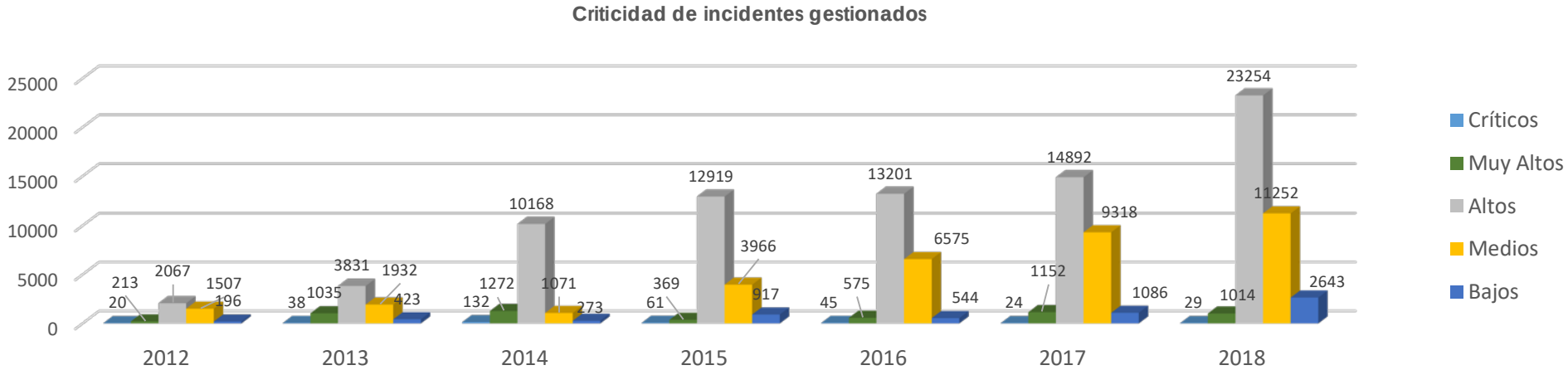
02. LUCIA Y FEDERACIÓN

Javier Candau
Jefe Departamento Ciberseguridad
Centro Criptológico Nacional
ccn@cni.es

