# VIII JORNADAS STIC CCN-CERT

## La defensa del patrimonio tecnológico frente a los ciberataques

**10 y 11 de diciembre de 2014**

CCN-CERT
centro criptológico nacional

LUCIA

CCN
Centro Criptológico Nacional

ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN


C/Argentona 20, 28023 MADRID

www.ccn-cert.cni.es

**Joaquín Seco Martínez**

**joaquin.seco@csa.es**

CSA

# Índice

# 1 Introducción

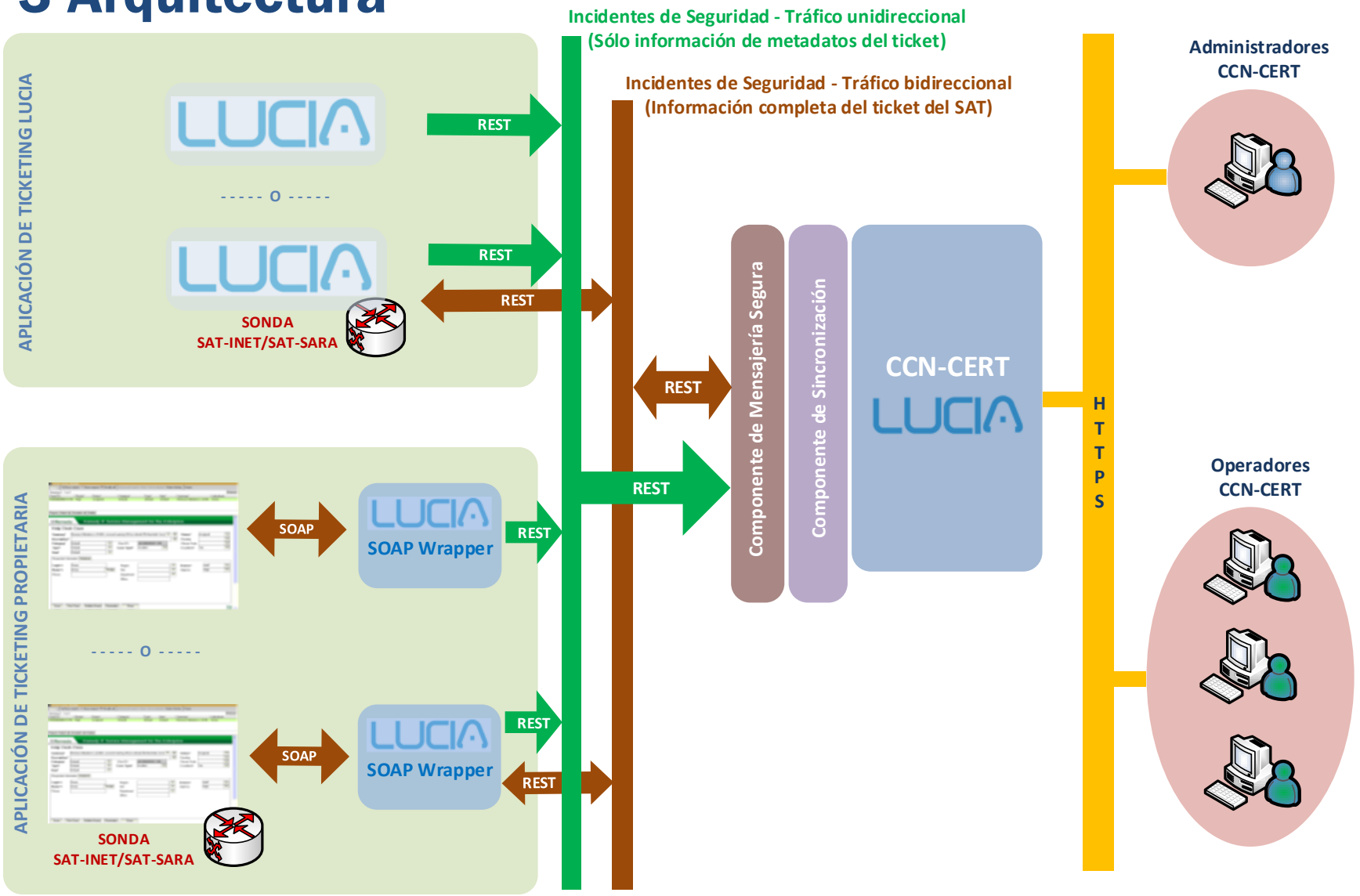
## LUCIA Listado Unificado de Coordinación de Incidentes y Amenazas

- Herramienta de gestión de incidentes de seguridad del CCN-CERT
- Basada en el sistema de incidencias Request Tracker (RT)
- Incluye extensión para equipos de respuesta a incidentes Request Tracker for Incident Response (RT-IR)
- Personalizado para cumplir los requerimientos y procedimientos del CCN-CERT y del ENS
- Arquitectura distribuida y federada
- Información sincronizada y compartida entre los diferentes organismos adscritos

