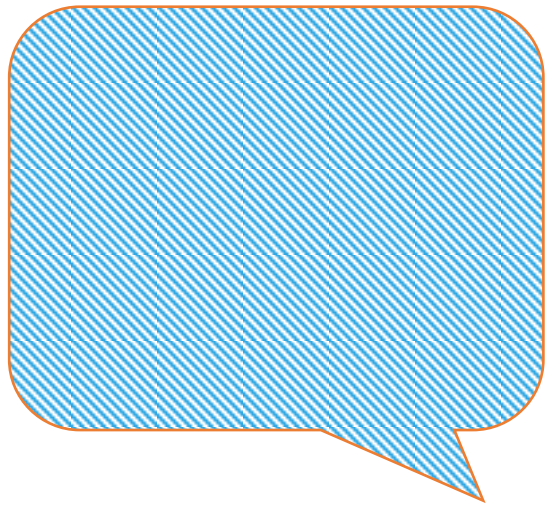
LUCIA: Experiencia de federación

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL



- Francisco J. Sampalo Lainz
- CRUE – Universidades españolas
- paco.sampalo@si.upct.es

Índice

LUCIA: Experiencia de federación

Informe INES (CCN-CERT IT 40/16)

- Visión del estado de la ciberseguridad focalizado en las Universidades públicas españolas.

op.pl	op.acc	op.exp	op.ext	op.cont	op.mon	Marco Operacional (Global)
29	66	69	53	25	35	**51**
40	52	32	20	-	38	**36**
48	89	69	13	20	34	**47**
33	45	33	27	3	33	**29**
34	70	60	60	30	35	**44**
65	81	68	67	30	33	**53**
2	13	18	20	0	35	**15**
25	25	23	23	2	33	**22**
14	19	21	23	10	36	**21**
20	32	23	23	2	17	**20**
75	61	59	75	75	37	**64**
46	66	49	32	5	36	**37**
28	34	34	30	20	38	**31**
42	54	51	66	0	38	**42**
26	43	53	37	30	36	**35**
33	**52**	**49**	**30**	**15**	**35**	**36**

Figura 14.- Resultados medidas operacionales agrupadas por comunidad autónoma

LUCIA: Experiencia de federación

Informe INES (CCN-CERT IT 40/16)

Proceso de Autorización	53	23	50	32	24	50	10	5	0	8	90	9	24	55	60	**24**
Análisis de Riesgos	50	100	30	50	15	70	0	25	0	25	75	80	53	50	0	**50**
Gestión de Derechos de Acceso	70	54	90	50	50	100	20	25	23	45	75	83	40	50	50	**50**
Gestión de Incidentes	90	50	68	44	40	100	13	19	12	35	75	40	5	28	80	**40**
Concienciación y Formación	28	39	50	31	19	68	5	25	3	25	20	25	14	27	30	**25**
Configuración	50	14	35	39	70	55	10	25	20	26	25	51	13	34	50	**34**
Gestión de cambios	71	12	55	32	60	60	12	25	29	28	37	52	40	39	80	**39**
Continuidad de operaciones	38	70	28	17	35	45	3	14	15	7	57	19	36	65	38	**35**
Global	**56**	**45**	**51**	**37**	**39**	**68**	**9**	**20**	**13**	**25**	**57**	**45**	**28**	**43**	**49**	**43**

Figura 20.- Resultados de cumplimiento en relación a los procesos críticos

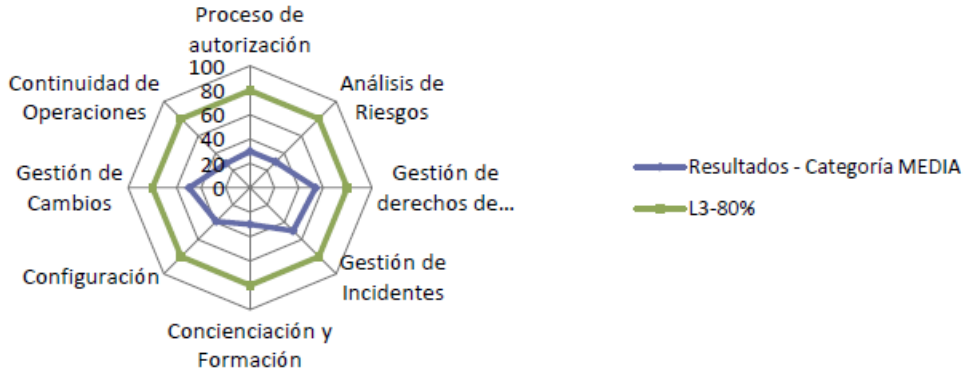


Figura 22.- Resultados de cumplimiento de los procesos críticos para sistemas de categoría MEDIA

LUCIA: Experiencia de federación

Informe INES (CCN-CERT IT 40/16)

- Las medidas sobre las que se recomienda emplear mayores recursos son las asociadas a:
  - El análisis de riesgos y declaraciones de aplicabilidad.
  - La existencia de normativa y procedimientos de seguridad.
  - La concienciación y formación.
  - La continuidad de la operación de los sistemas.

Informe Ejecutivo CCN-CERT IT-40/16

7. RECOMENDACIONES

3. Reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados según se recoge en la Estrategia de Ciberseguridad Nacional con la aprobación de los recursos extraordinarios que se reflejan en los planes derivados aprobados en julio de 2015.

