 - Informes periódicos de implantación


LA-1: Monitoreo de actividad maliciosa

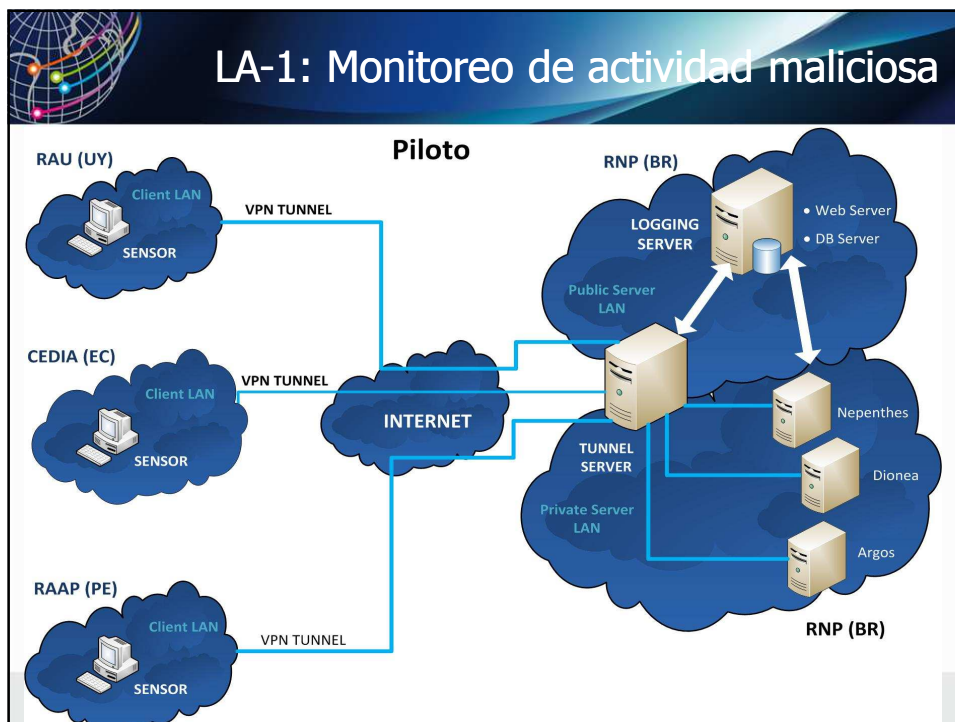
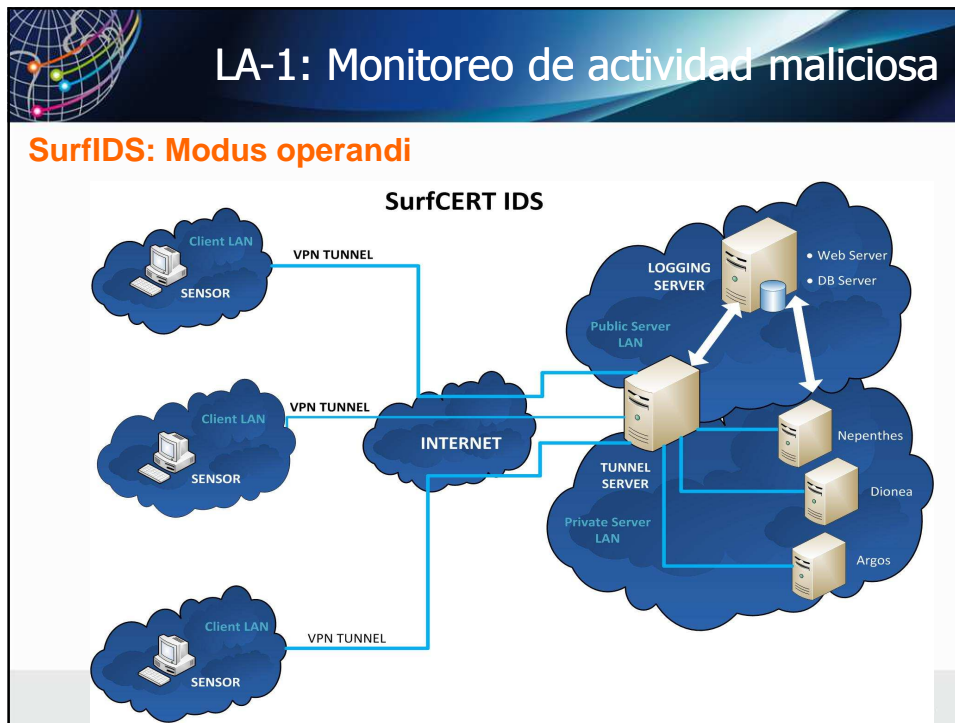
- Solución de Monitoreo: Surf IDS
 - IDS Distribuido (D-IDS) desarrollado por SurfNET (red académica holandesa)
 - <http://www.surfnet.nl/>
 - <http://ids.surfnet.nl>

