GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 845A

LUCIA – Manual de Usuario

octubre 2020

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

NIPO: 002-16-001-9

Fecha de Edición: octubre de 2020

El CCN y CSA han participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de enero de desarrollo del Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Febrero de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El siguiente documento desarrolla el procedimiento de gestión de *ticketing* o casos de Incidentes propios o casos de Sistemas de Alerta Temprana (SAT) mediante la herramienta LUCIA.
2. En su lectura debe tenerse en cuenta lo siguiente:
   - La gestión de incidentes propios solo puede llevarse a cabo si se posee una instancia de LUCIA propia federada.
   - La gestión de incidentes de SAT se puede llevar a cabo tanto en una instancia federada como en LUCIA Central.
   - En el caso de organismos no federados, éste poseerá un usuario diferenciado para cada una de las sondas SAT. Esto significa que los incidentes de una sonda SAT no pueden ser gestionados por el usuario de la otra y viceversa. En el caso de querer unificarlos, deberá consultar con el CCN-CERT.
   - En el caso de organismos no federados, si se requiere de un usuario de visualización de solo lectura sin posibilidad de modificación sobre los casos, también se habrá de consultar con CCN-CERT.

2. CONCEPTOS BÁSICOS DE RTIR/LUCIA

4. LUCIA es un sistema de gestión de *ticketing* o casos, basado en RT[1] y RTIR[2] que permite el seguimiento, notificación y trazabilidad de diferentes tipos de tickets, descritos con más detalle a continuación.

5. En resumen, LUCIA permite a un usuario crear una incidencia, y como consecuencia de ello, un equipo de soporte se encarga de su revisión, y según sus criterios, proceda a su aprobación, rechazo, realice las comprobaciones y trabajos necesarios asociados a la incidencia para finalmente proceder al cierre de la incidencia. Para ello, a través de LUCIA, el equipo puede solicitar información al usuario que notificó la incidencia (reportador), añadir información a la incidencia o iniciar una investigación con terceras partes para tratar de resolver o investigar un hecho en concreto relacionado con la misma.

6. A continuación, se detallan conceptos básicos que permiten entender la estructura y el funcionamiento de LUCIA.

2.1. TICKETS O CASOS

7. *Tickets* o *Casos* son la unidad básica de información de LUCIA. Un ticket está formado por varios atributos descriptivos que le dotan de información y por otros atributos que conforman su *metainformación* (i.e., información para su gestión).

8. Cabe destacar el concepto de *Cola*, en torno al cual se organizarán los permisos para que los usuarios puedan visualizar, editar o resolver tickets.

2.2. COLAS

9. Una *cola* es la unidad organizativa de tickets en LUCIA. Es un listado lógico donde se agrupan los tickets que, bien por temática o por tipo, deben agruparse. Las colas permiten y facilitan la gestión de los tickets, permitiendo el acceso, u otros permisos, a ciertos usuarios y denegándoselos a otros. En las colas es donde se definen qué atributos de información tendrán los tickets que en ellas se alojen.

10. Cada cola tiene asignado un ciclo de vida, donde se definen los estados en los que se pueden encontrar los tickets de dicha cola y las posibles transiciones entre ellos, así como de un granulado más finos de permisos necesarios para poder pasar de un estado a otro. LUCIA incorpora cuatro ciclos de vida propios: *LUCIA_incidents*, *LUCIA_SAT_incidents*, *LUCIA_incident_reports* y *LUCIA_investigations*. Con ellos se consigue una mayor flexibilidad a la hora de personalizar las colas de los tickets de LUCIA, así como no interferir con el funcionamiento habitual de las colas de RT o RTIR.

11. En LUCIA se definen cuatro tipos de tickets[3]: Incidentes (propios), Incidentes SAT, Reportes de incidentes, e Investigaciones. Todos ellos están bien diferenciados entre sí, a excepción de los Incidentes SAT y los Incidentes propios, que solo se diferencian en pequeños matices.

[1] Request Tracker. https://www.bestpractical.com/rt
[2] Request Tracker for Incident Response. https://www.bestpractical.com/rtir
[3] Esta clasificación estará disponible a partir de la actualización de LUCIA REV4.0

12. Para todos ellos, en el menú superior derecho se pueden seleccionar las dos vistas disponibles en las que se encuentran los campos asociados, así como la posibilidad de modificar sus valores:
    - **Mostrar**: Muestra el contenido del ticket junto con su Historial, pero sólo de aquellos campos que hayan sido cumplimentados.
    - **Editar**: Permite editar los valores de todos los campos sobre los que tenemos permisos.
    - **<<Primero**: Permite ir al primer ticket si se tiene permiso para ver el ticket.
    - **<Anterior**: Permite ir al ticket anterior si se tiene permisos para ver el ticket.
    - **Siguiente>**: Permite ir al siguiente ticket si se tiene permiso para ver el ticket.
    - **Último>>**: Permite ir al último ticket si se tiene permiso para ver el ticket.

2.2.1. REPORTE DE INCIDENTE (INCIDENT REPORT)

13. Todo correo recibido en el buzón monitorizado por LUCIA genera automáticamente un Reporte de Incidente (IR). Del mismo modo, puede ser creado desde la propia aplicación por un usuario si, por ejemplo, la notificación fue recibida por otro medio como el teléfono o el fax.
14. Los Reportes de Incidentes, al poder provenir de usuarios de cualquier nivel técnico, han de ser evaluados con el fin de confirmar que realmente suponen un incidente. Un Reporte de Incidente puede o no, dar lugar a un Incidente, en el caso de que el grupo de revisión asignado así lo defina. En el caso de que sí sea un incidente, el Reporte podrá ligarse al Incidente.
15. Un mismo Reporte de Incidente puede dar lugar a varios Incidentes y un mismo Incidente puede estar asociado a varios Reportes de Incidentes. Por tanto, que un Reporte de Incidente se resuelva, no indica que el Incidente se haya resuelto.
16. El Reporte de Incidente permite una vía de comunicación con la persona que informó del problema de forma independiente del resto de Reportes de Incidentes y de las posibles Investigaciones que pudieran originarse.
17. El orden de aparición de los siguientes campos está tomado desde el punto de vista de la creación del Reporte de Incidente por lo que puede diferir de la vista *'Mostrar'* del Reporte de Incidente. Los atributos disponibles son:
    - **Incidente**: Identificadores de los Incidentes a los que se encuentra vinculado.
    - **Cola**: Cola donde se crea el incidente.
    - **Estado**: Identifica si se encuentra abierto o cerrado. Por defecto es 'abierto'.

- **Propietario**: Usuario propietario del ticket.
- **Cómo se reportó**: Medio de comunicación origen del reporte.
- **Tipo de reportador**: Clasificación del organismo reportador.
- **Corresponsales**: Usuarios o direcciones de correo solicitantes.
- **Cc**: Usuario o direcciones de correo que recibirán copia de las mismas respuestas al caso que reciba el *Corresponsal* o *Solicitante*.
- **Admin Cc**: Misma característica que el *Cc* pero con permiso para modificar el caso.
- **Asunto**: Texto que identifica el Reporte de Incidente.
- **Mensaje**: Contenido del mensaje del Reporte de Incidente visible como primera entrada en el *Historial* en la vista *'Mostrar'*.
- **Adjunto**: Ficheros adjuntos de relevancia.
- **Fechas**: Fecha de comienzo y límite del Reporte de Incidente.
- **Tiempo**: Tiempo estimado, trabajado y restante del Reporte de Incidente.