centro criptológico nacional

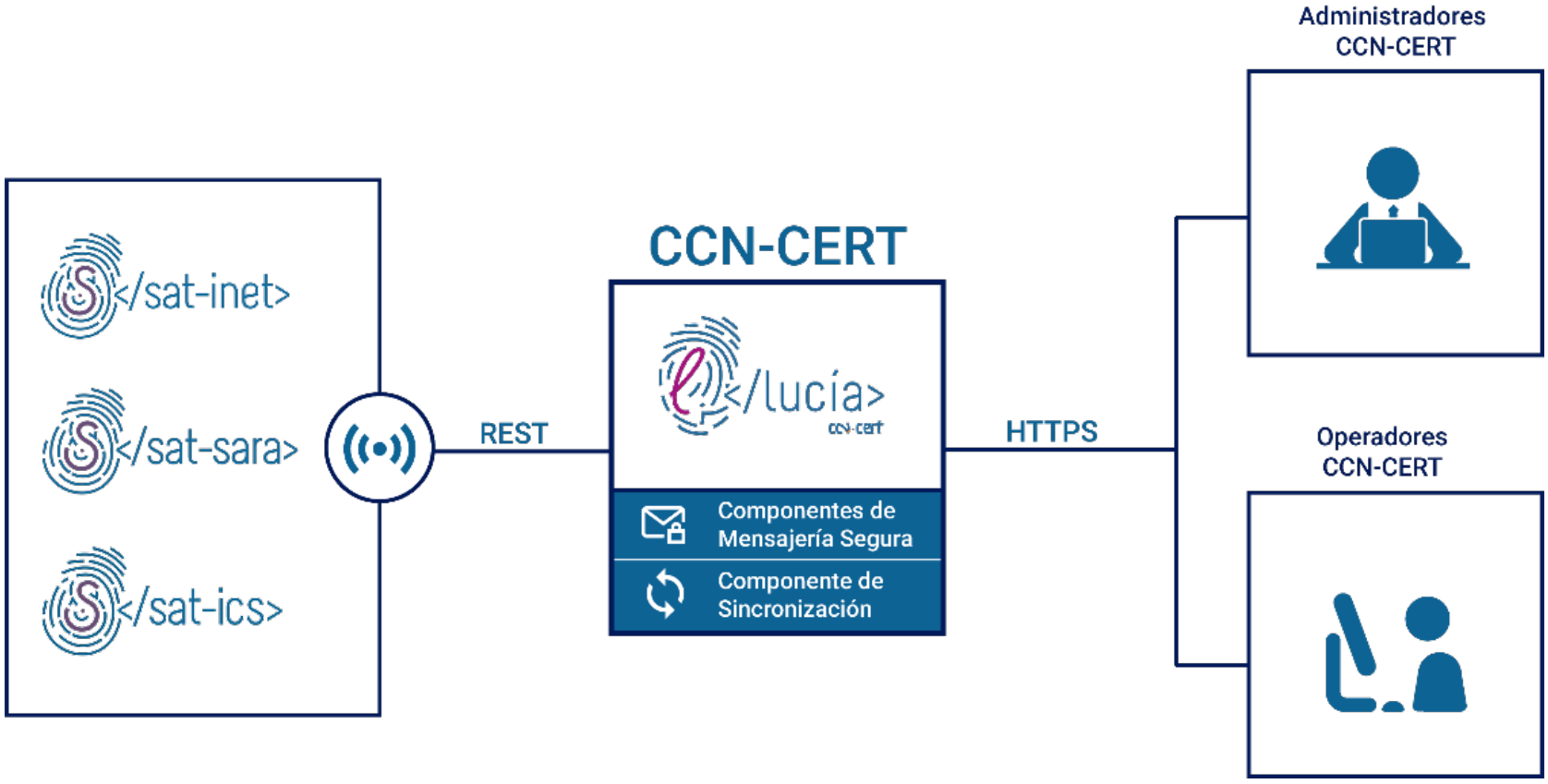
Incidentes gestionados en 2018



LUCIA. Definición

- **LUCIA** = **L**istado **U**nificado de **C**oordinación de **I**ncidentes y **A**menazas
  - Solución para la Gestión de **Ciberincidentes** en las entidades del ámbito de **aplicación del Esquema Nacional de Seguridad**. Ofrece un **lenguaje común** de peligrosidad y clasificación del incidente y mantiene la **trazabilidad** y el seguimiento del mismo.

LUCIA. Motivación



INTERCAMBIO / NOTIFICACIÓN

RD 3/2010 Artículo 36. Capacidad de respuesta a incidentes de seguridad de la información.

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

Las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I del presente real decreto.

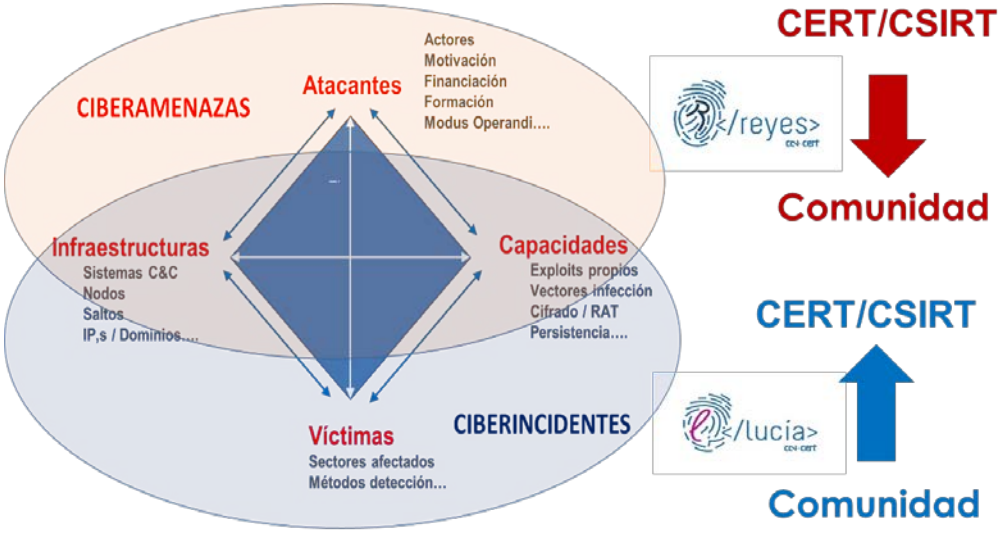
RDL 12/2018 TÍTULO V Notificación de incidentes

