IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

CENTRO CRIPTOLÓGICO NACIONAL

- Centro Criptológico Nacional
- CCN-CERT
- lucia@ccn-cert.cni.es

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas)

OBJETIVOS:

- Dotar a los organismos de una herramienta interna para la gestión de incidentes paquetizada y parametrizada basada en Request Tracker (RT) y Request Tracker for Incident Response (RTIR)
- Contar con una plataforma única y distribuida para la gestión de incidentes de seguridad en todos los organismos adscritos (SAT)
- Federar los sistemas desplegados
- Cumplir los requisitos del ENS acorde con la guía CCN-STIC 817
- Ofrecer un lenguaje común de peligrosidad y clasificación de los incidentes

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas)

PERSONALIZADO PARA:

- Mantener la trazabilidad y seguimiento del incidente
- Automatizar tareas (Notificaciones, recordatorios, cierres automáticos)
- Construir una base de datos de conocimiento
- Comunicar y sincronizar incidentes de seguridad entre el CCN-CERT y su comunidad mejorando el intercambio y coordinación con aquellos adscritos al Sistema de Alerta Temprana (SAT-INET / SAT-SARA)
- Reportar al CCN la información de contexto (metadatos) de todos los incidentes de seguridad identificados de forma anonimizada
- Permitir integrar otros sistemas (ej. REMEDY, OTRS, ServiceDesk,...)

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas)

BENEFICIOS DE INSTALACIÓN INSTANCIA PROPIA

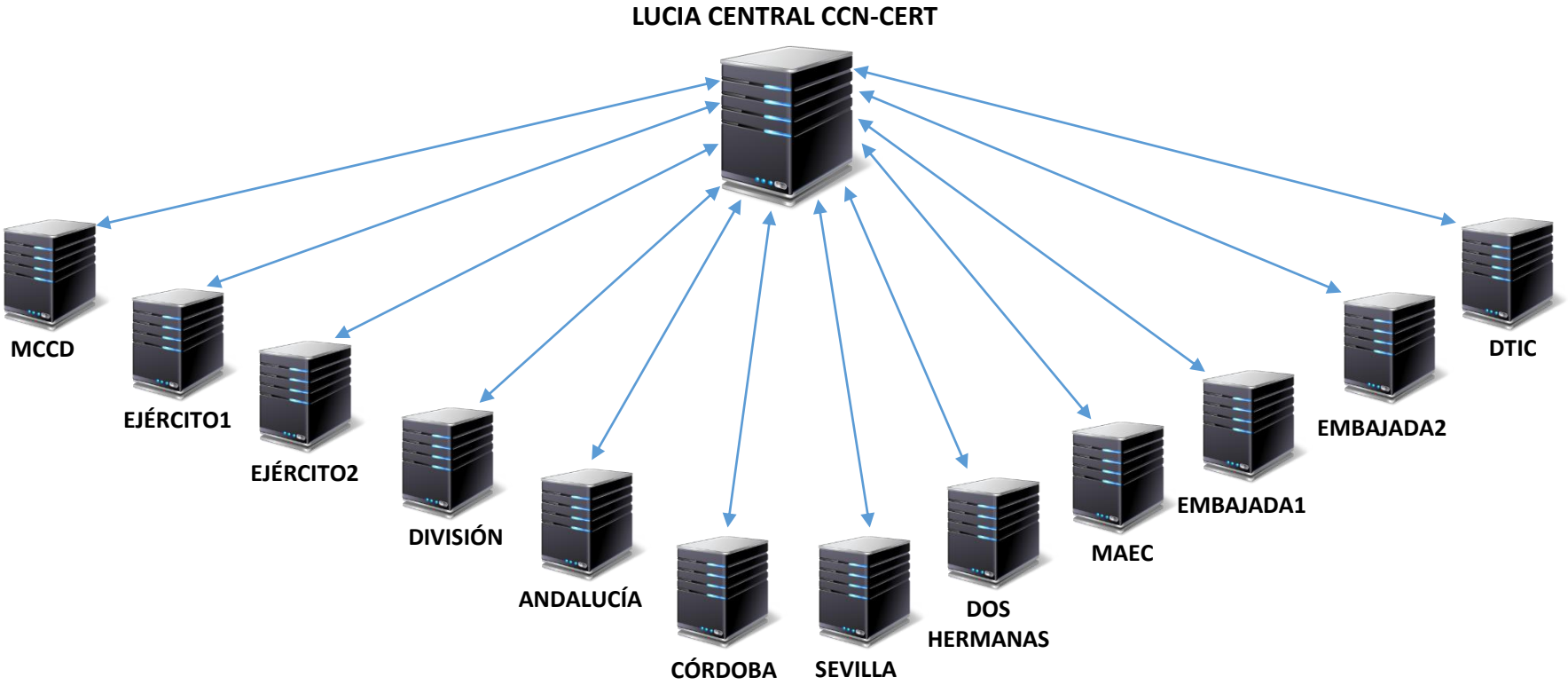
FUNCIONALIDADES DISPONIBLES	LUCIA CENTRAL (CCN-CERT)	LUCIA (ORGANISMO FEDERADO)
Gestión de incidentes propios del organismo	NO	SI
Gestión de incidentes SAT-INET	SI	SI
Gestión de incidentes SAT-SARA	SI	SI
Almacenamiento de la base de datos	Compartido	Organismo
Remisión automática al CCN de metadatos sobre incidentes sufridos en el organismo en cumplimiento del ENS	NO	SI
Granularidad de perfiles de usuarios	NO	SI
Explotación de datos para informes (p. ej. INES)	NO (excepto SAT)	SI