18. En la gestión de Incidentes SAT **no** se utilizan Reportes de Incidentes.

2.2.2. INVESTIGACIÓN (INVESTIGATION)

19. Una Investigación es una forma de iniciar un canal de comunicación con usuarios externos e independientes a los Reportes de Incidentes. Una Investigación es una unidad de información asignada a un incidente que se crea en caso de que se necesite ampliar información de un problema en concreto y, para ello, el equipo asignado debe ponerse en contacto con ciertas personas, organizaciones o autoridades, ajenas al usuario que informó el problema a través del reporte.
20. Que una Investigación se resuelva, no indica que el Incidente se haya resuelto, por lo que puede haber varias Investigaciones ligadas al mismo incidente. Sin embargo, una Investigación sólo puede estar ligada a un Incidente.
21. El orden de aparición de los siguientes campos está tomado desde el punto de vista de la creación de una Investigación por lo que puede diferir de la vista *'Lanzar'* de la investigación. Los atributos propios de una Investigación son:
    - **Incidente**: Identificador del incidente al que se encuentra vinculado.
    - **Cola**: Cola donde se crea el incidente.
    - **Estado**: Identifica si se encuentra abierto o cerrado. Por defecto es *'abierto'*.
    - **Propietario**: Usuario propietario del ticket.

- **IP**: Direcciones IP asociadas a la Investigación. En la creación se puede dejar vacío y el sistema es capaz de extraerlas automáticamente del *Mensaje*. Sin embargo, aquellas direcciones IP que se deseen incorporar posteriormente, deberán ser agregadas manualmente o mediante el enlace correspondiente que aparece con la etiqueta `[Añadir IP]` junto a una dirección IP detectada por el sistema en un texto contenido en un comentario del *Historial*.
- **Corresponsales**: Usuarios o direcciones de correo destinatarios.
- **Cc**: Usuario o direcciones de correo que recibirán copia de las mismas respuestas al caso que reciba el *Corresponsal* o *Solicitante*.
- **Admin Cc**: Misma característica que el *Cc* pero con permiso para modificar el caso.
- **Asunto**: Texto que identifica la Investigación.
- **Mensaje**: Contenido del mensaje de la Investigación visible como primera entrada en el *Historial* en la vista *'Mostrar'*.
- **Adjunto**: Ficheros adjuntos de relevancia.
- **Fechas**: Fecha de comienzo y límite de la Investigación.
- **Tiempo**: Tiempo estimado, trabajado y restante de la Investigación.

22. En la gestión de Incidentes SAT **no** se permite iniciar flujos de Investigaciones por parte de los operadores del CCN-CERT.
23. En la gestión de Incidentes SAT **no** se permite iniciar flujos de Investigaciones por parte del organismo en LUCIA Central.

2.2.3. INCIDENTE (INCIDENT) E INCIDENTE SAT (SAT INCIDENT)

24. Un Incidente es el tipo de ticket que representa el propio Incidente y vincula aquellos Reportes de Incidentes e Investigaciones con los que se encuentra relacionados.
25. Dispone de los atributos necesarios para permitir almacenar la información necesaria sobre el Incidente además de los atributos asociados a la resolución del incidente y el tiempo empleado para ello.
26. A diferencia de los objetos anteriores, la resolución de un Incidente cerrará en cascada todos los Reportes de Incidentes e Investigaciones relacionadas, dándose por concluida la gestión del caso.
27. **El Incidente es el único objeto susceptible de sincronización con LUCIA Central**.
28. El orden de aparición de los siguientes campos está tomado desde el punto de vista de la creación del Incidente por lo que puede diferir de la vista *'Mostrar'* del Incidente. Los atributos propios de un Incidente son:

- **Asunto**: Campo obligatorio. Texto que identifica el Incidente
- **Mensaje**: Contenido del mensaje del Incidente visible como primera entrada en el *Historial* en la vista *'Mostrar'*.
- **Adjunto**: Ficheros adjuntos de relevancia.
- **Cola**: Cola donde se crea el incidente.
- **Propietario**: Usuario propietario del ticket.
- **Peligrosidad Estimada**: Campo obligatorio. Una vez creado el Incidente **no** se podrá cambiar su valor y **no** será visible a posteriori. Su valor se copia en *Peligrosidad* cuando se crea el Incidente.
- **Peligrosidad**: Campo obligatorio. Su valor inicial se corresponderá con el de *Peligrosidad Estimada* establecida en la creación. Este valor será visible y se podrá modificar en caso de Incidentes propios.
- **Estado**: Identifica si se encuentra abierto o cerrado.
- **Descripción**: Opcionalmente se puede usar este campo para complementar información.
- **IP**: Direcciones IP asociadas al Incidente. En la creación se puede dejar vacío y el sistema es capaz de extraerlas automáticamente del *Mensaje*. Sin embargo, aquellas direcciones IP que se deseen incorporar posteriormente, deberán ser agregadas manualmente o mediante el enlace correspondiente que aparece con la etiqueta `[Añadir IP]` junto a una dirección IP detectada por el sistema en un texto contenido en un comentario del *Historial*.
- **Situación**: Campo obligatorio. Sus posibles valores son:
  - *'Sin actividad'*. Valor inicial al que, una vez editado el Incidente por primera vez, no se podrá volver.
  - *'Bajo Investigación'*: Valor que indica que el Incidente está siendo gestionado.
  - *'Solicita Información'*: Valor que indica que el Incidente está a la espera de complementarse con alguna información, por ejemplo, de la respuesta a una Investigación iniciada.
- **Tipo de Notificación**: Campo obligatorio. El valor *'Incidente'*, se emplea para categorizar un ticket como incidente de seguridad. El valor *'Información'*, es un campo derivado de la estructura de RT y se puede usar cuando se trata de informar de una alerta o aviso a ciertos usuarios, pero sin llegar a ser un incidente.

- **Tipo de Organismo**: Comunidad de usuarios a la que pertenece el organismo involucrado en el Incidente.
- **Clase del Ciberincidente**: Campo obligatorio. Sus definiciones pueden consultarse en la guía *CCN-STIC 817*.
- **Tipo del Ciberincidente**: Campo obligatorio. Sus definiciones pueden consultarse en la guía *CCN-STIC 817*.
- **Nivel de Clasificación**: Campo obligatorio. Dependerá del sistema afectado.
- **Fiabilidad**: Campo obligatorio. Valoración de la confianza de la notificación.
- **Origen de la Amenaza**: Valores personalizados por el propio organismo.
- **Campaña**: Valores personalizados por el propio organismo.
- **Reglas de detección**: Las reglas que ha aplicado la sonda para detectar el incidente.
- **Fechas**: Destaca el valor de la *'fecha límite'* que define el tiempo máximo de gestión de un Incidente y que se establece de forma automática en función de la *'Peligrosidad'*.
- **Historial**: Muestra la información del Incidente, así como de los comentarios derivados de la gestión del mismo por parte del organismo.

29. Además, se muestran también los campos de resolución que deben editarse antes de *'Resolver'* un Incidente para categorizarlo correctamente:
    - **¿Afecta al RGPD?[4]:** Indica si el Incidente afecta a datos de carácter personal según la LOPD/RGPD.
    - **Notificar a AGPD[5]:** Indica si el incidente debe notificarse automáticamente a la Agencia de Protección de Datos.
    - **Notificar al CNPIC[6]**: Indica si el Incidente afecta a una infraestructura crítica según la Ley Protección de Infraestructuras Críticas.
    - **Categoría del Sistema según ENS**: Campo obligatorio.
    - **Requiere intervención del CCN-CERT[4]**: Indica si el incidente debe ser notificado al CCN-CERT.
    - **Resolución**: Campo obligatorio que indica la conclusión de cierre del Incidente:
        - *'Incidente de seguridad'*: Incidente detectado y resuelto.
        - *'Falso positivo'*: No existe el Incidente notificado.