Artículo 19. Obligación de notificar.

1. Los operadores de servicios esenciales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios.

4. Las autoridades competentes y los CSIRT de referencia utilizarán una plataforma común para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes.

…//….



Obligaciones de notificación

- RD 3/2010 que regula el Esquema Nacional de Seguridad (ENS). En su artículo 36 se habla de la **notificación al Centro Criptológico Nacional de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados**.

- **Ley 8/2011 - RD 704/2011 Protección de las Infraestructuras Críticas**
  - Instrucciones de la Secretaria de Estado para la Seguridad en el caso de las Infraestructuras Criticas.

- **REGLAMENTO (UE) 2016/679 de 27 de abril de 2016. Tratamiento y libre circulación datos personales (GPDR) y LO 3/2018.**

- **Directiva Banco Central Europeo.** Notificar impacto significativo (luz publico, daño financiero – 5 millones €, incumplimiento legal, replica en otras…).

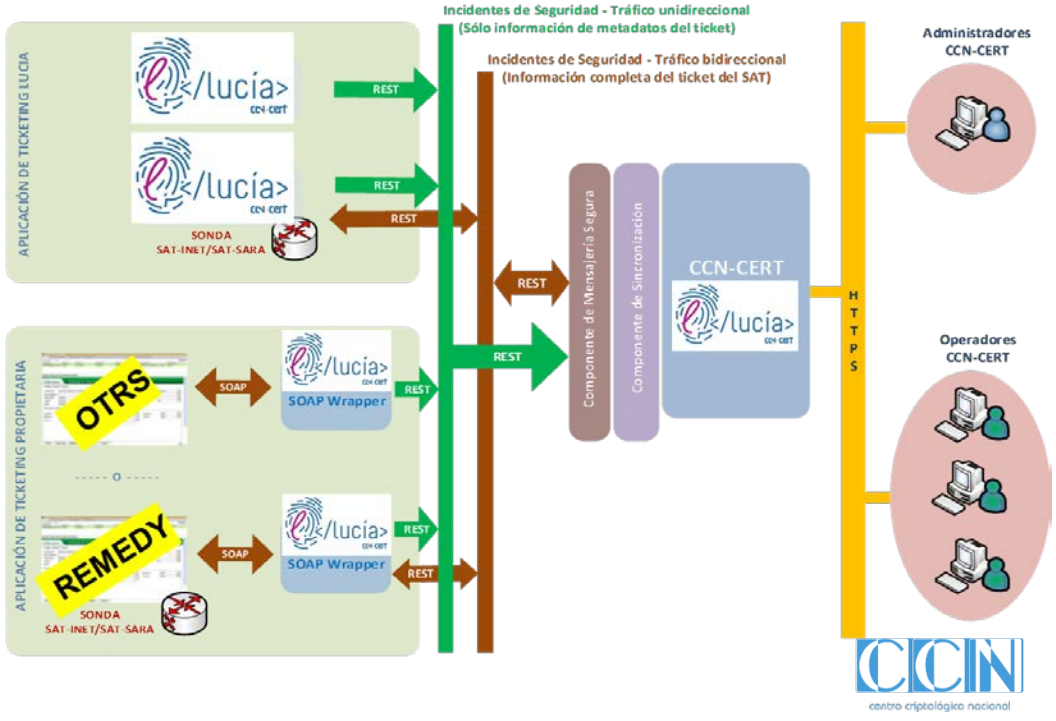
- **DIRECTIVA (UE) 2016/1148 de 06 de julio de 2016. (NIS) Medidas garantizar nivel común seguridad de redes y sistemas.**
- **LEY TRANSPOSICIÓN (RDL 12/2018, de 7 de septiembre),**
  - **Las autoridades** competentes y los CSIRT de referencia **utilizarán una plataforma común** para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes.