LUCIA: Experiencia de federación

Universidades españolas

- CRUE → Sectorial CRUE-TIC → GT eAdmon → Subgrupo de Seguridad
  - Este subgrupo coordina acciones de seguridad conjuntas para las Universidades y la relación con el resto de las AAPP.

- Al ser conscientes de esta “debilidad” se ha promovido el uso de LUCIA y SATINET entre las Universidades.
  - 10 universidades en SATINET.
  - 3 universidades utilizando LUCIA; 1 en proceso de instalación.
  - 3 con sonda SATINET integrada con LUCIA.

crue Universidades Españolas TIC

LUCIA: Experiencia de federación

Auditoría ENS en la UPCT

- En abril de 2015 la Universidad Politécnica de Cartagena realiza una auditoría de cumplimiento del ENS.
- Se detectan insuficiencias severas en las medidas de explotación (OP.EXP), lo que deriva en acciones concretas para nuestro plan de seguridad.

Op.exp.1	Gestión del inventario	Aplica. Medio.	50%
Op.exp.2	Configuración de la seguridad	Aplica. Medio.	10%
Op.exp.3	Gestión de la configuración de seguridad	Aplica. Medio.	10%
Op.exp.4	Mantenimiento	Aplica	10%
Op.exp.5	Cambios	Aplica. Medio.	50%
Op.exp.6	Protección frente a código dañino	Aplica	50%
Op.exp.7/9	Gestión de incidencias de seguridad	Aplica. Medio.	10%
Op.exp.8	Registros de actividad	Aplica. Medio.	90%
Op.exp.10	Protección de registros de actividad	No Aplica	
Op.exp.11	Claves criptográficas	Aplica. Medio.	10%

6.2.15.- Gestión de incidencias de seguridad [op.exp.7/9]

Sistemas afectados	Todos los sistemas afectados por el ENS
Nivel de Aplicabilidad	Aplica a nivel MEDIO
Madurez exigible	L3
Madurez evaluada	L1

LUCIA: Experiencia de federación

Federación LUCIA-SATINET (UPCT)

- Después de haber hecho pruebas de la aplicación y definir un procedimiento para gestión de los incidentes de seguridad, en Febrero de 2016 empezamos a usar LUCIA.
- En Abril de 2016 nos adherimos a SATINET.
- En Junio de 2016 tenemos ya los dos sistemas federados.