[4] Este campo estará disponible a partir de la actualización de LUCIA REV2.3
[5] Este campo estará disponible a partir de la actualización de LUCIA REV3.1
[6] Este campo estará disponible a partir de la actualización de LUCIA REV2.4

- *'Falta de información'*: No se puede determinar si existe o no el Incidente.
- *'Sin impacto'*: Incidente detectado, pero sin consecuencias.
- *'Sin respuesta'*: No existe gestión o finalización del Incidente. Es el valor que se asigna al Incidente cuando se ejecuta un autocierre de forma automática tras cumplirse su plazo de resolución (Ver *Autocierres* en la página 42).

– **Recursos Invertidos**: Campo obligatorio

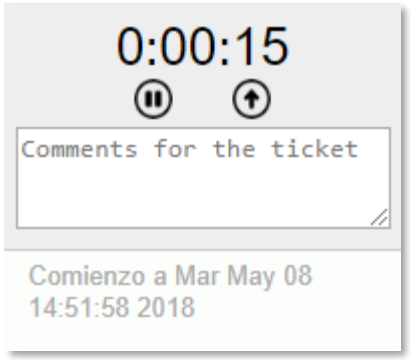
– **Impacto**: Campo obligatorio

– **Causa del Incidente**: Campo obligatorio de selección múltiple.

– **Incidencias durante la Resolución**: Campo obligatorio de selección múltiple.

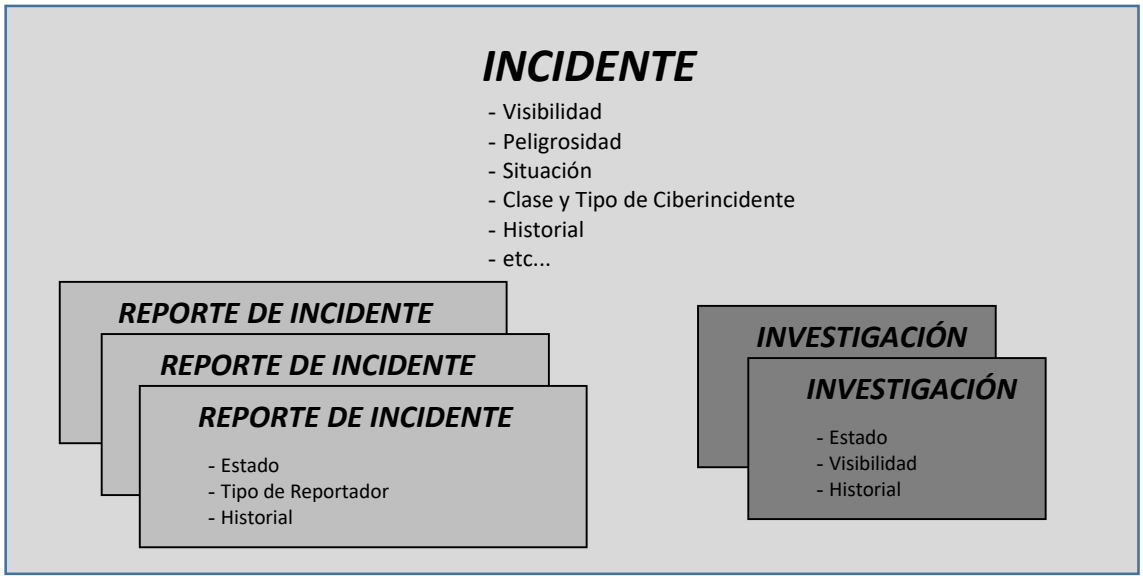
– **Número de Sistemas Afectados**: Campo obligatorio

– **Tiempo trabajado**: Aparece en la inserción de un *'Comentario'* o al *'Resolver'* un Incidente indicando el tiempo dedicado a todo el Incidente. Al menos en la resolución, este valor debe ser cumplimentado para futuros cálculos de métricas. Se ha añadido una nueva funcionalidad que permite cronometrar el tiempo de manera automática para que no tenga que ser introducido a mano. Para ello mientras se esté trabajando en el ticket hay que pulsar sobre el icono del cronómetro de la parte superior izquierda de la pantalla, con lo que nos aparecerá una ventana como la que se muestra a continuación:



Existe la opción de pausar el cronómetro en cualquier momento con el botón de pausa , y actualizar el tiempo trabajado con el botón de subir . Se puede añadir directamente un comentario que se actualizara cuando enviemos el tiempo. La unidad mínima de tiempo a contabilizar es el minuto. Cada vez que se pulsa el botón de subir, el tiempo cronometrado se acumulará al que ya existiera para el ticket. Si rellenamos el campo durante la edición o resolución del ticket, se sobrescribirá el valor que se hubiera calculado y se utilizará ese nuevo valor como base para futuros cálculos del cronómetro.

30. A modo de resumen y relacionando los tres tipos de objetos descritos, un Incidente debe considerarse como un contenedor de Reportes de Incidentes e Investigaciones relacionadas, en los que cada uno de ellos posee una serie de campos que lo define y un histórico de hechos y actuaciones que lo describe.



2.3. CICLO DE VIDA DE UN TICKET

31. Los posibles estados de un ticket son los siguientes:
    - **Nuevo (new)**: Estado por defecto para Reportes de Incidentes que se generan automáticamente cuando se recibe un correo en el sistema.
    - **Abierto (open)**: Estado por defecto al crear un ticket desde la interfaz de LUCIA. En el caso de los Incidentes, lleva asociado el atributo *Situación*, que aporta más información sobre el estado concreto del ticket.
    - **Resuelto (resolved)**: Indica la resolución del ticket. En el caso de los Incidentes, lleva asociado el campo *Resolución* para detallar más información.
    - **Rechazado/Abandonado (rejected/abandoned)**: Indica que el ticket fue rechazado/abandonado.
32. Además, existen en LUCIA varios procedimientos programados para su ejecución automática que completan el ciclo de vida:
    - **Peligrosidad**: Al crear un Incidente se le asigna una *Peligrosidad estimada* que ya no se podrá cambiar. Inicialmente el valor de *Peligrosidad estimada* se copia a *Peligrosidad* que sí es un atributo modificable, y que, en adelante, es el que se utiliza para determinar la fecha límite de resolución del ticket. La comparación de los campos *Peligrosidad estimada* y *Peligrosidad* permite conocer su evolución desde la creación del incidente.

- **Situación**: Al crear un Incidente, este campo se establece a *'Sin actividad'*. Ante cualquier actuación, pasa automáticamente a *'Bajo investigación'*, no pudiendo volver ya nunca al estado *'Sin actividad'*. En este punto, únicamente se permiten los cambios entre *'Bajo investigación'* y *'Solicita información'* o viceversa.
- **Recordatorios**: Cada noche se enviarán recordatorios de aquellos casos cuya fecha límite esté cercana y no tengan una actividad reciente.
- **Autoresolución**: Cada noche se marcarán con *Estado 'Resuelto'* y *Resolución 'Sin respuesta'* aquellos tickets cuya fecha límite haya expirado y no se haya resuelto manualmente. Los casos de peligrosidad *'Muy Alta'* y *'Crítica'* no se verán afectados. Un ticket resuelto puede editarse o reabrirse si se considera necesario.