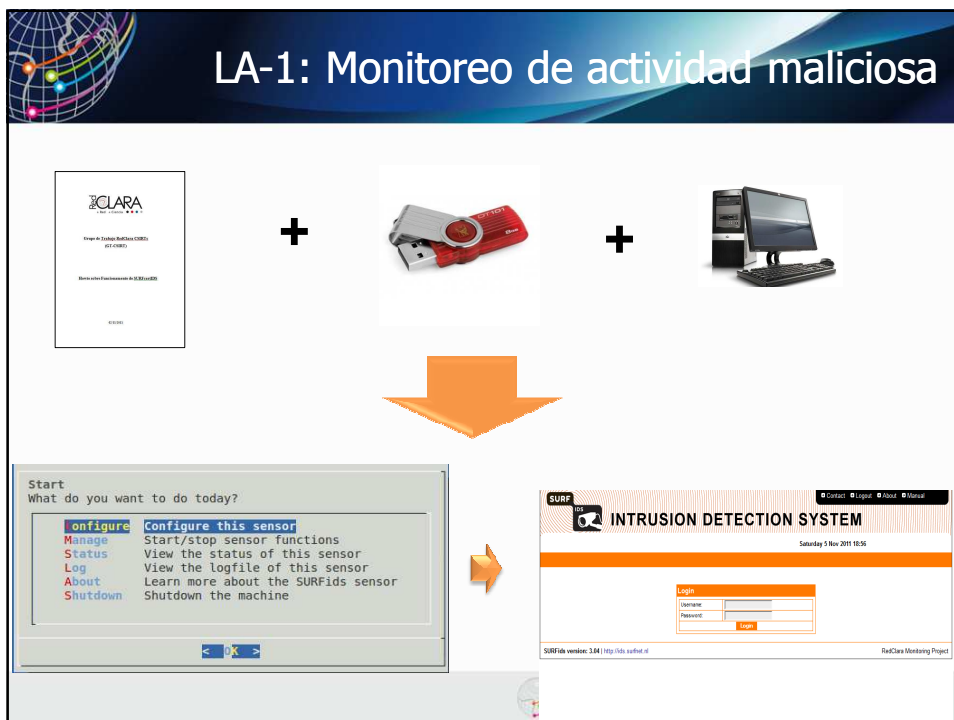
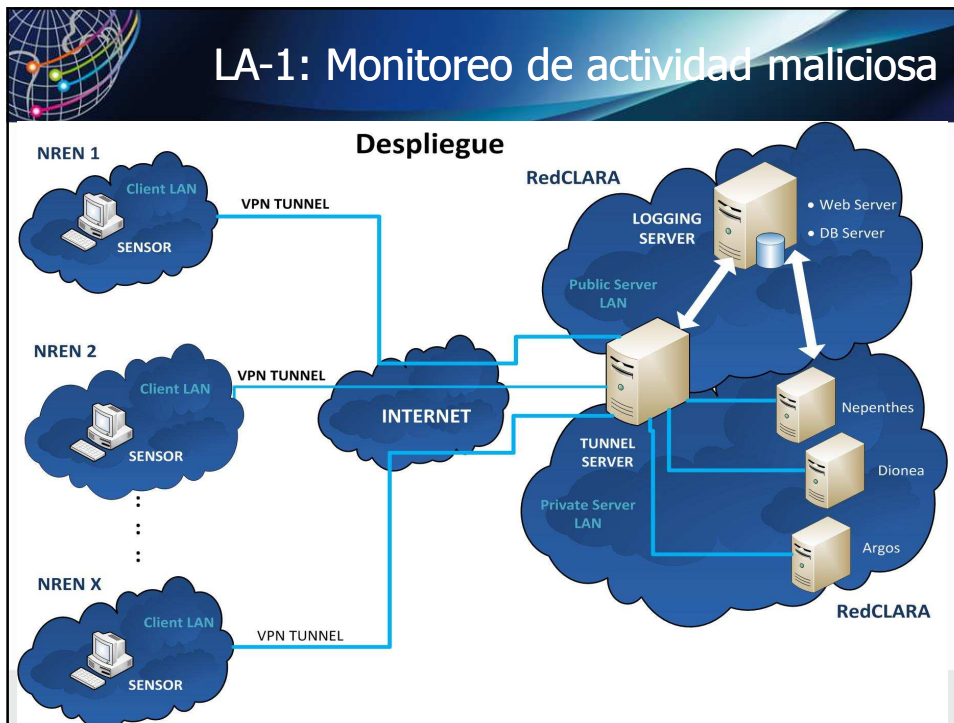