- ***…//…***

Herramienta LUCIA: Sistema de gestión federada de tickets

- Cumplir los requisitos del ENS.
- Mejorar la coordinación entre CCN-CERT y los organismos (Mejorar intercambio de incidentes)
- Lenguaje común de **peligrosidad** y **clasificación del incidente**
- Mantener la **trazabilidad y seguimiento del incidente**
- Automatizar tareas
- **Federar Sistemas**
- Permitir integrar otras herramientas …. REYES / MARTA / MARIA
- **Reportar a terceros**

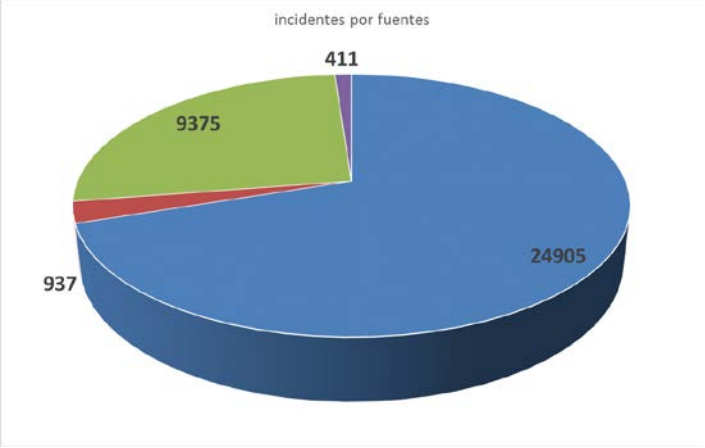
- **Basada en sistema de incidencias Request Tracker (RT)**
- **Incluye extensión para CERT Request Tracker for Incident Response (RT-IR)**