2.4. FECHAS DE LOS TICKETS

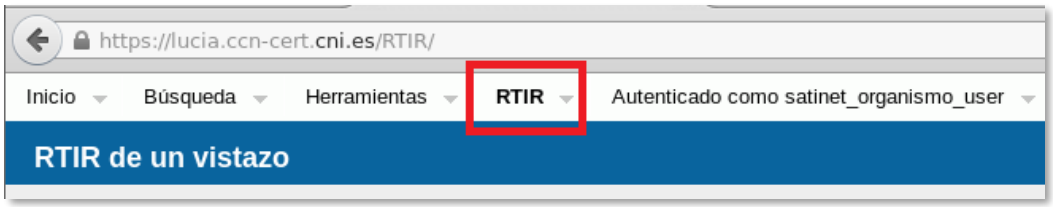
33. Todos los tickets tienen una serie de campos de fechas. Algunos de estos campos solo se pueden establecer a través de la edición del ticket y no en la creación del mismo. A continuación, se listan estos campos indicando su uso y comportamiento:
    - **Creado**: Fecha de creación del ticket. Se establece automáticamente y no puede ser editada.
    - **Comienzo**: Fecha en la que se detectó la incidencia por primera vez. Se establece manualmente y es editable.
    - **Comenzado**: Fecha en la que el personal responsable ha empezado a trabajar con el ticket. Se establece manualmente y es editable.
    - **Cerrado**: Fecha en la que el ticket se cerró por resolución o abandono. Se establece automáticamente. Esta fecha solo podrá ser editada si el administrador así lo ha configurado mediante el parámetro `$lucia_core_allow_modify_resolved`[7].
    - **Fecha Límite**: Fecha límite de resolución del ticket. Se establece automáticamente acorde a la prioridad del ticket y puede ser editada.
    - **Último Contacto**: Fecha de último contacto con un agente externo. Se establece automáticamente al recibir una respuesta y puede ser editada.
    - **Actualizado**: Fecha de última actualización del ticket. Se establece automáticamente tras cualquier cambio en el ticket y no puede ser editada.

[7] Este parámetro se llamaba `$LuciaAllowModifyResolved` en LUCIA REV3.1 y anteriores

3. ACCESO A LUCIA

3.1. ACCESO A LUCIA CENTRAL

34. En caso de no poseer una instancia federada de LUCIA, solo se pueden gestionar incidentes generados por sondas SAT accediendo a la instancia de LUCIA Central.
35. El acceso a LUCIA Central se realiza, con el certificado de usuario previamente cargado en el navegador y con las credenciales suministradas para la gestión de Incidentes SAT, a través de la URL https://lucia.ccn-cert.cni.es.
36. En el caso de que un organismo disponga de gestión de incidentes procedentes de SAT-INET y SAT-SARA simultáneamente poseerá dos usuarios de acceso diferenciados. Esto significa que los incidentes de un SAT no es posible gestionarlos con el usuario proporcionado para el otro y viceversa puesto que no tendrá permisos para verlos. Si se desea combinar la visibilidad de ambos tipos de Incidentes bajo un mismo usuario póngase en contacto con el CCN-CERT.



NOTA IMPORTANTE:

La página que por defecto se muestra al identificarse es *'RTIR de un vistazo'*, siempre que el usuario pertenezca a algún grupo. Si el usuario no pertenece a ningún grupo aparece la página de referencia de RT, *'RT de un vistazo'*.

3.2. ACCESO A LUCIA (INSTANCIA PROPIA)

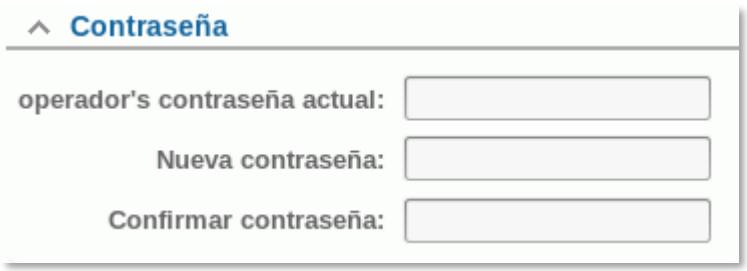
37. En caso de poseer una instancia propia de LUCIA, el acceso se realiza, con el certificado de usuario previamente cargado en el navegador y con las credenciales suministradas, a través de la URL de servicio de la instancia de LUCIA instalada en el organismo.

NOTA IMPORTANTE:

La página que por defecto se muestra al identificarse es *'RTIR de un vistazo'*, siempre que el usuario pertenezca a algún grupo. Si el usuario no pertenece a ningún grupo aparece la página de referencia de RT, *'RT de un vistazo'*.

3.3. CAMBIAR LA CONTRASEÑA

38. La contraseña de acceso a LUCIA Central puede modificarse desde la opción del menú *'Autenticado como <usuario> →Configuración →Acerca de mí'*.
39. Desde este menú *'Preferencias'*, pueden modificarse otros datos como el nombre o la dirección de correo del usuario.



4. EL PANEL PRINCIPAL

40. Para operar con LUCIA se recomienda utilizar la vista '*RTIR*' en la parte superior (barra de navegación). Se dejaría la vista '*RT*' para otras operaciones sobre RT/RTIR (e.g., gestión interna de ticketing).

41. Esta vista ya está preparada con una serie de secciones. Por defecto en el bloque principal se verán los nuevos reportes de incidente de LUCIA, incidentes de LUCIA próximos a vencer (asignados al usuario actual, sin asignar, y en general, en tres secciones respectivamente). Además se verá en el panel lateral otra sección 'Trabajar con visibilidad', que permitirá filtrar por visibilidad/*constituency*.

42. En las versiones de LUCIA REV3.1 y anteriores estas secciones mostraban tickets de LUCIA y RTIR entremezclados. Desde LUCIA REV4.0 son secciones independientes entre sí (i.e., los tickets de LUCIA se mostrarán en unas secciones y los de RTIR en otras diferentes).

43. Aquellos usuarios que tengan personalizado el panel de RTIR no verán estos cambios por defecto, ya que la política seguida en el proceso de instalación de LUCIA REV4.0 es respetar estas personalizaciones en caso de que existan. Para añadir estas vistas, desde la vista '*RTIR*' se editará a través de la acción '*Editar*' (esquina superior derecha).

44. Una vez en el editor de 'RTIR de un vistazo' se mostrarán dos secciones: El cuerpo (panel principal) y la barra lateral. Ambos tienen a la izquierda una lista con los componentes que se pueden añadir y a la derecha otra lista con los componentes ya añadidos. Si quisiéramos añadir los componentes "Nuevos Reportes de Incidentes de LUCIA no enlazados…", "Incidentes de LUCIA con fecha límite más cercana cuyo propietario es el usuario actual", "Incidentes de LUCIA con fecha límite más cercana sin propietario" e "Incidentes de LUCIA con fecha límite más cercana" (los componentes introducidos en LUCIA REV4.0), se seleccionarían de la lista de disponibles y se pulsaría el botón '→' para añadirlos a la vista. Si quisiéramos reordenarlos, los seleccionaríamos en la lista de añadidos y pulsaríamos los botones de subir y bajar a su derecha. Igualmente, el botón '*Borrar*' los quitará de la vista (pero no así de los disponibles). Similarmente, se podría añadir el componente "LuciaWorkWithConstituency" si éste no estuviera ya añadido en el panel lateral.

5. GESTIÓN DE INCIDENTES SAT

45. El organismo parte de un Incidente SAT creado por los operadores del CCN-CERT en LUCIA Central y que se ha sincronizado completamente en la instancia local del organismo si se dispone de ella. En el caso de no disponer de una instancia propia, la gestión se hará directamente en LUCIA Central.
46. A continuación se resumen las acciones que conforman el flujo de trabajo con un incidente, pasándose posteriormente a detallar cada una de ellas:
    - Reasignarse el Incidente.
    - Actualizar el incidente, modificando la información asociada al incidente.
    - Solicitar más información para los casos en que sea necesario.
    - Añadir comentarios en cada una de las fases de su resolución.
    - Resolver el incidente.