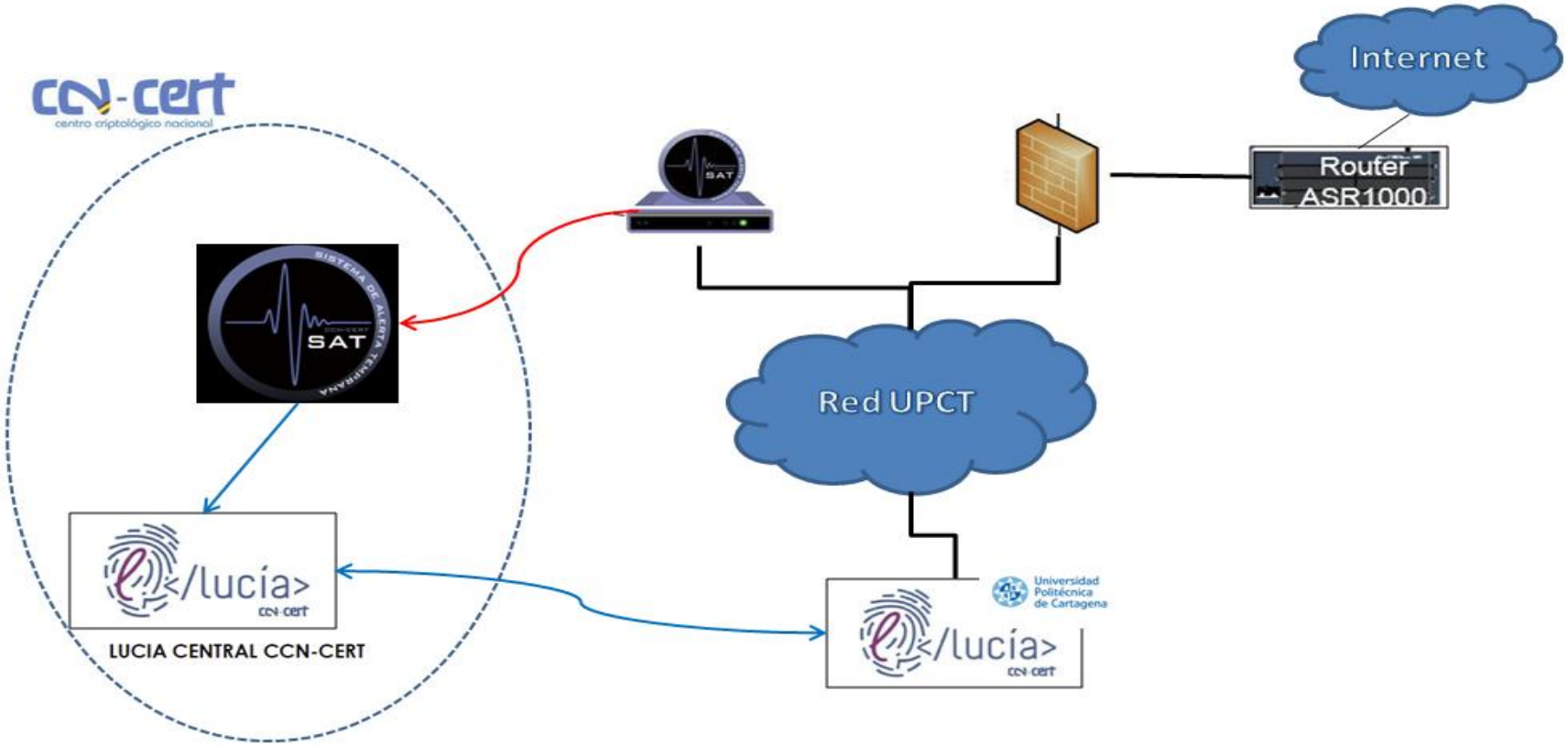
LUCIA: Experiencia de federación

Federación LUCIA-SATINET (UPCT)

- Se crean usuarios para la sincronización (interfaz REST) entre LUCIAs (Central e instancia propia).
  - Estos usuarios deben ser “transparentes” y no se deben gestionar los incidentes con ellos.
- Se crea una constituency (visibilidad), diferenciada de la propia de la institución, en la que podemos gestionar los incidentes de SATINET.
- Hay que dar permiso a nuestros usuarios locales para que puedan tener visibilidad de los incidentes SATINET.
- Los incidentes SATINET deben resolverse en nuestra instancia de LUCIA desde los usuarios locales.
- Algunos problemas para la configuración correcta del envío de correos (notificaciones).
- **Guías CCN-STIC 845 (Manuales)**

LUCIA: Experiencia de federación

Federación LUCIA-SATINET (UPCT)



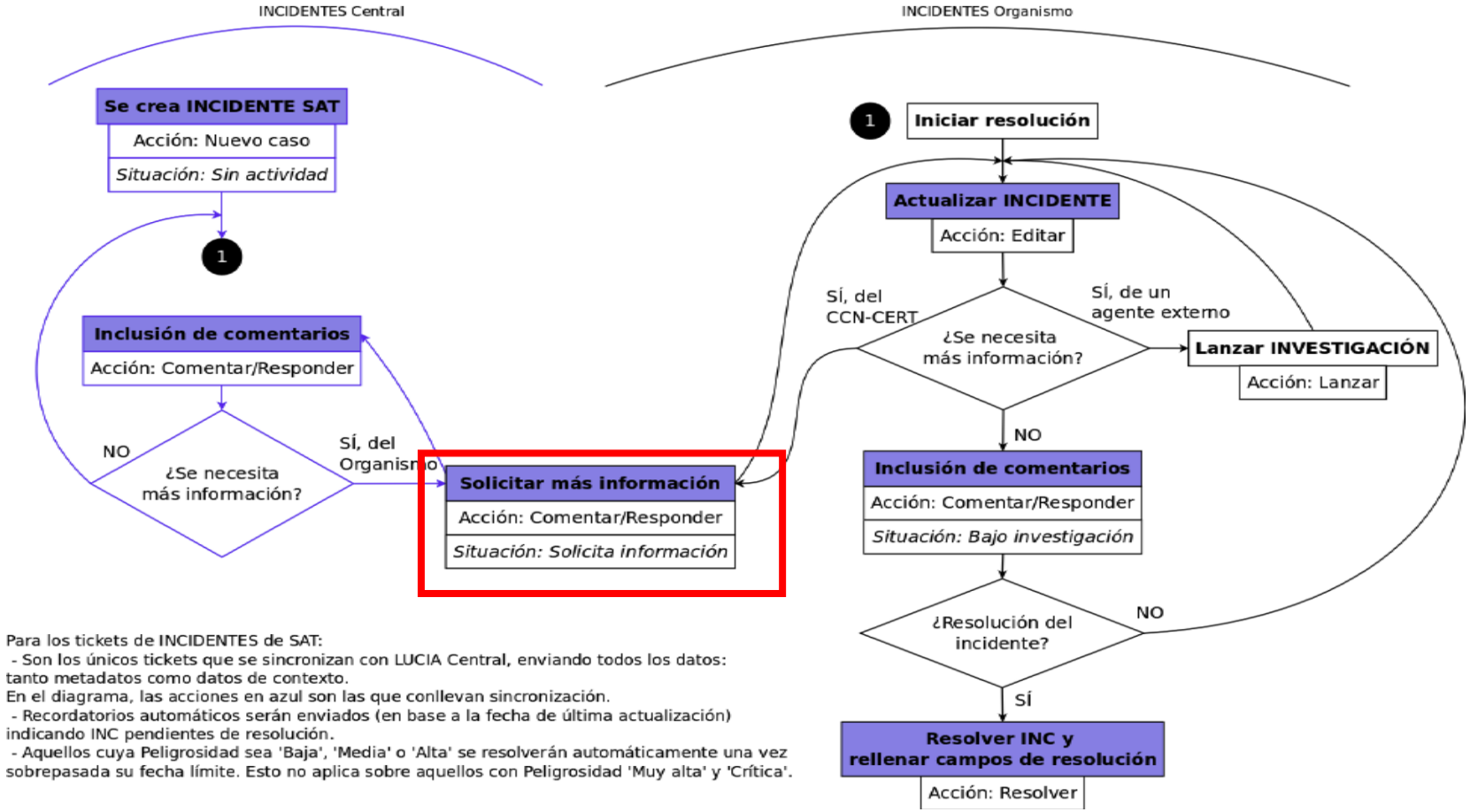
LUCIA: Experiencia de federación

Gestión unificada de incidentes (UPCT)

1. **Detección y Reporte**: desde nuestro help-desk o por los técnicos o a través de herramientas. Por sonda SATINET.
2. **Alta y clasificación**: considerar o no el aviso, introducir metadatos y asignar técnico responsable.
3. **Seguimiento y resolución**: implicando e informando a otras áreas de la Universidad si es necesario.
4. **Cierre:** comunicar, documentar y enlazar con Gestión del Cambio.