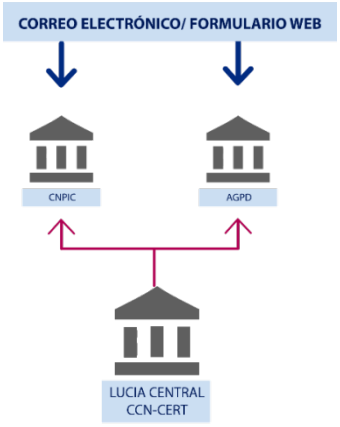
</lucia>
CCN-CERT

Organismos en Lucia Central

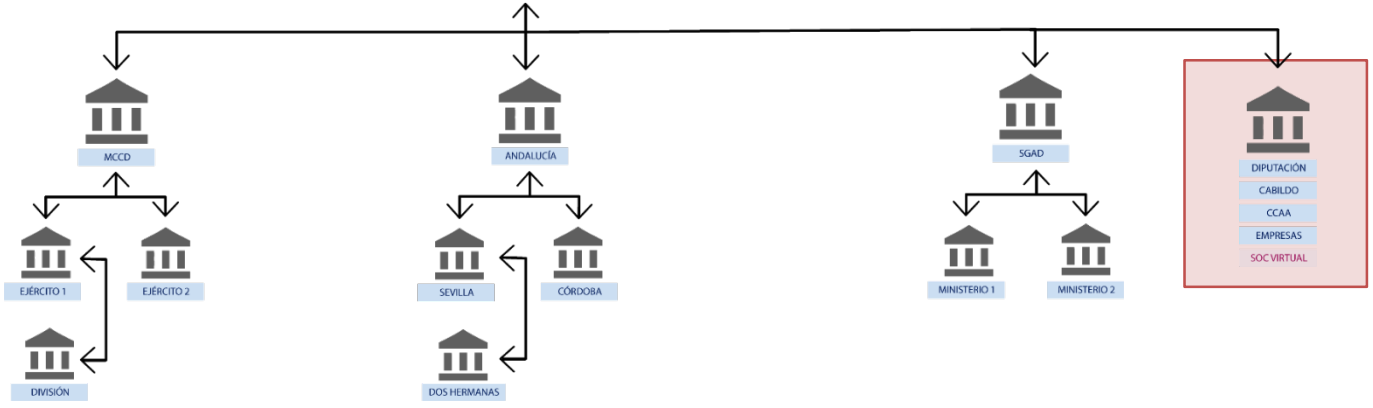
Organismos Federados
31 diciembre de 2018



REPORTE A TERCEROS



FEDERACIÓN

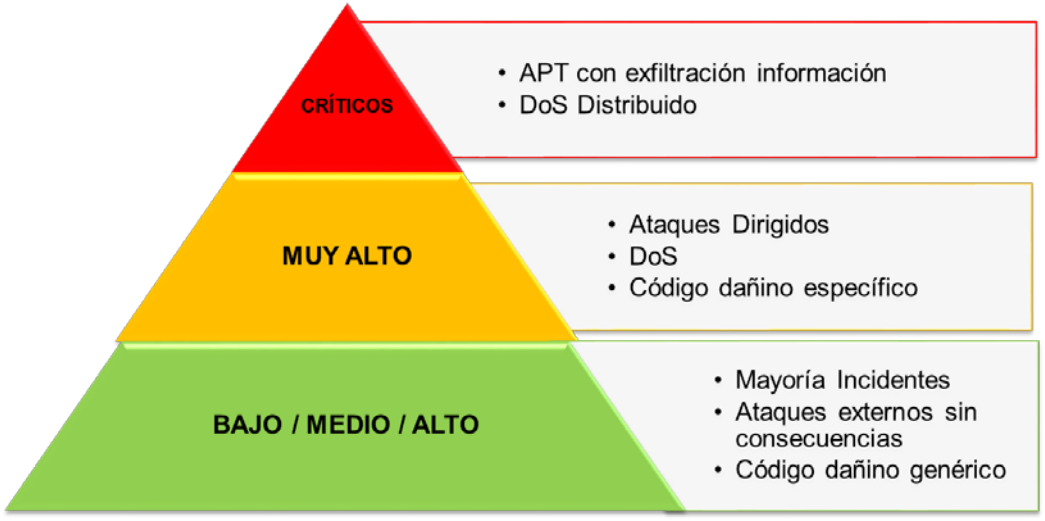


SATINET 69%
LUCIA 27%
SATSARA 2%
CCN-CERT 1%
SAT ICS 1%

CCN
centro criptológico nacional

CCN-STIC 817

- Peligrosidad / Impacto
- Taxonomía
- Otros criterios
- Causas
- Límites de cierre
- Métricas eficiencia
  - T(10) T (50) T(90)
  - Incidentes cerrados



