Presentación

Versión 2.02

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Índice

1. CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. INTRODUCCIÓN

Durante los últimos años se ha asistido a un incremento muy importante del número de incidentes ocurridos. En este tiempo los equipos de respuesta a incidentes de seguridad (CSIRTs/CERTs), se centraban en mejorar la detección proactiva de problemas dentro de sus ámbitos de actuación a través de inversiones en herramientas que les permitían aumentar la visibilidad de los eventos de seguridad existentes y así poder evitar posibles incidentes de seguridad que puedan incurrir en situaciones de mucha más gravedad. Además se ha visto como los intentos de intrusión son cada vez más complejos y más numerosos contra los sistemas, aprovechando cualquier mal configuración o mala administración que estos puedan tener. Todo esto ha llevado a que el número de incidentes, que el equipo de respuesta a incidentes de la Administración Pública, CCN-CERT, tiene que atender es cada día mayor, y que por tanto el esfuerzo que debe dedicar a ello es también más grande.

La utilización de herramientas de gestión de incidentes ayuda a mejorar considerablemente dicha tarea, pero el trabajo no debe quedar ahí, ya que se debe seguir avanzando en otros aspectos que ayuden a dar un servicio de cada vez más calidad desde el CCN-CERT. Para ello se quieren mejorar los procesos de atención de incidentes, automatizando aquellas tareas que lo permitan, y ayudando por tanto a reducir el tiempo de respuesta que se da ante un incidente de seguridad; también se deben mejorar los procesos de intercambio de información y la forma en que dicha información se comparte, no solo creando canales seguros que avalen la autenticidad e integridad de la información, sino que permitan hacer un análisis y tratamiento de la información más exacto a través de las herramientas de gestión de incidentes, aportando valor al proceso de atención, y facilitando la toma de decisiones al gestor de incidentes de seguridad adaptando sus procedimientos al Esquema Nacional de Seguridad (ENS).

Por este motivo el equipo de respuesta ante incidentes de seguridad de la información del Centro de Criptológico Nacional (CCN-CERT) se ha decidido a mejorar su herramienta de gestión de incidentes de forma que le permita colaborar con el resto de organismos dentro de su ámbito de actuación, permitiéndole compartir información de una forma más eficaz, y con una mayor rapidez, teniendo por objetivo mejorar la respuesta ante cualquier amenaza o incidente de seguridad al que se puedan enfrentar.

3. ¿QUÉ ES LUCIA?

LUCIA (**L**istado **U**nificado de **C**oordinación de **I**ncidentes y **A**menazas), es el proyecto de implantación de la nueva herramienta de gestión de incidentes de seguridad del CCN-CERT, basada en el sistema de incidencias *Request Tracker* (RT) y en su extensión para equipos de respuesta a incidentes *Request Tracker for Incident Response* (RT-IR). Dichas herramientas han sido personalizadas para cumplir los requerimientos y procedimientos del CCN-CERT y alineadas con el cumplimiento del Esquema Nacional de Seguridad (ENS).

Como se ha mencionado, una de las mejoras más importantes que incorpora LUCIA es la posibilidad de interacción entre sistemas de gestión de incidentes, pudiendo llegar a crear una federación de sistemas, en la que el sistema del CCN-CERT establecería un canal con cada uno de los sistemas independientes, y a través de esté enlace seguro, se transmitirían incidentes de seguridad de los organismo adscritos al SAT o la metainformación de los incidentes entre las distintas organizaciones y el CCN-CERT (depende de la participación en el proyecto), facilitando por tanto la coordinación, intercambio y resolución de los incidentes de seguridad.

Aunque las incidencias de SAT-INET y SAT-SARA se podrán seguir gestionando por parte de los organismos adheridos, en su forma tradicional, es decir, accediendo a la herramienta, LUCIA proporcionará una nueva forma de atenderlas, para aquellos organismos que la desplieguen, debido a que la herramienta del CCN-CERT y la herramienta local del organismo se sincronizarán y compartirán la información del evento, ya no habrá necesidad de acceso al sistema central, sino que los organismos podrán realizar todas las operaciones de actualización sobre el sistema local.