LUCIA: Experiencia de federación

Gestión unificada de incidentes



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'.

LUCIA: Experiencia de federación

Gestión unificada de incidentes

Se crea INCIDENTE SAT

Acción: Nuevo caso

Situación: Sin actividad

Incidente #642: [SAT-INET] Detectado posible Ransomware Locky - UPCT

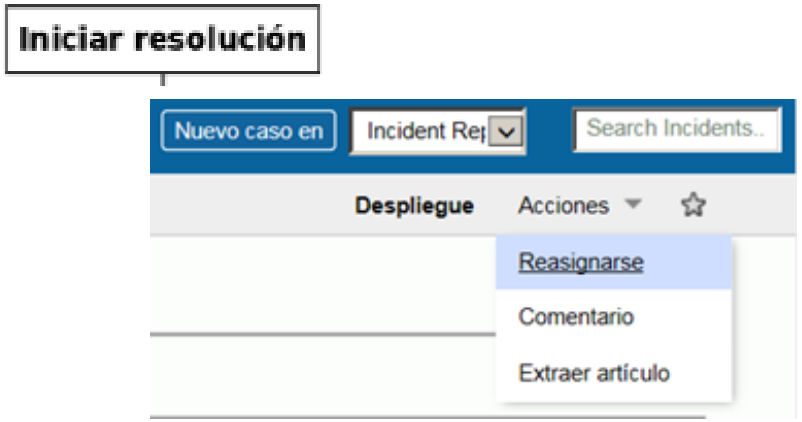
Metadatos del caso

Incidente #642

Asunto:	[SAT-INET] Detectado posible Ransomware Locky - UPCT
Propietario:	satinet_ccn-cert (REST SATINET_CCN-CERT)
Visibilidad:	SATINET_CCN-CERT
Peligrosidad:	Medio
Estado:	abierto
Descripción:	Incidente