Código	Descripción	ENS
C.1	Incumplimiento o carencia de normativa de seguridad	org.1 org.2
C.2	Incumplimiento o carencia de procedimientos de seguridad	org.3
C.3	incumplimiento del proceso de autorización	org.4
C.4	Fallo técnico u operativo de identificación o autenticación	op.acc.1 op.acc.5
C.5	Fallo técnico u operativo de los controles de acceso	op.acc.2 op.acc.4
C.6	Acceso local no autorizado	op.acc.6
C.7	Acceso remoto no autorizado	op.acc.7
C.8	Ausencia o deficiencia de la segregación de funciones y tareas	op.acc.3
C.9	Entrada de datos incorrectos que no han sido detectados a tiempo	
C.10	Configuración inadecuada	op.exp.2 op.exp.3
C.11	Ausencia o deficiencia de mantenimiento	op.exp.4
C.12	Inadecuada ejecución de un cambio	op.exp.5
C.13	Falta de concienciación del personal	mp.per.3
C.14	Defectos de formación del personal	mp.per.4
C.15	Puestos de trabajo no despejados	mp.eq.1
C.16	Información remanente no autorizada	mp.si.5
C.17	Defectos en la especificación de una aplicación SW	mp.sw
C.18	Defectos en la implantación de una aplicación SW	mp.sw.2
C.19	Entrada en operación de equipamiento (SW, HW, Comunnicaciones) defectuoso	mp.sw.2
C.20	Servicio externo: causados por negligencia del proveedor	mp.ext.2
C.21	Servicio externo: que no se han comunicado dentro de los plazos y cauces acordados	mp.exp.2
C.22	Servicio externo: el proveedor responsable ha incumplido las obligaciones acordadas	mp.exp.2

[1] JP – Jornada-persona; estimación del esfuerzo necesario para realizar una tarea cuya unidad equivale a una jornada de trabajo ininterrumpido de un trabajador medio.