- Modelo focalizado em ambientes donde el uso de la red no es muy controlado (NREN)
- Focalizado en la detección de worms, tentativas de acceso no autorizadas y outro tipo de tráfico malicioso.
- Ventajas: Instalación simple, bajo número de falsos positivos, fácil actualización.







LA-1: Monitoreo de actividad maliciosa

Interface web

The screenshot displays the SURFnet IDS web interface. At the top, it shows the user is logged in as 'jannichielsen' on 'Friday 23 Nov 2007 10:24' with 'Active sensors 5 of 5'. The interface includes a navigation menu with 'Home', 'Report', 'Analyze', 'Configuration', and 'Administration'. The main content area is divided into several sections:

- Attacks:** A table showing detected connections with statistics.

Detected connections	Statistics
Possible malicious attack [?]	299 M
Malicious attack [?]	67 M
Neperthes	85 M
Argos	2 M
Malware offered [?]	85 M
Malware downloaded [?]	15 M
- Exploits:** A table showing malicious attacks with statistics.

Malicious attacks	Statistics
Smartec AV	50 M
DCOM	15 M
NHDE	11 M
ASNT	6 M
Total	85 M
- Attackers:** A table listing IP addresses, last seen times, and total hits.


IP Address	Last Seen	Total Hits
192.168.0.0	23-11-2007 06:25:00	44 M
	23-11-2007 06:21:38	30 M
	23-11-2007 06:22:38	28 M
	23-11-2007 06:26:01	28 M
	23-11-2007 01:59:22	26 M
	23-11-2007 02:34:04	24 M
	23-11-2007 06:15:48	22 M
	23-11-2007 06:18:36	20 M
	23-11-2007 10:55:04	20 M
	23-11-2007 06:54:11	18 M
- Ports:** A table listing destination ports, descriptions, and total hits.

Destination Ports	Description	Total Hits
2967	No description	101 M
445	microsoft-ds	90 M
139	netbios-ssn	67 M
135	msrpc	53 M
8555	No description	50 M
2968	No description	7 M
9988	No description	5 M
80	http	4 M
16238	No description	1 M
3549	No description	1 M

At the bottom, it shows 'SURFids version: 2.00' and 'CLARA' branding.




LA-1: Cronograma

# tarea	Nombre de la tarea	Periodo de ejecución de la tarea	Relación de dependencia
T-1	Estructuración del ambiente de monitoreo de actividad maliciosa	de Jul/11 – Ene/2012 Ago/11 – Feb/2012	Ninguna
T-2	Estructuración del ambiente de tratamiento a incidentes de seguridad	de Jul/11 – Ene/2012	Ninguna
T-3	Entrenamiento sobre Monitoreo y Tratamiento de Incidentes de Seguridad	1a Reunión CLARA-TEC 2012	T-1 y T-2 finalizadas
T-4	Implantación de la solución de monitoreo en las NRENS	de May 2012 – Jun 2013 Jun 2012 – Jun 2013	T-3 finalizada
T-5	Implantación del ambiente de tratamiento de incidentes en las NRENS.	de May 2012 – Jun 2013	T-3 finalizada
T-6	Estableciendo un CSIRT	de Jul 2011 – Dic 2011	Ninguna




LA-1: Monitoreo de actividad maliciosa

- Cronograma – ok
- Próximos pasos:
 - Instalación de los sensores en las NRENs (piloto)
 - Iniciar proceso de "monitoreo asistido" (duración: 2 meses)
 - Análisis y validación del modelo
 - Elaboración del Término de Adhesión.
 - Preparación del material del curso (CLARA-Tec).
 - Riezgo: Entrenamiento no ocurrir durante evento jun/2012.