LUCIA: Experiencia de federación

Gestión unificada de incidentes



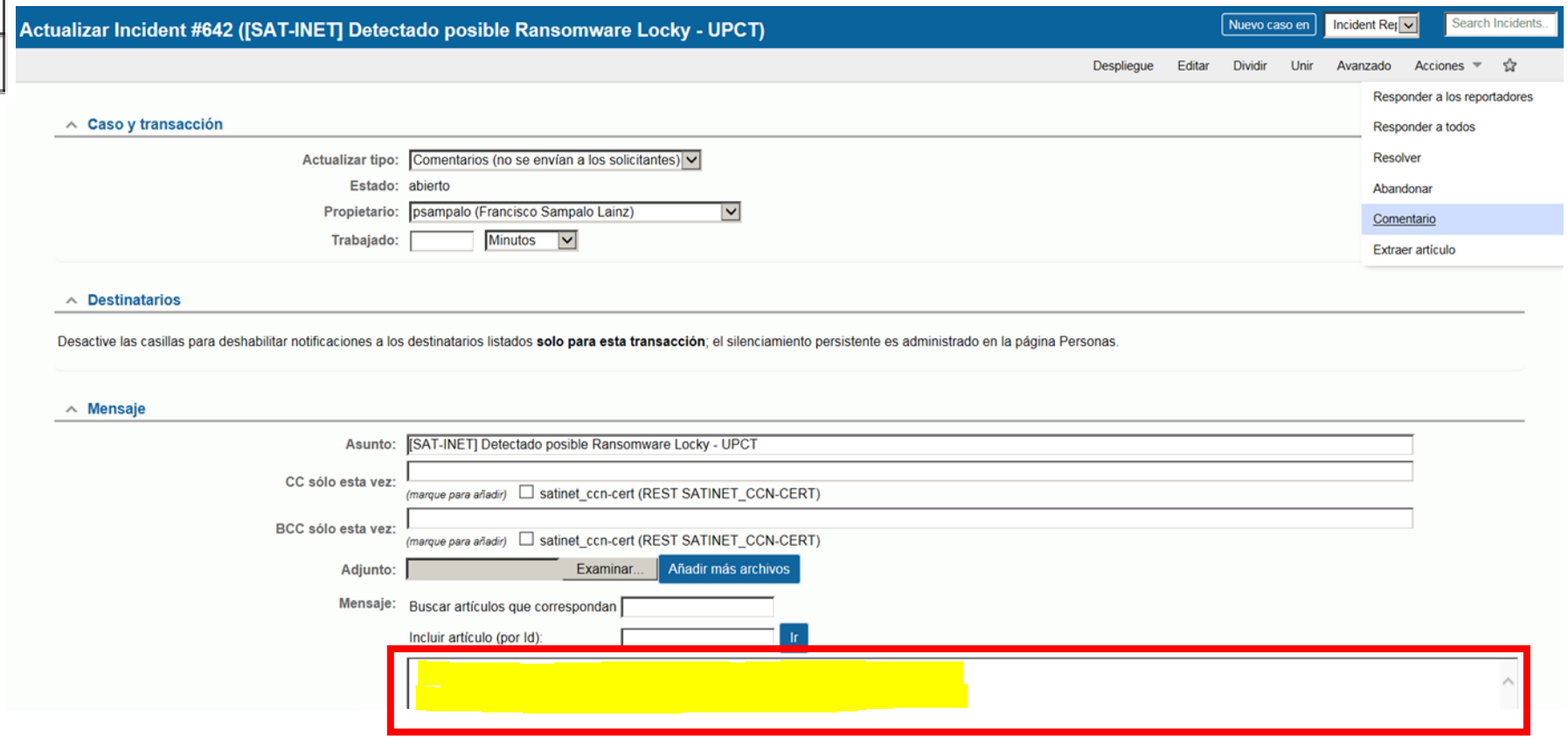
LUCIA: Experiencia de federación

Gestión unificada de incidentes

Inclusión de comentarios

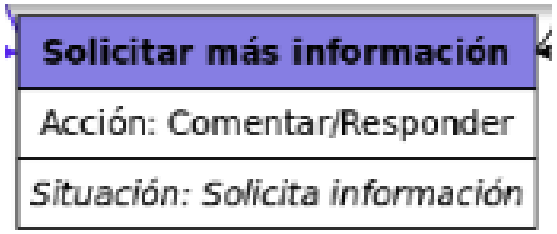
Acción: Comentar/Responder

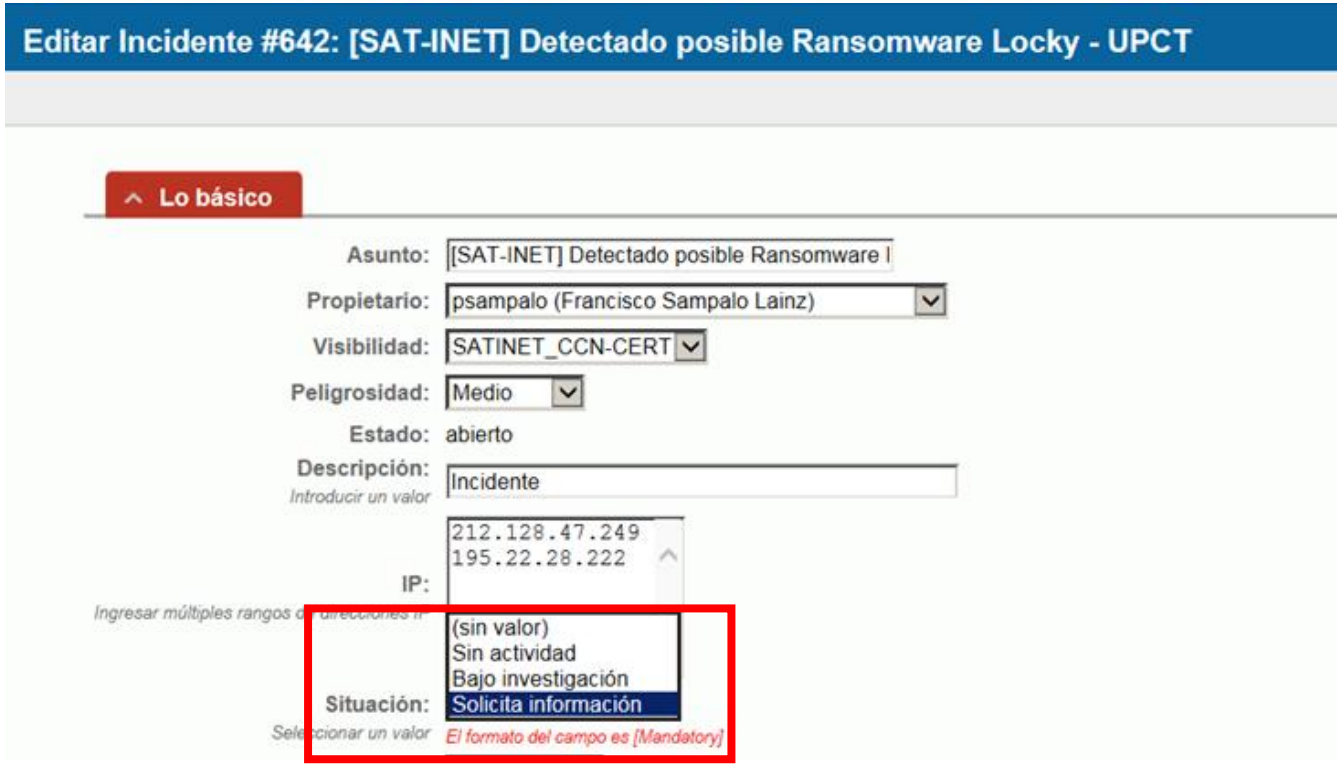
Situación: Bajo investigación



LUCIA: Experiencia de federación

Gestión unificada de incidentes



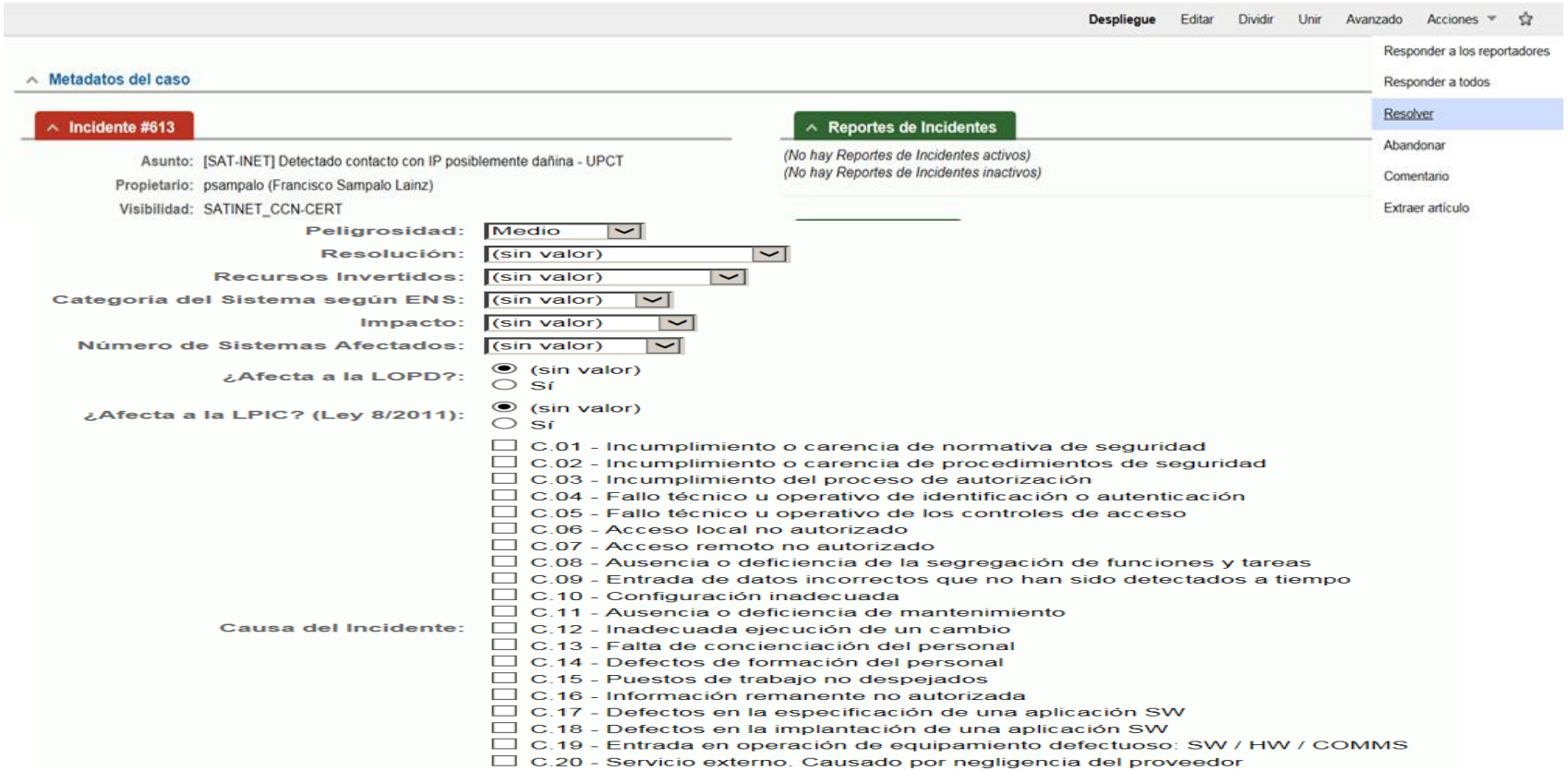


LUCIA: Experiencia de federación

Gestión unificada de incidentes

Resolver INC y rellenar campos de resolución

Acción: Resolver



LUCIA: Experiencia de federación

Sincronización de incidentes

- **Incidentes propios**: metadatos, excepto: asunto, el cuerpo, la descripción, campaña, origen de la amenaza.
- **Incidentes SAT**: todos los metadatos.
- No se sincronizan: “Incidents Reports” ni “Investigaciones”.

LUCIA: Experiencia de federación

Sincronización de incidentes

- **La sincronización se ejecuta en el mismo momento en que se crea, actualiza o resuelve un incidente.**
- En caso de fallo, se reintenta hasta (un máximo de 3 veces) y si persiste el fallo queda encolada, para evitar inconsistencias.
- Existe un proceso "cron" nocturno para revisar todas las peticiones de sincronización pendientes que las ejecuta.
- En caso de error y restauración de la conectividad, un sistema federado correctamente tardaría un máximo de 24 horas en sincronizar completamente su instancia de forma automática.