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas)

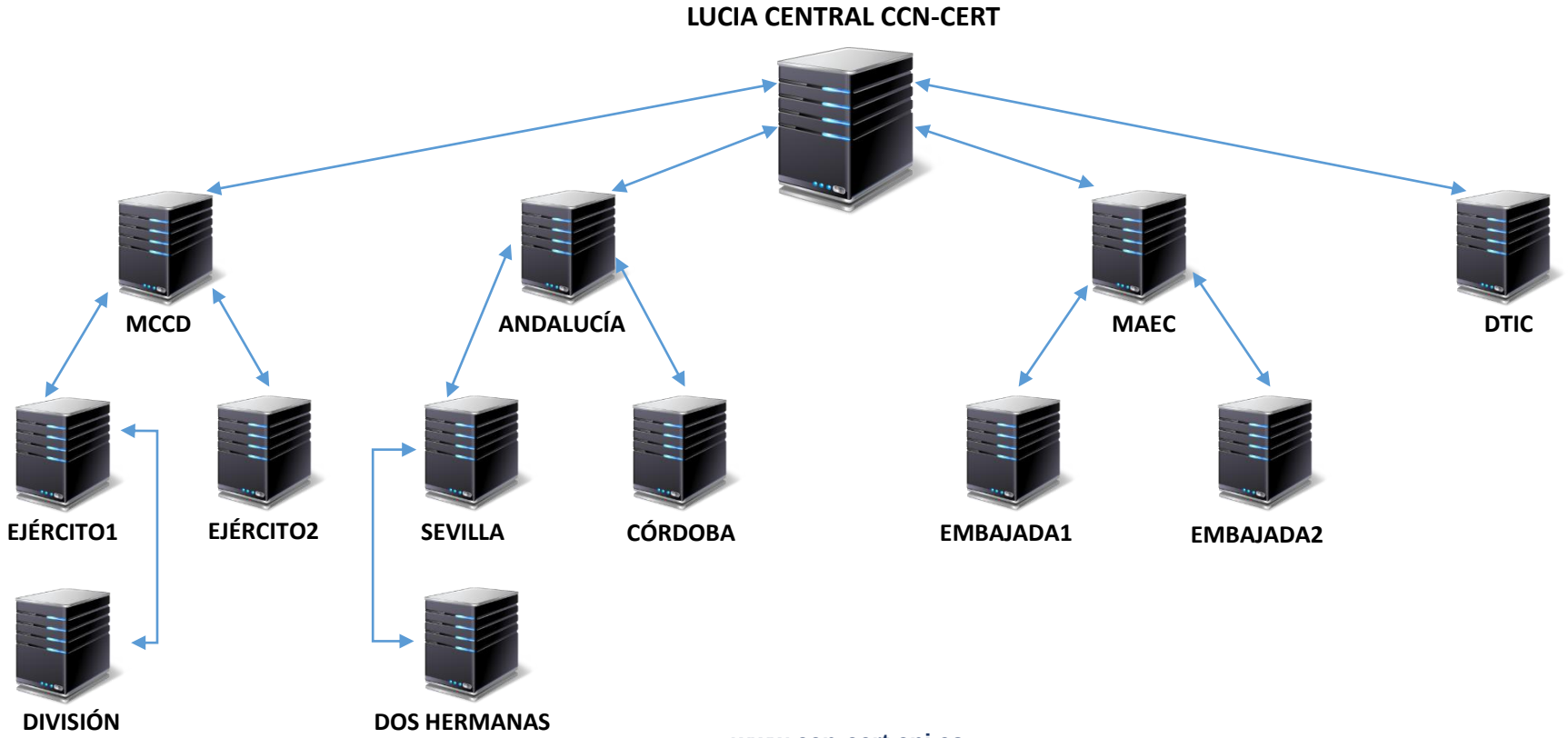
ESTADO DEL PROYECTO:

- Actualmente instalándose en 9 organismos (que se conozca)
- Versión estable Rev2 liberada a finales de Septiembre 2015
- Solucionadas incidencias reportadas e integración de peticiones de mejoras de organismos.
- Actualización Rev2.1 (mediados Diciembre 2015):
  - Actualización de la nueva clasificación de incidentes (CCN-STIC 817)
  - Actualización protocolo de sincronización LUCIA-REST-2.0
  - Sincronización de ficheros
  - Bugs menores….
- ¡¡ Entrada en producción en el CCN-CERT el 1 de enero 2016 !!

PROYECTO LUCIA 2015



PROYECTO LUCIA 2016



LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas)

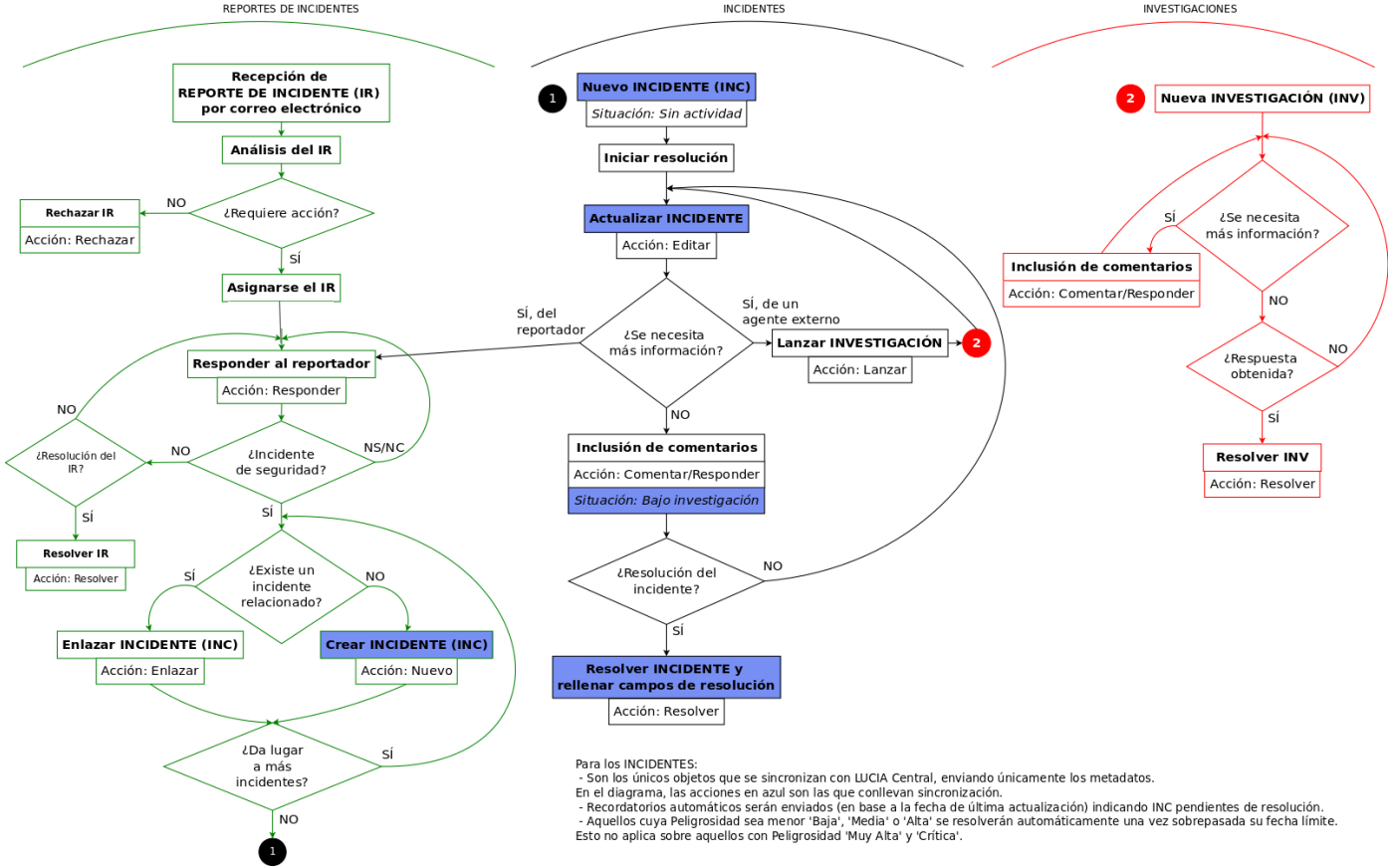
CONCEPTOS:

Existen tres tipos de tickets organizados en colas:

- **Reporte de Incidente (IR):** Comunicación con la persona que informó el problema.
- **Investigación (INV):** Comunicación con terceros.
- **Incidente (INC):** Representa una incidencia. Puede tener asociados varios Reportes de Incidentes y/o Investigaciones y es el único elemento susceptible de sincronización con LUCIA Central. Dispone de los atributos necesarios para permitir almacenar la información necesaria definida en la guía CCN-STIC 817.

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas)

GESTIÓN DE INCIDENTES PROPIOS

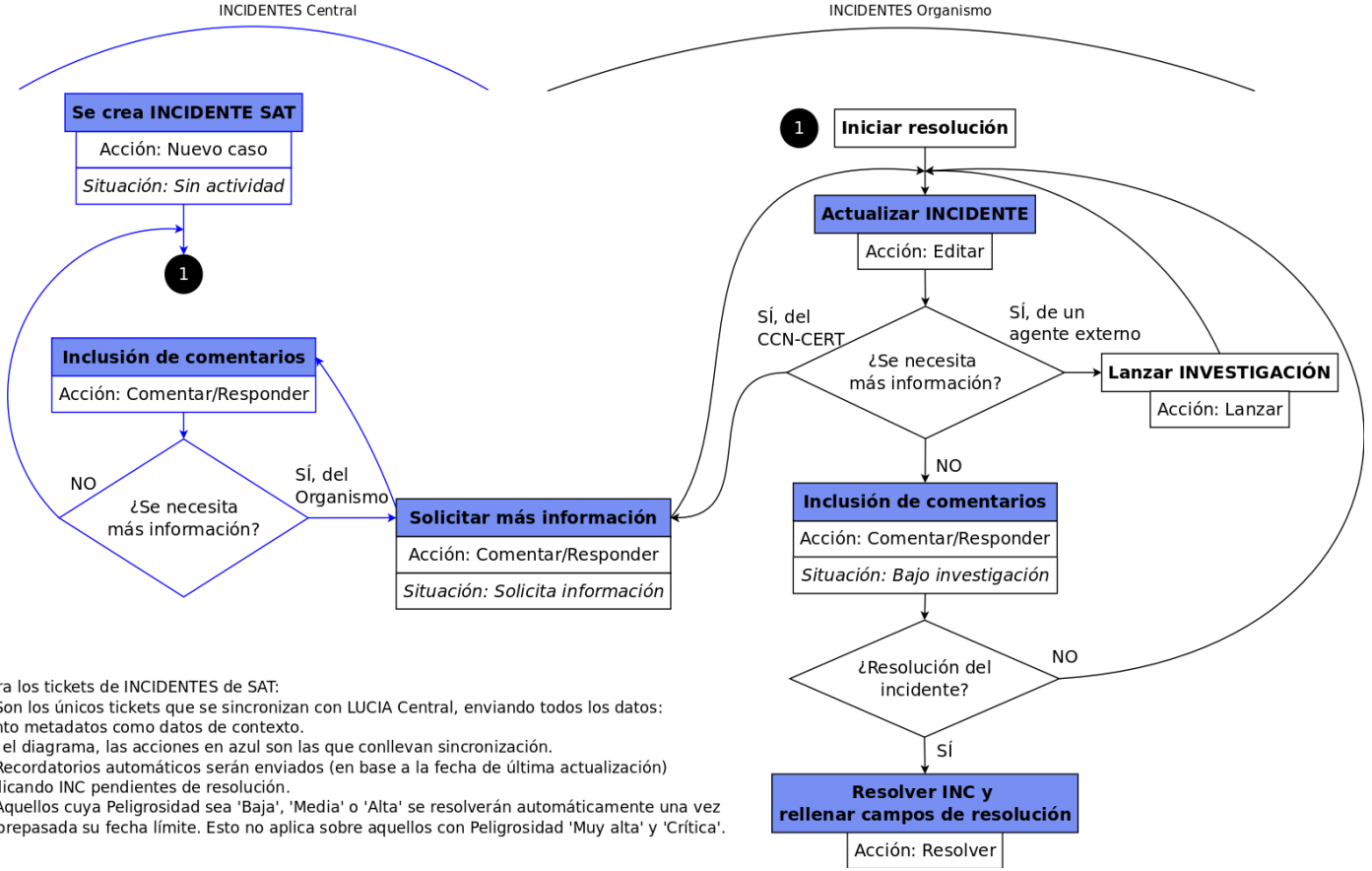


Para los INCIDENTES:
- Son los únicos objetos que se sincronizan con LUCIA Central, enviando únicamente los metadatos.

En el diagrama, las acciones en azul son las que conllevan sincronización.
- Recordatorios automáticos serán enviados (en base a la fecha de última actualización) indicando INC pendientes de resolución.
- Aquellos cuya Peligrosidad sea menor 'Baja', 'Media' o 'Alta' se resolverán automáticamente una vez sobrepasada su fecha límite.

Esto no aplica sobre aquellos con Peligrosidad 'Muy Alta' y 'Crítica'.

GESTIÓN DE INCIDENTES SISTEMA DE ALERTA TEMPRANA (SAT)