4. BENEFICIOS APORTADOS A LOS ORGANISMOS ADSCRITOS

Los beneficios directos que los organismos adscritos al proyecto podrán obtener son:

- Una herramienta de gestión de incidentes en el caso de que no dispongan ninguna o necesiten una específica.
- Cumplir los requisitos del Esquema Nacional de Seguridad (ENS) y la guía CCN-STIC 817 (Gestión de incidentes en el ENS),
- Ofrecer un lenguaje común de peligrosidad y clasificación del incidente en consonancia con las guías CCN-STIC 403 y CCN-STIC 817 basado en dos niveles y avalado por instituciones internacionales.
- Mejorar la coordinación entre el CCN-CERT y todos los organismos a los que ofrece sus servicios mediante la Integración de los incidentes de seguridad con el CCN-CERT.
- Mejorar el intercambio de información de incidentes de seguridad.
- Mantener la trazabilidad y seguimiento del incidente
- Mejora en los procesos de gestión
- Automatizar tareas y permitir su integración con otros sistemas
- Categorización del cierre y causas del incidente
- Construir bases de datos de conocimiento
- Mejora de gestión de los proyectos SAT-SARA y SAT-INET

5. ARQUITECTURA

LUCIA se basa en un sistema de software libre que no acarrea ningún coste de licencias por parte del organismo adscrito.

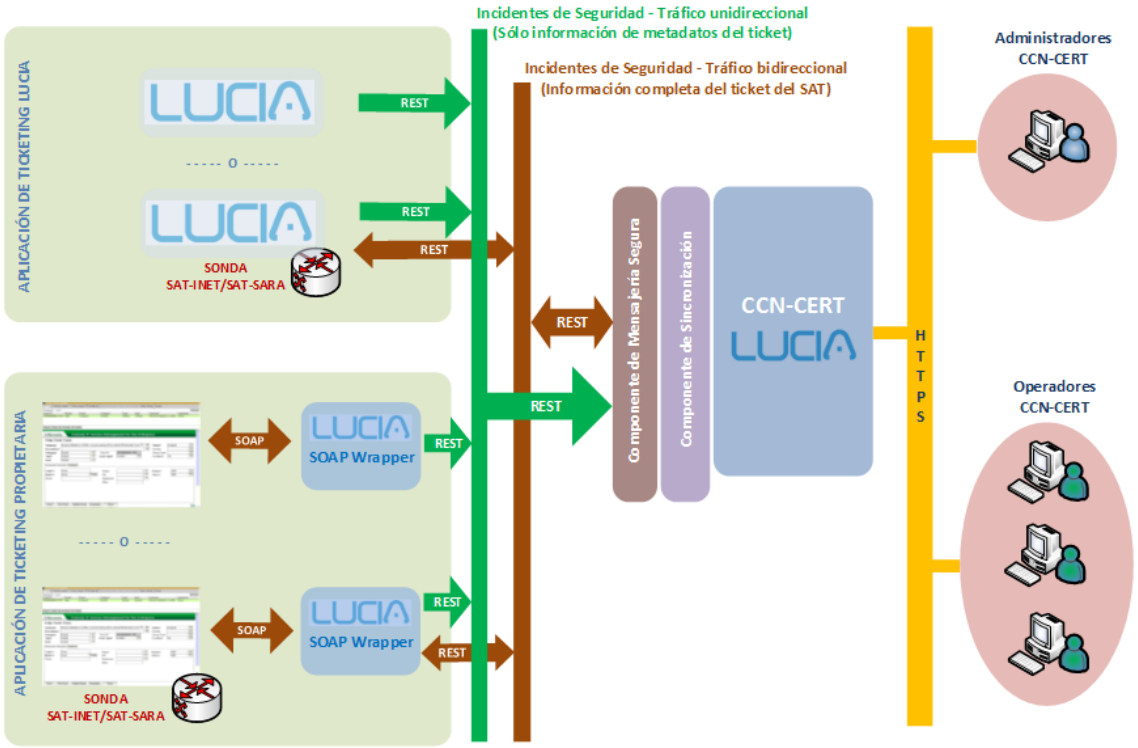
El sistema se encuentra virtualizado mediante VMware (compatible con KVM [http://www.linux-kvm.org]) y configurado sobre una plataforma linux Centos de 64 bits (en su versión 7 actualmente) por lo que su compatibilidad se encuentra asegurada para cualquier plataforma que disponga de un mínimo de 2 núcleos de procesador (no necesariamente 2 procesadores físicos), 4 GB de memoria y 200 Gb de disco duro. Al ser una máquina virtual los recursos pueden ampliarse según la plataforma a utilizar.