LUCIA: Experiencia de federación

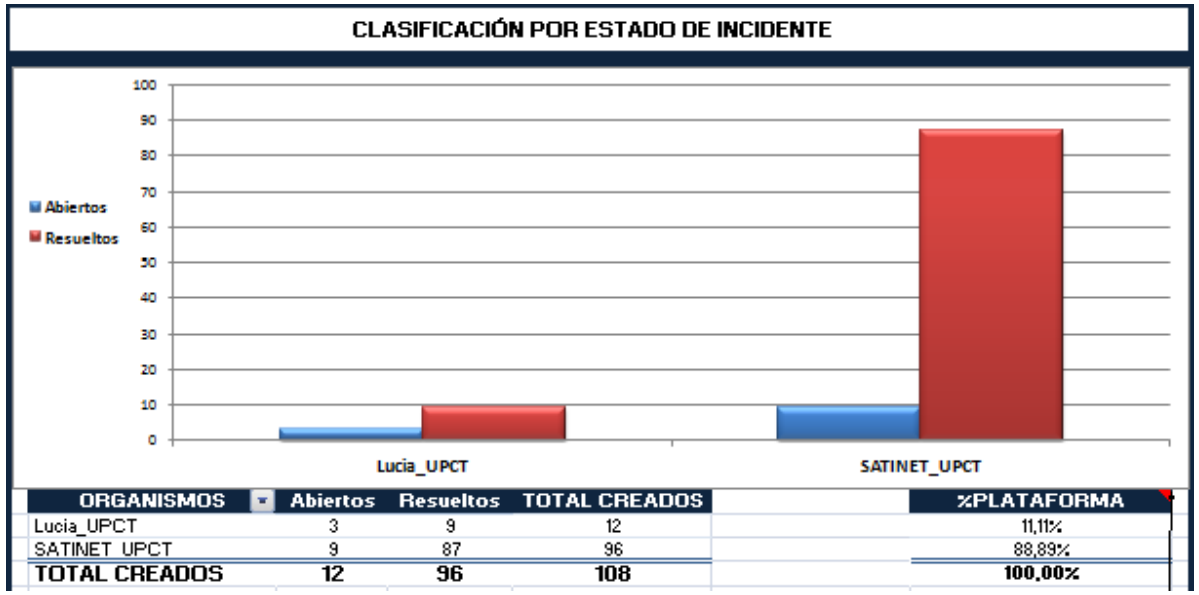
Explotación de la información en LUCIA

- LUCIA permite la extracción de la información completa de los tickets (incidentes) en formato XML.

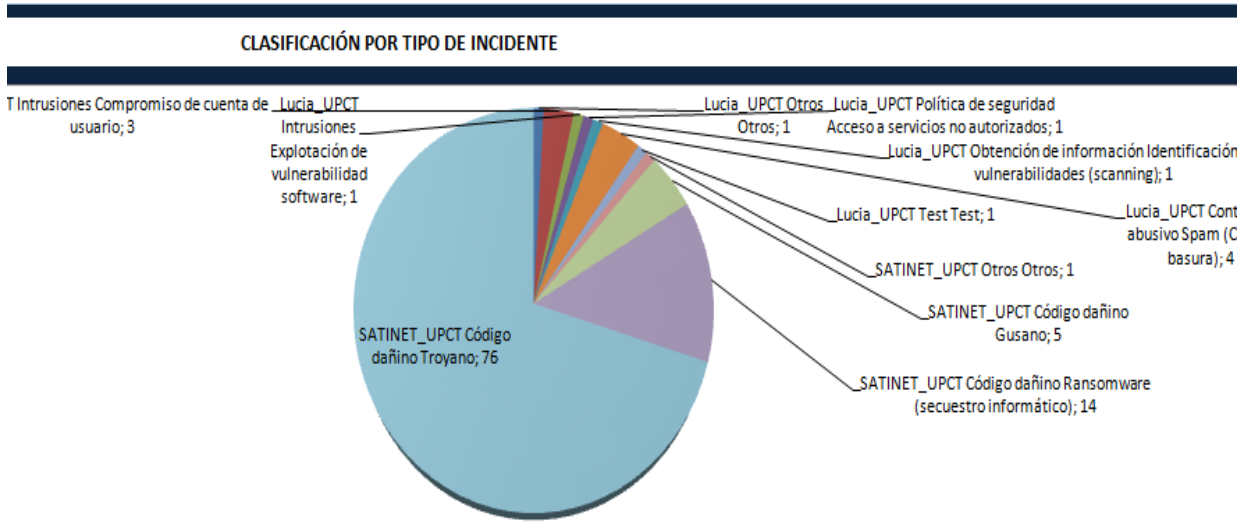
- Esto facilita:
  - Tratamiento y análisis de los datos en hoja de cálculo.
  - **Importación de los datos en INES para obtención automática de indicadores**.

LUCIA: Experiencia de federación

Datos LUCIA – Universidad (UPCT)