Para los tickets de INCIDENTES de SAT:
- Son los únicos tickets que se sincronizan con LUCIA Central, enviando todos los datos: tanto metadatos como datos de contexto.

En el diagrama, las acciones en azul son las que conllevan sincronización.
- Recordatorios automáticos serán enviados (en base a la fecha de última actualización) indicando INC pendientes de resolución.
- Aquellos cuya Peligrosidad sea 'Baja', 'Media' o 'Alta' se resolverán automáticamente una vez sobrepasada su fecha límite. Esto no aplica sobre aquellos con Peligrosidad 'Muy alta' y 'Crítica'.

¿PREGUNTAS?

lucia@ccn-cert.cni.es

Equivalencias en otros idiomas			
Idioma	**Traducción**	**Idioma**	**Traducción**
Gallego	Lucía	Danés	Lucia
Valenciano	Llúcia	Islandés	Lúcía
Catalán	Llúcia	Noruego	Lucia
Francés	Lucie	Sueco	Lucia
Italiano	Lucia	Ruso	Светлана (Se lee Svetlana)
Portugués	Lúcia, Luzia	Español	Lucía
Inglés	Lucy	Polaco	Łucja o Lucja
Alemán	Lucia o Luzie	Eslovaco	Lucia
Holandés	Loes	Finés	---
Vasco	Luke	Griego	Λουκία (se lee Luquía)
Búlgaro	Светлана (se lee Svetlana)	Húngaro	Luca (se lee Lutza)

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
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en Linked in