CLARA



LA-2: Tratamiento de incidentes

- Tareas y entregables:
 - [T2] Estructuración del ambiente de respuesta (piloto).
 - Estructura para recibimiento de incidentes (checklist)
 - Templates de notificación y respuesta desarrollados
 - Toolkit de tratamiento de incidentes de seguridad
 - Informe final de ejecución del piloto
 - [T3] Entrenamiento
 - Material del curso
 - Curso hands-on
 - [T5] Despliegue
 - Cronograma de implantación
 - Estructura implantada en todas las NRENs
 - Informes periódicos de implantación

CLARA

LA-2: Tratamiento de incidentes

- Proceso de tratamiento de incidentes



```


graph LR
    A[Recepción del incidente] --> B[Análisis]
    B --> C[Contención/Mitigación]
    C --> D[Recuperación]
    D --> E[Post-incidente]
  
```

- Recibimiento de la notificación
 - Sensores de Monitoreo (GT-CSIRT – Monitoreo)
 - Fuentes de incidentes de organizaciones/proyectos/iniciativas/csirts
 - Shadowserver, zone-h, spamcop, acuerdos, etc
 - Notificaciones diversas (administradores, usuarios comunes, otros CSIRTs, etc).



LA-2: Tratamiento de incidentes

- Dificultades encontradas (experiencia RNP)
 - Gran cantidad de incidentes (NREN)
 - Muchos de ellos seguían un padrón
 - Aún así eran tratados manualmente!
 - Algunos clientes requerían incidentes agrupados
 - Elaboración de scripts de automatización no seguían un procedimiento padrón, no documentados
 - Difícil actualización de la base de datos de contactos.



LA-2: Tratamiento de incidentes

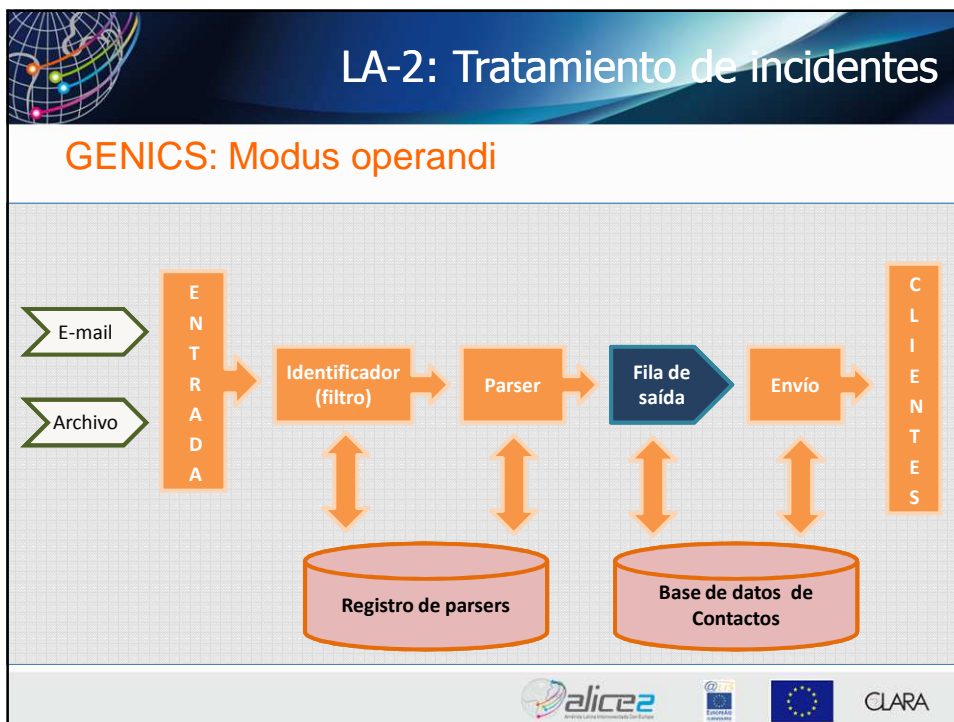
- **Dificultades encontradas (experiencia RNP)**
 - Gran cantidad de incidentes (NREN)
 - Muchos de ellos seguían un padrón
 - Aún así eran tratados manualmente!
 - Algunos clientes requerían incidentes agrupados
 - Elaboración de scripts de automatización no seguían un procedimiento padrón, no documentados
 - Difícil actualización de la base de datos de contactos.