# 2 Objetivos

- Dotar a los organismos adscritos de una herramienta interna para la gestión de incidentes
- Federar los sistemas LUCIA desplegados
- Contar con una plataforma única y distribuida para la gestión de incidentes de seguridad en todos los organismos adscritos
- Reportar al CCN la información de contexto (metadatos) de todos los incidentes de seguridad identificados
- Comunicar y sincronizar incidentes de seguridad entre el CCN y la comunidad CCN-CERT y mejorar los procedimientos con aquellos adscritos al Sistema de Alerta Temprana (SAT Internet / SAT SARA)
- Posibilitar la comunicación de incidentes de seguridad desde plataformas externas (ej. REMEDY)
- Cumplir los requisitos del Esquema Nacional de Seguridad (ENS)

# 3 Arquitectura



# 4 Características

- Basada en la utilización de servicios REST
  - Mayor flexibilidad y mejora de la integración y rendimiento en RT
- Comunicación segura dotada de transaccionalidad para garantizar la correcta recepción sin pérdida de cualquier incidente notificado
- Plataforma única disponible para todos los organismos adscritos
  - Distribución de una Máquina Virtual previamente paquetizada
  - Adaptable a la arquitectura de almacenamiento de cada organismo
- Trazabilidad de incidentes entre organismos y CCN-CERT
- Clasificación de incidentes unificada (“lenguaje común”)
- Registro de tiempos de respuesta en el paso entre diferentes estados del incidente (SLA)

# 5 Formularios Inteligentes

- Funcionalidad que pretende dotar a los formularios de notificación de incidentes de cierta inteligencia para su categorización
- Adaptación de términos y conceptos al Esquema Nacional de Seguridad
- Adaptación de los conceptos de Prioridad y Criticidad al concepto de Peligrosidad
- Peligrosidad
  - Al crear un nuevo ticket: asignada de forma manual en función de la peligrosidad estimada
  - Al cerrar el ticket: peligrosidad real asignada de forma automática en base a la combinación de los diferentes parámetros del ticket
    - Cálculo de valores ponderados en función de su importancia

# 6 Interconexión: Conectores

- Permiten la integración de organismos que ya dispongan de sistemas de ticketing con la instancia de LUCIA del CCN-CERT
- Capa SOAP para la conexión con sistemas estándar
  - LUCIA SOAP Wrapper: Comunicación REST-SOAP
- Posibilidad de realizar desarrollos a medida para sistemas que no permitan la integración SOAP
- Disponibilidad actual de conector BMC Remedy
- Posibles futuras integraciones:
  - OTRS
  - HP Service Manager
  - Track, RedMine, Mantis

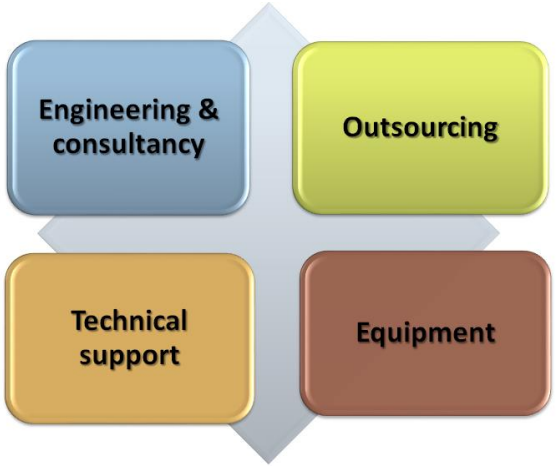
# 7 Roadmap

| Hito | |
|---|---|
| Recogida y análisis de necesidades – Arranque de LUCIA versión 2 |  |
| Instalación de LUCIA en el CCN |  |
| Entrega máquina virtual para organismos | |
| Presentación de LUCIA en Jornadas de Ciberseguridad | |
| Implantación de LUCIA. Formación CCN-CERT | |
| Entrega de máquina virtual con conector REMEDY | |
| Consultoría e implantación en organismos que requieran soporte específico | |

# 8 CSA. Presentación Corporativa

- Compañía Tecnológica fundada 1996

- Servicios de IT




- Oficinas y Centros de Trabajo


- Desarrollo de Soluciones de Software
  - Desarrollo en diferentes tecnologías
  - Desarrollos verticales y especializados

www.csa.es

info@csa.es

- **E-Mails**
  - lucia@ccn-cert.cni.es
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - sondas@ccn-cert.cni.es
  - redsara@ccn-cert.cni.es
  - carmen@ccn-cert.cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es

Síguenos en Linked in