La comunicación entre sistemas LUCIA se realiza mediante comunicación HTTPS/REST/SOAP en un canal cifrado y autenticado.

Se distribuye una máquina virtual preconfigurada a los organismos federados para su sistema local.

Las actualizaciones de seguridad y cambio de versiones correrán a cargo del CCN-CERT, el cual enviará periódicamente a los organismos para su implementación. En el caso de personalizaciones concretas para ampliar o adaptar los servicios internos serán responsabilidad del organismo existiendo el buzón lucia@ccn-cert.cni.es para dirigir las dudas y consultas.

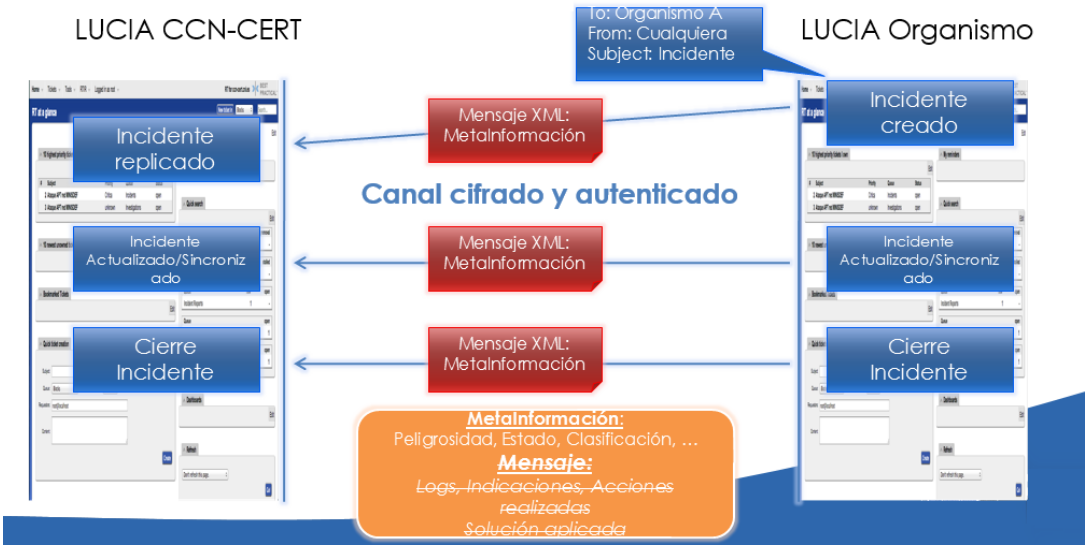
El esquema de federación de sistemas LUCIA es la siguiente:



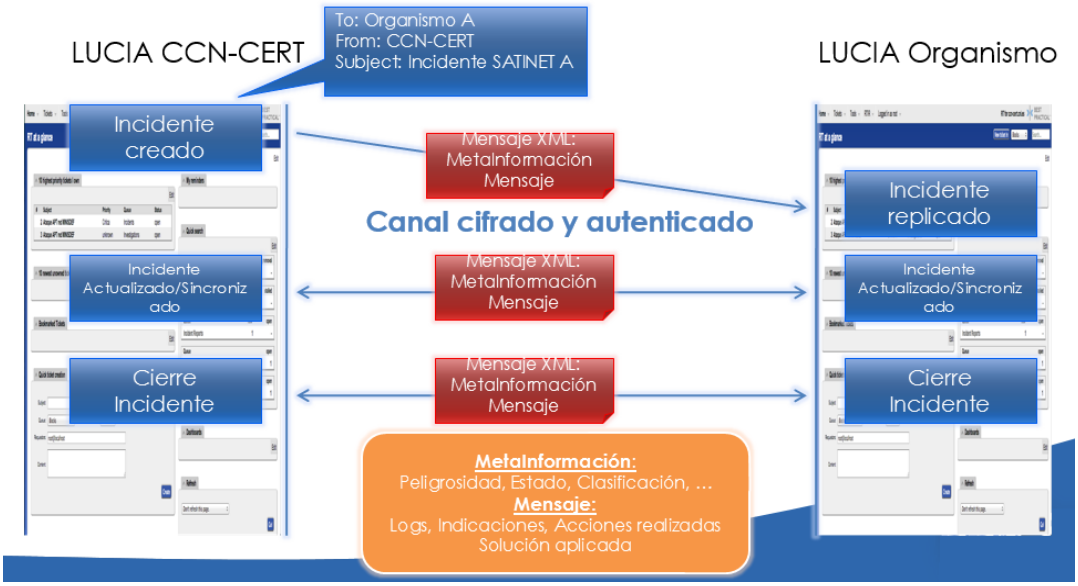
6. INTERCAMBIO DE INFORMACIÓN

Una vez instalado y configurado LUCIA, el sistema será totalmente autónomo e independiente para su uso en local desde el organismo.

El intercambio de información con el CCN-CERT en cuanto a los incidentes de seguridad propios del organismo, será exclusivamente unidireccional de la metainformación del incidente (Peligrosidad, estado, categorización,…) sin incluir mensajes o datos confidenciales o datos sujetos a la LOPD.



En el caso de que el organismo se encuentre adscrito a alguno de los proyectos del CCN-CERT (SAT-INET, SAT-SARA,…), la replicación y actualización de los incidentes será bidireccional y completa incluyendo toda la información puesto que serán generados desde los sistemas del CCN-CERT. De esta forma la gestión y seguimiento local del organismo podrá ser supervisada por el CCN-CERT según el siguiente esquema:



7. PREGUNTAS FRECUENTES

¿Qué es Request Tracker?

Request Tracker, comúnmente abreviado como RT, es un sistema de tickets de seguimiento escrito en Perl utilizado para coordinar las tareas y gestionar las solicitudes entre una comunidad de usuarios. La primera versión de RT en 1996 fue escrita por Jesse Vincent, que más tarde creó Best Practical Solutions LLC para distribuir, desarrollar y apoyar el paquete. RT es de código abierto (FOSS) y se distribuye bajo la Licencia Pública General GNU.

Request Tracker for Incident Respond (RTIR) es una extensión especial de RT para cumplir con las necesidades específicas de los equipos CERT/CSIRT. Fue diseñado incialmente por JANET-CERT (equipo de seguridad de la red academica del Reino Unido), y desarrollado por Best Practical. En 2006 se actualizó y amplió con la financiación conjunta de nueve Equipos de Respuesta a Incidentes de Seguridad (CSIRT) europeos, tanto de ámbito academico, como gubernamental.

¿Cómo se comunican los sistemas LUCIA?

Los mensajes con el CCN-CERT y viceversa se transfieren a través de un canal cifrado HTTPS utilizando el protocolo REST. Existe la posibilidad de desarrollar una capa SOAP para interconectar los sistemas que así lo requieran

¿Qué información se envía ?

El intercambio de información con el CCN-CERT en cuanto a los incidentes de seguridad propios del organismo, será exclusivamente unidireccional de la metainformación del incidente (Peligrosidad, estado, categorización,…) sin incluir mensajes o datos confidenciales o datos sujetos a la LOPD. Existe la posibilidad de que el organismo comparta la totalidad de la información si así lo desea.

¿Quién se puede suscribir a este servicio?

Cualquier organismo perteneciente a la Administración Pública puede adherirse contactando con el CCN-CERT.

¿Dónde puedo obtener más información o consultar mis dudas?

Web: https://www.ccn-cert.cni.es/lucia

E-Mail: lucia@ccn-cert.cni.es