GENICS → RedCLARA!






CLARA



LA-2: Tratamiento de incidentes

Página inicial

CAIS Centro de Atendimento a Incidentes de Segurança

Genics

Bem vindo ao Genics - Gerenciador de Envio de Incidentes e Contatos de Segurança.

Gerenciador de Contatos

O gerenciador de contatos permite a administração dos contatos de segurança para as redes relacionadas aos PoPs, instituições e departamentos cadastrados.

Gerenciador de Incidentes

O gerenciador de incidentes é responsável pelo recebimento, parseamento e envio de mensagens de incidentes. Ao receber uma mensagem de algum dos tipos cadastrados, os incidentes são extraídos pelo parser configurado e salvos no banco de dados. Periodicamente, esses incidentes são agrupados e mensagens são enviadas para os contatos de segurança responsáveis pelos IPs de origem dos incidentes.

alice2 CLARA

LA-2: Tratamiento de incidentes

Gerenciador de contactos: Panel de control

CAIS Centro de Atendimento a Incidentes de Segurança

Gerenciador de Contatos

Estado PoP Instituições Departamentos Endereços Contatos

Gerenciador de Contatos

Máscaras	PoPs	Instituições	Departamentos
1 addresses /8 22 addresses /16 4 addresses /17 5 addresses /18 10 addresses /19 26 addresses /20 23 addresses /21 23 addresses /22 75 addresses /23 808 addresses /24 25 addresses /25 59 addresses /26 4 addresses /27	Há atualmente 30 pops 0 sem contato 3 sem endereço 1 sem instituição Mostrar tudo	Há atualmente 462 instituições 1 sem contato 1 sem endereço 459 sem departamento 3 com departamento Mostrar tudo	Há atualmente 149 departamentos 3 sem contato 1 sem endereço Mostrar tudo
	Endereços	Contatos	Base de dados

alice2 CLARA

LA-2: Tratamiento de incidentes

Gerenciador de contactos: Visión PoPs (NRENs)

Estado
PoP
Instituições
Departamentos
Endereços
Contatos

PoPs
exportar como csv
📄 novo

pop-ac Instituições: 1 Contatos: 1	pop-al Instituições: 5 Contatos: 1	pop-am Instituições: 13 Contatos: 1	pop-ap Instituições: 3 Contatos: 1	pop-ba Instituições: 18 Contatos: 2
pop-ce Instituições: 17 Contatos: 1	pop-df Instituições: 24 Contatos: 2	pop-es Instituições: 17 Contatos: 1	pop-go Instituições: 11 Contatos: 1	pop-ma Instituições: 6 Contatos: 1
pop-mg Instituições: 29 Contatos: 1	pop-ms Instituições: 8 Contatos: 4	pop-mt Instituições: 2 Contatos: 2	pop-pa Instituições: 10 Contatos: 3	pop-pb Instituições: 11 Contatos: 2
pop-pe Instituições: 25 Contatos: 1	pop-pi Instituições: 10 Contatos: 3	pop-pr Instituições: 24 Contatos: 1	pop-rj Instituições: 64 Contatos: 2	pop-rn Instituições: 7 Contatos: 1
pop-ro Instituições: 3 Contatos: 1	pop-rr Instituições: 11 Contatos: 1	pop-rs Instituições: 43 Contatos: 1	pop-sc Instituições: 31 Contatos: 2	pop-se Instituições: 5 Contatos: 1
pop-sp Instituições: 57 Contatos: 2	pop-teste Instituições: 1 Contatos: 2	pop-teste2 Instituições: 0 Contatos: 2	pop-to Instituições: 5 Contatos: 3	REUNA Instituições: 1 Contatos: 1