5.1. ASIGNARSE EL INCIDENTE

47. Una vez seleccionado un Incidente, inicialmente el propietario será un operador *"SAT CCN-CERT"*, por lo que el organismo debe asignárselo mediante la opción *'Reasignarse'* bajo la opción del menú *'Acciones'* para ser su propietario y ser responsable de la resolución del mismo.

5.2. MODIFICAR LOS VALORES DE LOS CAMPOS DEL INCIDENTE

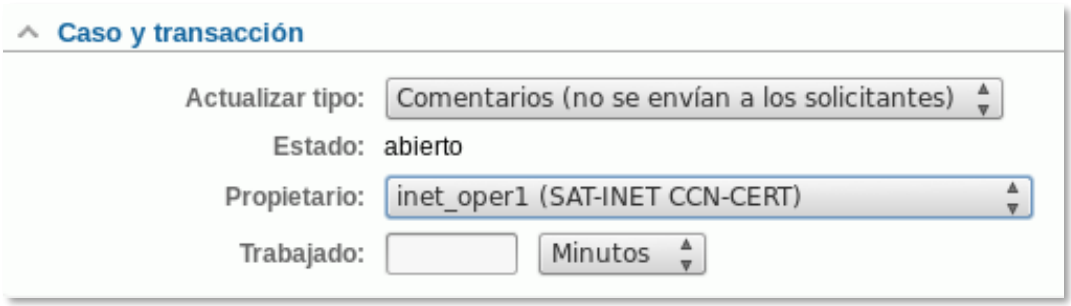
48. Si se desea modificar alguno de los valores de los campos permitidos del Incidente o bien para cumplimentar los campos de resolución previamente al cierre, se debe utilizar la opción *'Editar'*.
49. Es necesario seleccionar el botón *'Guardar Cambios'* para almacenar las modificaciones.
50. Consulte el apartado 2.2.3 "Incidente (Incident) e Incidente SAT (SAT Incident)" para una descripción detallada de todos los campos y sus posibles valores

5.3. COMENTAR UN INCIDENTE

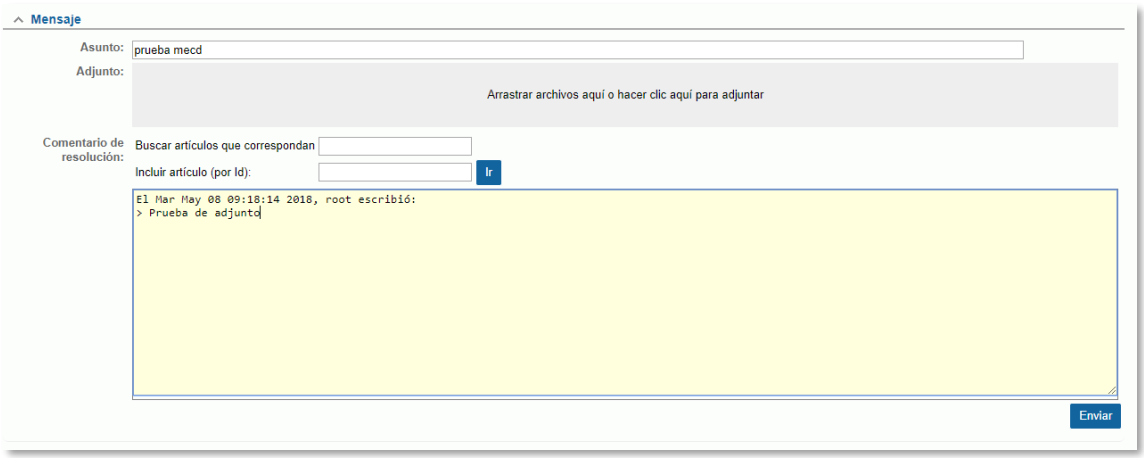
51. Un Incidente SAT notificado por el CCN-CERT nunca tendrá asociado Reportes de Incidentes ni Investigaciones. Del mismo modo, no deben utilizarse Reportes de Incidentes ni Investigaciones para intercambiar información con LUCIA Central. La información al respecto del incidente o comunicaciones a los operadores del SAT debe realizarse mediante "comentarios" en el propio Incidente desde el *'Historial'* en la vista *'Mostrar'*.

52. El comportamiento de *'Comentario'* es similar al de *'Responder'* con la diferencia de que no existen destinatarios a los que enviar la respuesta, sino que quedará registrada en el propio Incidente. En el caso de la gestión de incidentes SAT, nunca se utilizará la opción *'Responder'*.

53. Una vez pulsado el botón de *'Comentario'*, aparecerá una plantilla similar a la de redacción de un correo en la que se podrá documentar las acciones o peticiones, agregar adjuntos y modificar el tiempo total empleado para todo el incidente.



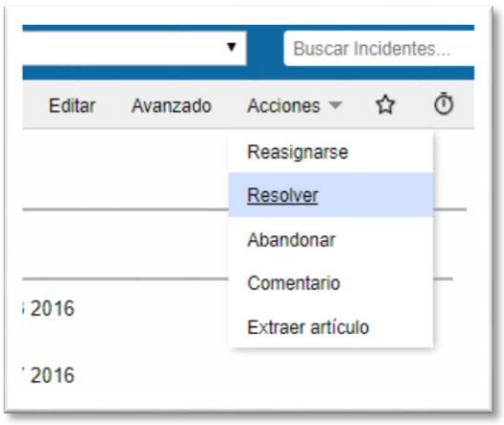
54. Es necesario seleccionar el botón 'Enviar' para guardar el comentario.



55. En caso de que un comentario contenga una consulta a los operadores del CCN-CERT, se puede llamar su atención asignando el valor 'Solicita Información' al campo 'Situación'.

5.4. RESOLVER (CERRAR) UN INCIDENTE

56. Para resolver un Incidente, se usará la acción *'Resolver'* bajo el menú *'Acciones'*.



57. La opción *'Resolver'* muestra una nueva pantalla donde se muestran los campos de *Resolución* para ser cumplimentados si no se ha hecho con anterioridad.

58. Cuando se resuelve un Incidente del SAT, no es necesario indicar ninguna dirección de correo electrónico puesto que la información se almacena directamente en el sistema. Ni siquiera es necesario en el caso de instancias remotas puesto que la información se sincroniza automáticamente.

59. Si se necesita documentar las acciones o el cierre o adjuntar ficheros, debe realizarse mediante el botón *'Comentar'* que se encuentra en la sección *'Histórico'* de la vista *'Mostrar'* del incidente. Tampoco debe utilizarse la opción *'Responder'*.