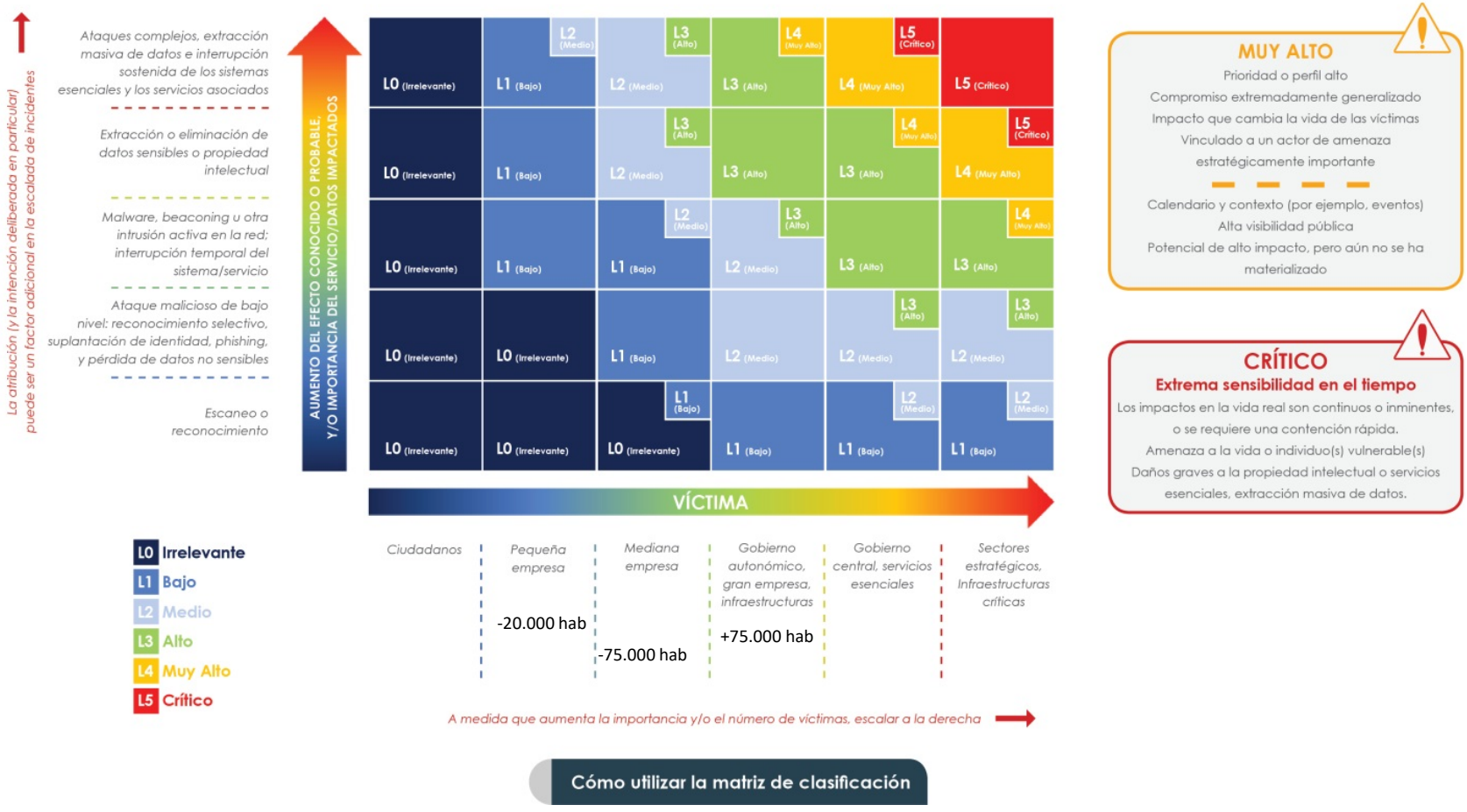
CRITERIOS PARA CLASIFICAR UN INCIDENTE

Cómo utilizar la matriz de clasificación

1. Evaluar el efecto conocido o probable del incidente:
- La naturaleza de lo que está ocurriendo y el efecto en el sistema o sistemas de destino
- Si los efectos son continuos, empeoran o se mueven lateralmente
- La importancia de los sistemas, servicios o datos de destino
- Considerar la atribución (capacidad e intención) o cualquier interés operativo

2. Evaluar la(s) víctima(s) del incidente:
- El número de víctimas
- La relevancia de la(s) víctima(s)
- Considerar tanto a las víctimas primarias como a las secundarias

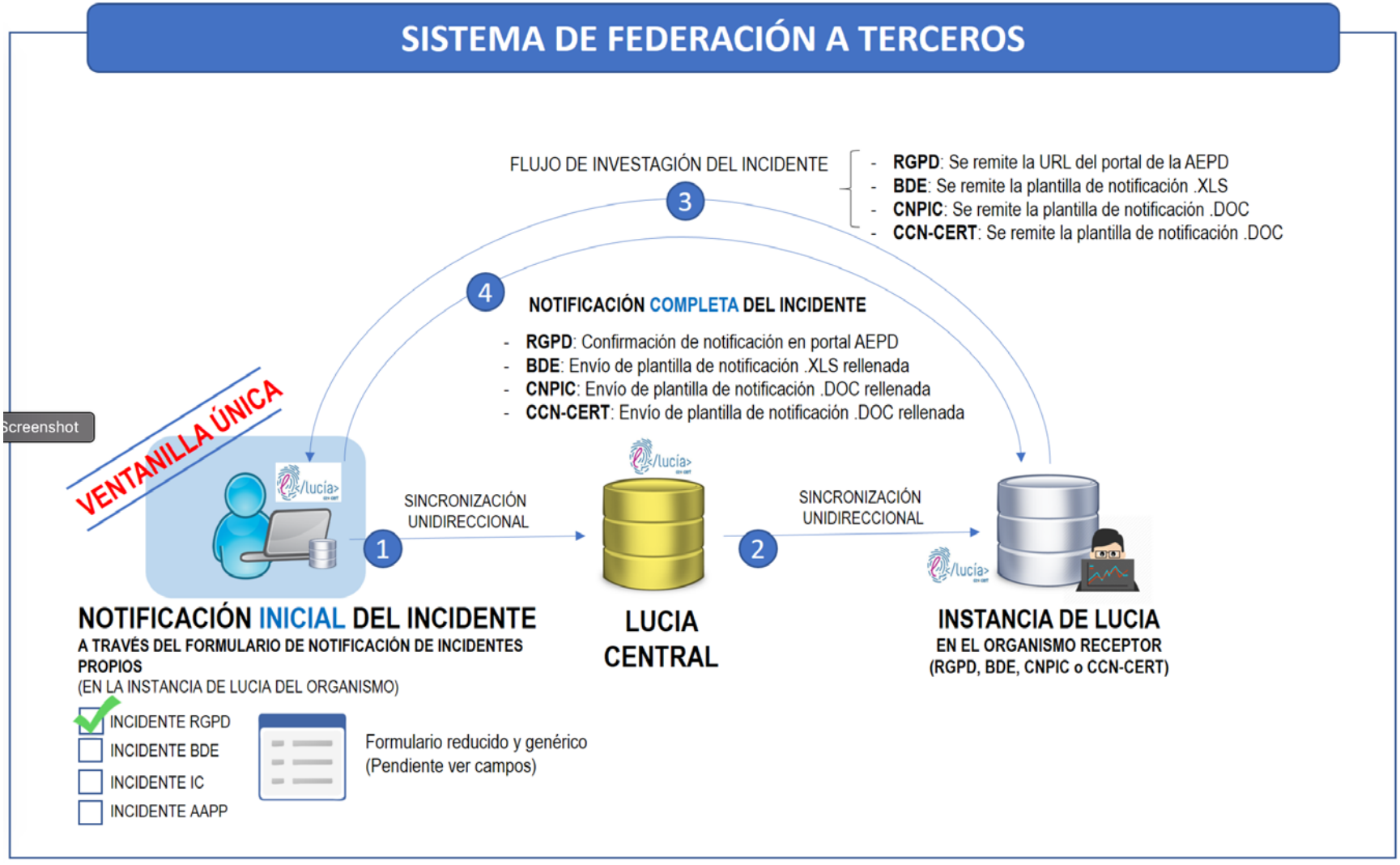
3. En situaciones excepcionales, añada un indicador ALTO o CRÍTICO:
- Puede ser aplicado a cualquier categoría o incidente
- Se utiliza en circunstancias excepcionales cuando se requieren mayores recursos o una respuesta rápida de emergencia