**NREN:
REUNA**

LA-2: Tratamiento de incidentes

Gerenciador de contactos: Detalles de la NREN

Página Inicial
Contatos
Incidentes
Admin
Ajuda
Sair

CAIS Centro de Atendimento a Incidentes de Segurança

Gerenciador de Contatos

Estado
PoP
Instituições
Departamentos
Endereços
Contatos

Detalhes do PoP

REUNA

Nome: REUNA

Contatos do PoP ➕ Adicionar

Claudia Inostroza
Email: cinostro@reuna.cl Fone: +5623370335

Instituições do PoP

Universidad de Chile

Acronimo: UCHILE
PoP: REUNA

Ações

- Voltar
- Editar pop
- Apagar pop
- Mostrar Histórico

Atalhos

- ⌘ + e edit
- ⌘ + c add contact
- ⌘ + a add address

LA-2: Tratamiento de incidentes

Gerenciador de contactos: Detalles de la Institución

The screenshot shows the 'Gerenciador de Contactos' interface. At the top, there are navigation tabs: Estado, PoP, **Instituições**, Departamentos, Endereços, and Contatos. The main content area is titled 'Detalhes da Instituição' and displays information for 'Universidade de Chile'. The acronym is 'UCHILE', the name is 'Universidade de Chile', and the PoP is 'REUNA'. Below this, there are sections for 'Contatos da instituição' (listing Rodrigo Gutierrez with email and phone), 'Departamentos da instituição' (showing no departments), and 'Endereços da instituição' (with an 'Address to add' field and a list containing '146.83.0.0/18'). On the right, there are 'Ações' (Voltar, Editar instituição, Remover instituição, Mostrar Histórico) and 'Atalhos' (edit, add contact, add dept., add address). The footer includes logos for alice2, Europa, and CLARA.

LA-2: Tratamiento de incidentes

Gerenciador de incidentes: Panel de control

The screenshot shows the 'Gerenciador de Incidentes' control panel. At the top, there are navigation tabs: Página Inicial, Contatos, **Incidentes**, Admin, Ajuda, and Sair. The main content area is titled 'Gerenciador de Incidentes' and features several components:

- Emails Recebidos:** A line chart showing the number of received emails from 01 Nov to 07 Nov. The values are approximately: 50, 20, 45, 45, 30, 10, 5.
- Emails Enviados:** A line chart showing the number of sent emails from 01 Nov to 07 Nov. The values are approximately: 250, 200, 150, 250, 250, 50, 50.
- Incidentes:** A summary box with the following data:
 - Incompleto (0)
 - IP não registrado (1)
 - Contato não registrado (0)
 - Completo (12)
 - Enviado (372728)
 - Falso positivo (0)
 - Incidente ignorado (9)
- Processar:** A box indicating 'Processamento inicia em 1 hora, 5 minutos' and a 'Processar agora' button.
- Parsers:** A box showing 'Há atualmente 31 parsers'.
- Receiver:** A box with a green status indicator and the text 'Está executando'.
- Sender:** A box with a green status indicator and the text 'Ocioso'.

 The footer includes logos for alice2, Europa, and CLARA.

LA-2: Tratamiento de incidentes

Gerenciador de incidentes: Parsers

The screenshot shows the CAIS (Centro de Atendimento a Incidentes de Segurança) web interface. The top navigation bar includes links for 'Página Inicial', 'Contatos', 'Incidentes', 'Admin', 'Ajuda', and 'Sair'. The main header displays 'Gerenciador de Incidentes' with a sub-menu containing 'Estado', 'Parsers', 'Emails Recebidos', 'Fila', 'Emails Enviados', and 'Estatísticas'. The 'Parsers' section shows a list of 31 parsers, with the following details visible:

- cert-botnet-rustock**: Identificador: ^Subject: Alerta: maquinas fazendo parte da botnet Rustock
- copyright**: Identificador: ^Subject:\s*.*Notice\s*ID:
- copyright_sem_xml**: Identificador: ^Subject:\s*Casels*ID
- f1-botnet**: Identificador: ^Subject:\s*Fornecedor 1 - botnetcc
- f1-botnetcc-url**: Identificador: ^Subject:\s*Fornecedor 1 - dnsrr

At the bottom of the interface, there are logos for 'alice2', 'European Union', and 'CLARA'.