60. En el proceso de cierre de incidentes es importante rellenar todos los campos que se encuentran en la página de resolución ya que se usan para cumplimentar los requerimientos del ENS y, por ejemplo, a largo plazo, extraer la información necesaria para completar con fiabilidad los requerimientos de INES. Los campos son los siguientes:

    - **Peligrosidad**: el valor debe de ser distinto de *"(sin valor)"*
    - **Resolución**: el valor debe de ser distinto de *"(sin valor)"*
    - **Recursos Invertidos**: el valor debe de ser distinto de *"(sin valor)"*
    - **Categoría del sistema según ENS**: el valor debe de ser distinto de *"(sin valor)"*
    - **Impacto**: el valor debe de ser distinto de *"(sin valor)"*
    - **Número de sistemas afectados**: el valor debe de ser distinto de *"(sin valor)"*
    - **Causa del incidente**: Al menos un elemento marcado
    - **Incidencias durante la resolución**: Al menos un elemento marcado
    - **Tiempo trabajado**: Valor numérico entero positivo mayor que cero
    - **¿Afecta al RGPD?**: Seleccionar *"Sí"* si procede

- **Notificar a AGPD**: Seleccionar *"Sí"* si procede y se ha marcado *¿Afecta al RGPD?*
- **Notificar al CNPIC**: Seleccionar *"Sí"* si procede
- **Categoría del Sistema según ENS**: Seleccionar un valor si procede

61. Para mayor comodidad, estos campos son los mismos que aparecen en la sección *"Resolución"* de la edición del ticket, por lo que no es necesario llegar hasta la página de resolución para cumplimentarlos.
62. Los Incidentes resueltos no se muestran en el panel de inicio ni en el de RTIR. No obstante, pueden ser localizados mediante búsquedas, agregar comentarios y reabrirse si es necesario.
63. Recordar que existen procesos automáticos que resuelven tickets automáticamente.

6. GESTIÓN DE INCIDENTES EN INSTANCIAS DE LUCIA

64. El flujo de trabajo se puede iniciar con cualquiera de los tres tipos de objetos disponibles:
    - Reporte de Incidente: Se creará automáticamente por cada correo recibido en la cuenta monitorizada por LUCIA, o bien manualmente desde la aplicación si fue recibido por otro medio (teléfono, fax, etc.)
    - Investigación: Se lanzará una Investigación para establecer un nuevo canal de comunicación que se inicia desde LUCIA. Nótese que la diferencia con el anterior reside en quién es el que inicia la comunicación.
    - Incidente: Se puede crear un Incidente para documentar información sobre un caso sin que existan Reportes de Incidentes ni Investigaciones asociadas, sin embargo, no se podrá comunicar con agentes externos.
65. A continuación se ilustra con un ejemplo:
    - Un usuario remite un correo a la cuenta de correo de LUCIA informando que ha sido infectado por un troyano al visitar una página web.
    - El correo generará un ticket Reporte de Incidente que un operador revisará y se lo asignará para ser su propietario y ser responsable de la resolución del mismo. En caso de que no sea válido (por ejemplo, un correo de SPAM) el Reporte de Incidente podrá ser rechazado por el operador.
    - El operador se comunicará con el usuario exclusivamente a través de ese ticket Reporte de Incidente que se encuentra identificado con un número único en el asunto de los correos intercambiados.
    - Paralelamente, el operador puede crear un nuevo ticket Incidente donde lo categorizará y almacenará información que no será compartida con el usuario. En el caso de que ya exista un ticket Incidente relacionado, el Reporte de Incidente puede ser enlazado con él.
    - Durante la gestión del incidente, el operador identifica el servidor infectado y decide ponerse en contacto con el administrador para que tome las medidas oportunas. Para ello, lanza una nueva Investigación enlazada al Incidente con la que se comunicará con el administrador.
    - El operador resolverá (cerrará) los Reportes de Incidentes e Investigaciones según se vayan solucionando. Si resolviera el Incidente, todos los objetos relacionados se resolverían automáticamente en cascada.
66. Como se puede observar en el ejemplo, si se utilizan los distintos tipos de ticket correctamente, no hay posibilidad de mezclar información entre comunicaciones ni

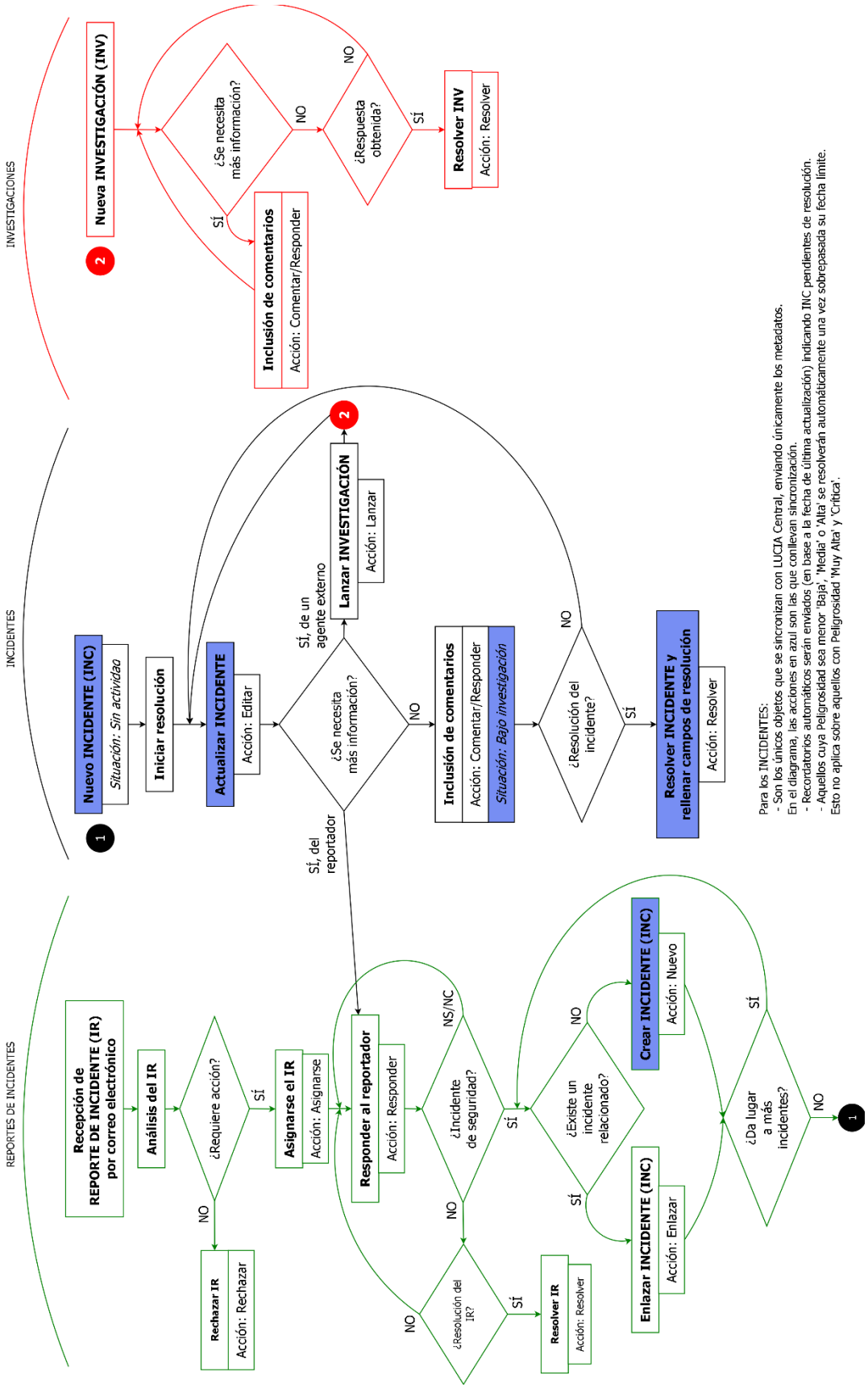
de posibles fugas de información sensible que pueda almacenarse en los comentarios del ticket Incidente.

Durante este proceso, si la instancia se encuentra sincronizada con el CCN-CERT, únicamente los metadatos del ticket Incidente se sincronizan con LUCIA Central. Por tanto, no se envía ni el texto, ni los comentarios, ni ninguna información relativa a los Reportes de Incidentes o Investigaciones.