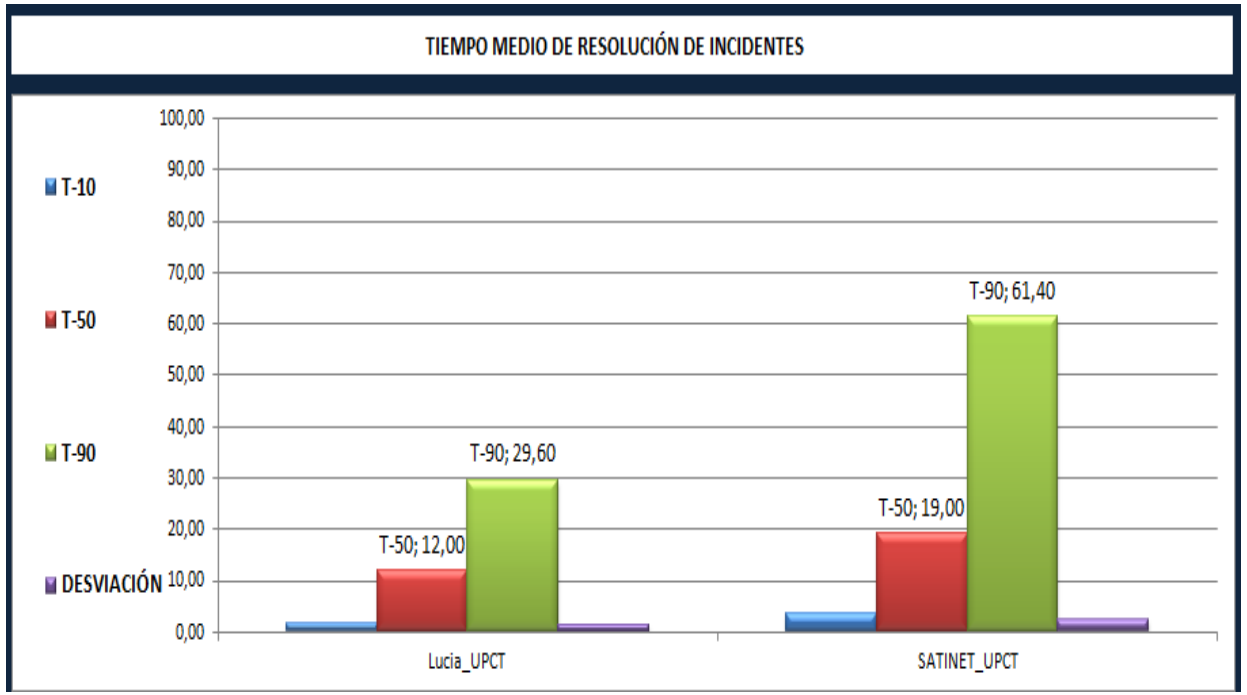


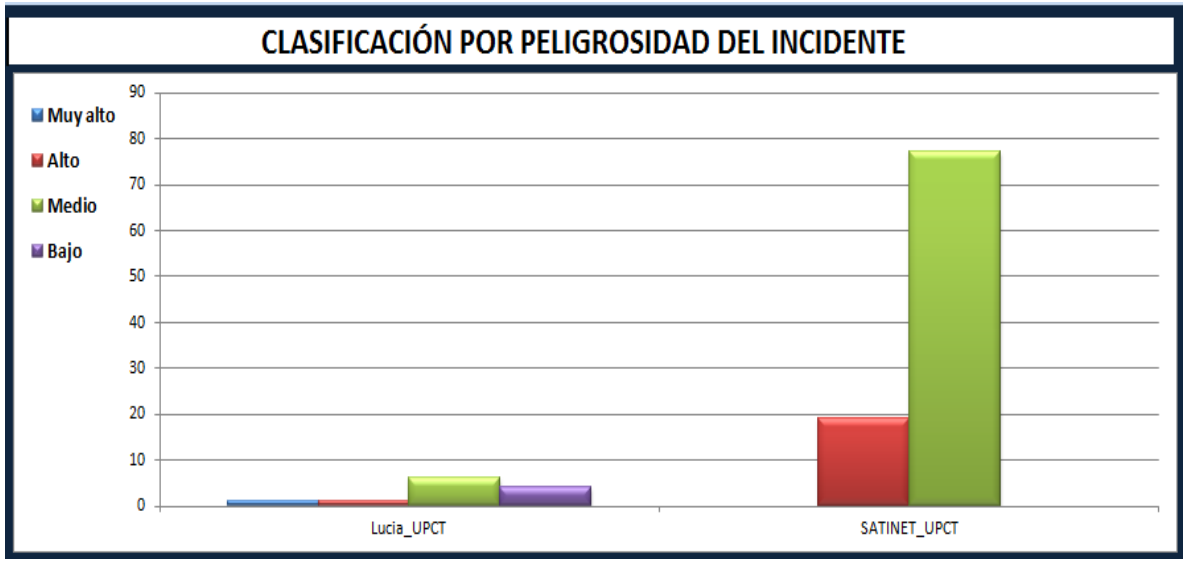
ORGANISMOS	Abiertos	Resueltos	TOTAL CREADOS	%PLATAFORMA
Lucia_UPCT	3	9	12	11,11%
SATINET_UPCT	9	87	96	88,89%
TOTAL CREADOS	**12**	**96**	**108**	**100,00%**



LUCIA: Experiencia de federación

Datos LUCIA – Universidad (UPCT)





LUCIA: Experiencia de federación

Informe INES (CCN-CERT IT 40/16)

- La federación LUCIA-SATINET es muy positiva para la gestión de la Seguridad:
    - Facilita la coordinación interna (propio CSIRT) y con el CCN-CERT.
    - Facilita el control por parte del Responsable de Seguridad.
    - Generación de información:
        - históricos de incidentes
        - Indicadores INES
    - Proceso sencillo y práctico.
    - Cumplimiento legal (ENS)

Gracias por su atención

Grupo de Trabajo de Administración Electrónica
CRUE – Comisión Sectorial TIC (http://www.crue.org/TIC/)

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@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