LA-2: Tratamiento de incidentes

Gerenciador de incidentes: Detalhes del parser

The screenshot shows the 'Detalhes do Parser' (Parser Details) view in the CAIS interface. The navigation and header are identical to the previous screenshot. The main content area displays the configuration for the 'copyright' parser:

- Nome copyright**
- Identificador Principal**: ^Subject:\s*.*Notice\s*ID:
- Identificadores Extra (Um por linha)**: ^From:\s*.*@copyright-compliance
- Variáveis do Obrigatórias (Separados por vírgula)**: (Empty field)
- Incluir incidentes originais na mensagem
- Template**: (Empty field)

On the right side, there is an 'Ações' (Actions) menu with the following options: 'Salvar Mudanças', 'Testar Parser', and 'Remover Parser'. The footer contains the same logos as the previous screenshot.


LA-2: Cronograma

# tarea	Nombre de la tarea	Periodo de ejecución de la tarea	Relación de dependencia
T-1	Estructuración del ambiente de monitoreo de actividad maliciosa	Jul/2011 – Ene/2012	Ninguna
T-2	Estructuración del ambiente de tratamiento a incidentes de seguridad	Jul/2011 – Ene/2012 Ago/2011 – Feb/2012	Ninguna
T-3	Entrenamiento sobre Monitoreo y Tratamiento de Incidentes de Seguridad	1a Reunión CLARA-TEC 2012	T-1 y T-2 finalizadas
T-4	Implantación de la solución de monitoreo en las NRENS	May/2012 – Jun/2013	T-3 finalizada
T-5	Implantación del ambiente de tratamiento de incidentes en las NRENS.	May/2012 – Jun/2013 Jun/2012 – Jun/2013	T-3 finalizada
T-6	Estableciendo un CSIRT	Jul 2011 – Dic 2011	Ninguna



LA-2: Tratamiento de incidentes

- Cronograma – ok
- Próximos pasos:
 - Finalizar la infra-estructura base de respuesta (piloto)
 - RFC 2142: abuse@dominio [11/14], security@dominio [6/14]
 - Responsables de seguridad (NREN SPoCs) [11/14]
 - Detalles adicionales de los responsables de seguridad (RFC 2350)
 - Detalles de las NRENS
 - ASNs, Fajas IPs designados
 - Incluir "abuse-c" en el LACNIC Whois
 - Como? Individualmente? RedCLARA/LACNIC?
 - Incluir csirt@redclara.net en el campo "remarks" en el LACNIC Whois (?)
 - Implantar GENICS en infra-estructura RedCLARA



LA-3: Apoyo a la creación de CSIRTs

- Tareas:
 - [T6] Implementación de un CSIRT
 - Orientaciones de cómo crear un CSIRT
 - Checklist de implementación de un CSIRT
 - Piloto: UTPL (CEDIA), RNP: CSIRT CEDIA.
 - Nuevo entregable
- Cronograma: ok
 - Modificado para abrigar entregable #3 (Piloto).
 - Ago/2011 – Jun/2012.





CLARA

LA-3: Cronograma


# tarea	Nombre de la tarea	Periodo de ejecución de la tarea	Relación de dependencia
T-1	Estructuración del ambiente de monitoreo de actividad maliciosa	Jul/11 – Ene/2012	Ninguna
T-2	Estructuración del ambiente de tratamiento a incidentes de seguridad	Jul/11 – Ene/2012	Ninguna
T-3	Entrenamiento sobre Monitoreo y Tratamiento de Incidentes de Seguridad	1a Reunión CLARA-TEC 2012	T-1 y T-2 finalizadas
T-4	Implantación de la solución de monitoreo en las NRENS	May 2012 – Jun 2013	T-3 finalizada
T-5	Implantación del ambiente de tratamiento de incidentes en las NRENS.	May 2012 – Jun 2013	T-3 finalizada
T-6	Estableciendo un CSIRT	Jul 2011 – Dic 2011 Ago/2011 – Jun/2012	Ninguna






CLARA



Preguntas



Liliana Velásquez Solha
nina@cais.rnp.br



CLARA