Cómo utilizar la matriz de clasificación

CCN centro criptológico nacional

LUCIA. REPORTE A TERCEROS



LUCIA. VIRTUAL SOC

VSOC :centro de operaciones de seguridad que centraliza las acciones y monitorizaciones de varios organismos en materia de seguridad.

Características: Está orientado a entidades locales para que puedan conocer su superficie de exposición y optimicen sus recursos en función de la información que manejan y los servicios que prestan.

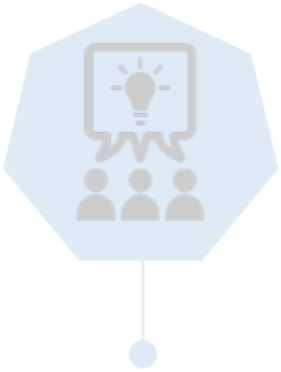
Objetivos: Mejorar las capacidades de despliegue, actuación y protección de las entidades.

PROYECTO: Con una sola instancia de LUCIA, se podrá dar servicios a varios organismos para:

- Agrupar los incidentes y tener sus propias estadísticas.
- Tener mayor visibilidad sobre incidentes.
- Interconectar con LUCIA central la arquitectura VSOC

LUCIA. VIRTUAL SOC. Ventajas

socccn@ccn-cert.cni.es



Más información de ataques

Mayor visibilidad sobre incidentes

Una sola instancia da servicio a varios organismos

CSIRT.es

Equipos de Seguridad y Gestión de Incidentes españoles

Objetivo: optimizar la cooperación entre los CSIRT de ámbito nacional para actuar frente a problemas de seguridad informática.

Compartir, Cooperar, Divulgar

Intercambio

Coordinación

CCN centro criptológico nacional

Muchas Gracias

E-mails

info@ccn-cert.cni.es

ccn@cni.es

sondas@ccn-cert.cni.es

redsara@ccn-cert.cni.es

organismo.certificacion@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es