67. En la actualización de LUCIA 3.1 se introduce la notificación de incidentes a otros organismos, atendiendo a los valores del grupo de campos “Normativa Aplicable”. Al activar un campo de notificación el incidente será notificado al organismo responsable, creándose (tras unos minutos) un Reporte de incidente asociado. El reporte creado estará sincronizado con el organismo responsable y por tanto servirá de canal de comunicación entre ambos. La siguiente tabla muestra la relación entre los campos de normativa aplicable y el organismo que será notificado:

Campo	Organismo notificado
Notificar a AGPD	Agencia Española de Protección de Datos
Notificar al CNPIC	Centro Nacional de Protección de Infraestructuras Críticas
Requiere intervención del CCN-CERT	Centro Criptológico Nacional

6.1. DIAGRAMA DEL FLUJO DE TRABAJO



6.2. DESCRIPCIÓN DEL PANEL RTIR

68. Situados en la página *'RTIR de un vistazo'*, en la columna de la izquierda veremos los siguientes bloques:
    - *Nuevos Reportes de Incidentes no enlazados...*: Esta sección muestra los Reportes de Incidentes aún no asignados a ningún usuario. Haga clic en el identificador o la descripción de cualquier entrada para mostrar la página de información básica del caso o en *'Asignarse'* para asignárnoslo. También aparece la opción *'Rechazar en lote'* que permite hacer una limpieza rápida de aquellos Reportes de Incidentes que se deseen eliminar.
    - *Incidentes con fecha tope más cercana con propietario <usuario>*: Se listan los casos que posee el usuario, ordenados por su Fecha Límite.
    - *Incidentes con fecha tope más cercana sin propietario*: Se listan los casos que no están asignados a ningún usuario, ordenados por su Fecha Límite.
    - *Incidentes con fecha tope más cercana*: Se listan los casos sobre los que el usuario tiene, al menos, permiso de lectura, estén o no están asignados a su usuario, ordenados por su Fecha Límite.
69. Y en la columna de la derecha de la misma página:
    - *Recargar*: Este menú desplegable permite seleccionar si la página se actualiza automáticamente o no pasados ciertos minutos. Haga clic en *'¡Ir!'* para seleccionar el retardo de actualización automática que se muestra.
    - *Búsqueda rápida*: Este panel contiene el acumulado de todas aquellas colas a las que, como usuario del sistema, el usuario está autorizado a acceder.

7. OPERACIONES

7.1. CREAR (SOLO PARA ORGANISMOS FEDERADOS)

70. Para la creación de un nuevo ticket de forma manual, se hará clic en la cola deseada a través del desplegable situado a la derecha del botón *'Nuevo ticket en'* en la parte superior derecha de la pantalla, o bien creándolo desde la opción correspondiente del menú *'RTIR'*.

71. A continuación, aparecerá la página de creación del ticket con los campos propios a cumplimentar. Como se ha comentado anteriormente, los campos dependerán de la cola que se haya elegido.

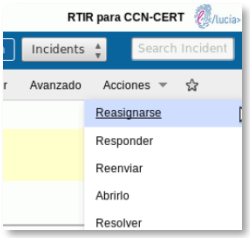
72. **En ningún caso se podrán crear incidentes de SAT**, solo incidentes propios.

7.2. ASIGNARSE Y REASIGNARSE UN TICKET (SOLO ORGANISMOS FEDERADOS)

73. *'Asignarse'* un ticket significa asignar al usuario como propietario del mismo. Para ello es necesario entrar en la vista de un ticket y seleccionar *'Asignarse'* en el desplegable de *Acciones* que aparece en la parte superior derecha.

74. *'Reasignarse'* un ticket tiene el mismo efecto que asignárselo, pero cuando ya se encuentra asignado a otro usuario. La diferencia está en que, en vez de asignarse

un ticket sin propietario, se está asignado un ticket que tiene a otro usuario como propietario.



75. El hecho de asignarse o reasignarse un ticket es porque existen acciones que sólo pueden ser ejecutadas por el propietario del ticket.

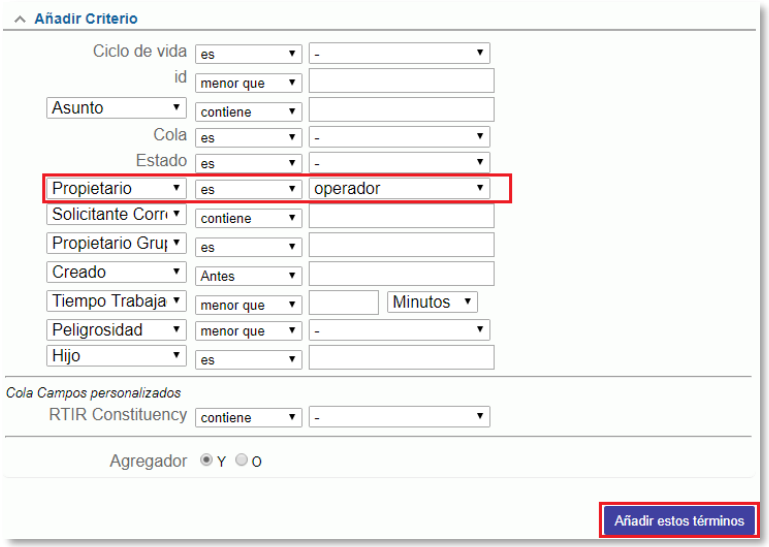
7.3. EDITAR

76. Si se desea modificar alguno de los valores de los campos de un ticket, se debe utilizar la opción del menú *'Editar'*. Consulte el apartado relativo al ticket para una descripción detallada de todos los campos y sus posibles valores.
77. Es necesario seleccionar el botón *'Guardar Cambios'* para almacenar las modificaciones.

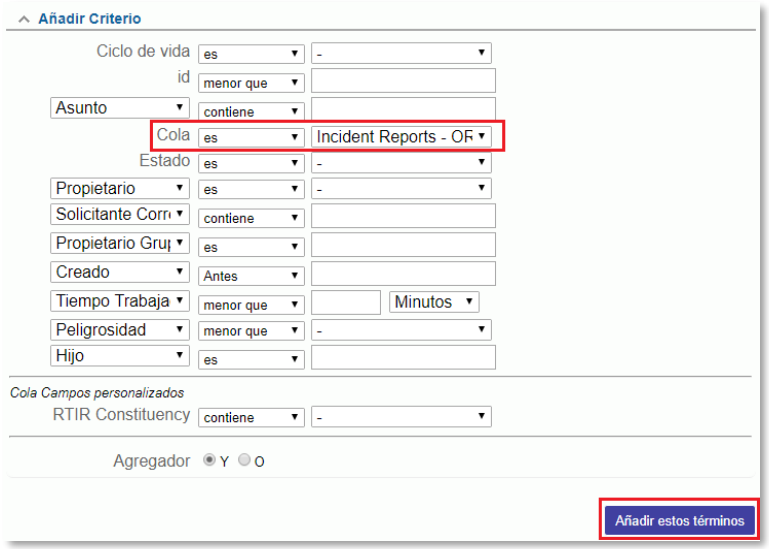
7.4. BUSCAR

78. Desde la opción *'Búsqueda'* del menú RTIR es posible construir búsquedas con una lógica similar al lenguaje SQL para localizar tickets que cumplen las condiciones definidas en la consulta.
79. Las búsquedas abarcan todo ticket dado de alta en LUCIA, lo que permite buscar incluso aquellos que ya han sido cerrados y no son visibles desde el panel principal.
80. La opción *'Mostrar Resultados'*, permite ejecutar de nuevo la última consulta sin ser necesario volver a definirla.
81. A continuación, como ejemplo, se describe cómo generar una búsqueda que muestre los Reportes de Incidentes y las Investigaciones recientemente actualizados, es decir, marcados como *"Nuevos Mensajes"*. Posteriormente, esta búsqueda se podrá añadir como panel a la página de inicio de RTIR, tal y como se explica en la sección *"Modificar Paneles"*:

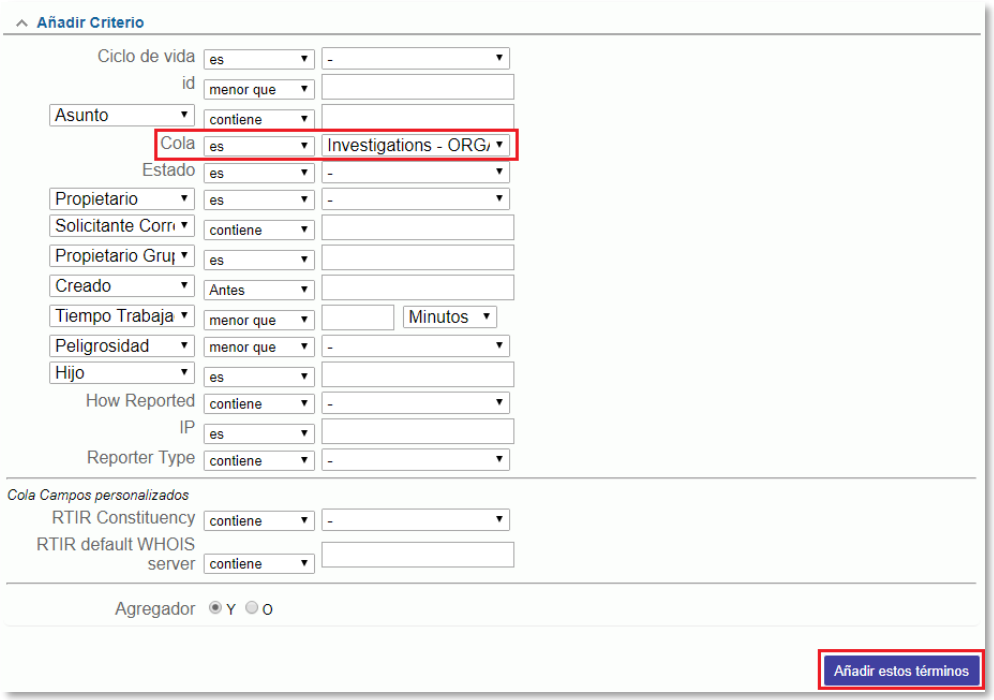
- Desde la página de *'RTIR→Búsqueda→Nueva búsqueda'*, seleccionar el criterio *'Propietario' 'es' 'nombre_usuario'* y pulsar en el botón *'Añadir estos términos'*.



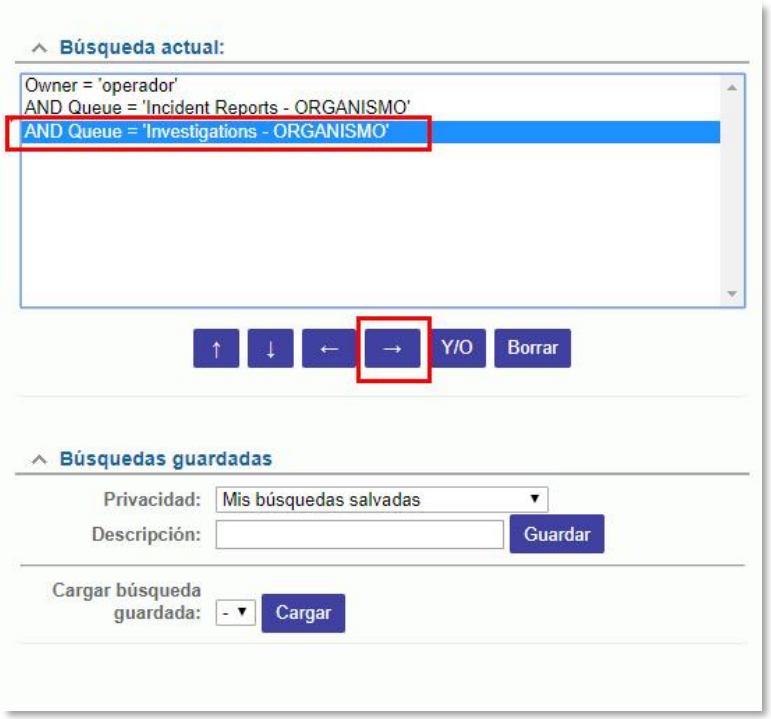
- Seleccionar el criterio *'Cola' 'es' 'Incident Reports – NOMBRE_VISIBILIDAD'* y pulsar en *'Añadir estos términos'*.



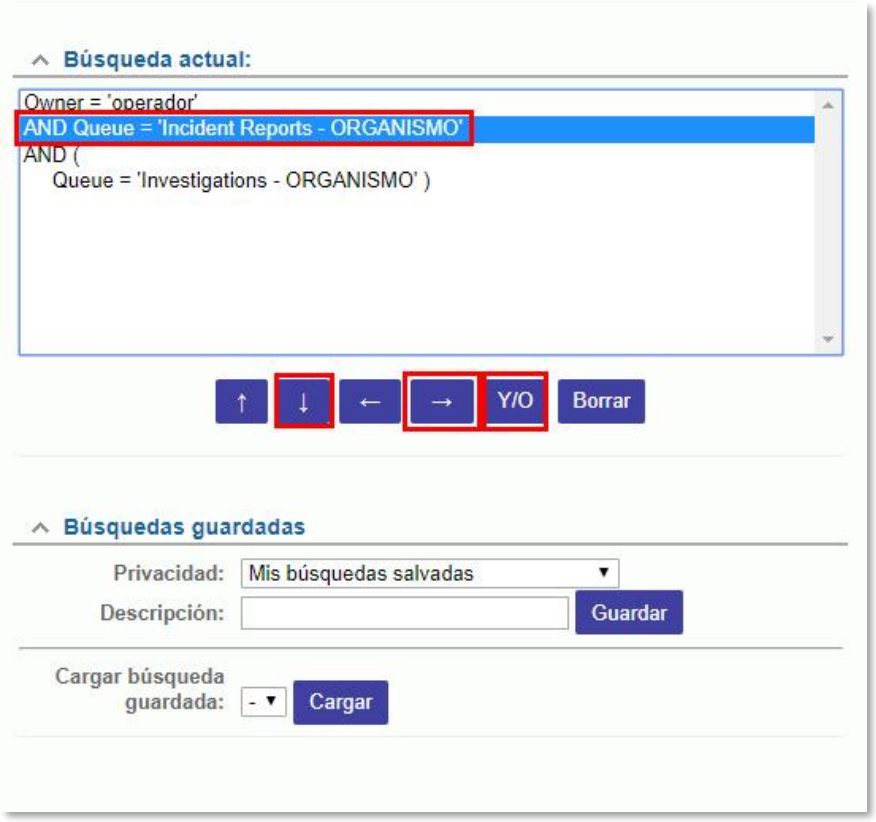
– Seleccionar el criterio *'Cola' 'es' 'Investigations – NOMBRE_VISIBILIDAD'* y pulsar en *'Añadir estos términos'*.



– Seleccionar en los criterios añadidos *AND Queue = 'Investigations - NOMBRE_VISIBILIDAD'* y pulsar en el botón identificado como una flecha a la derecha.



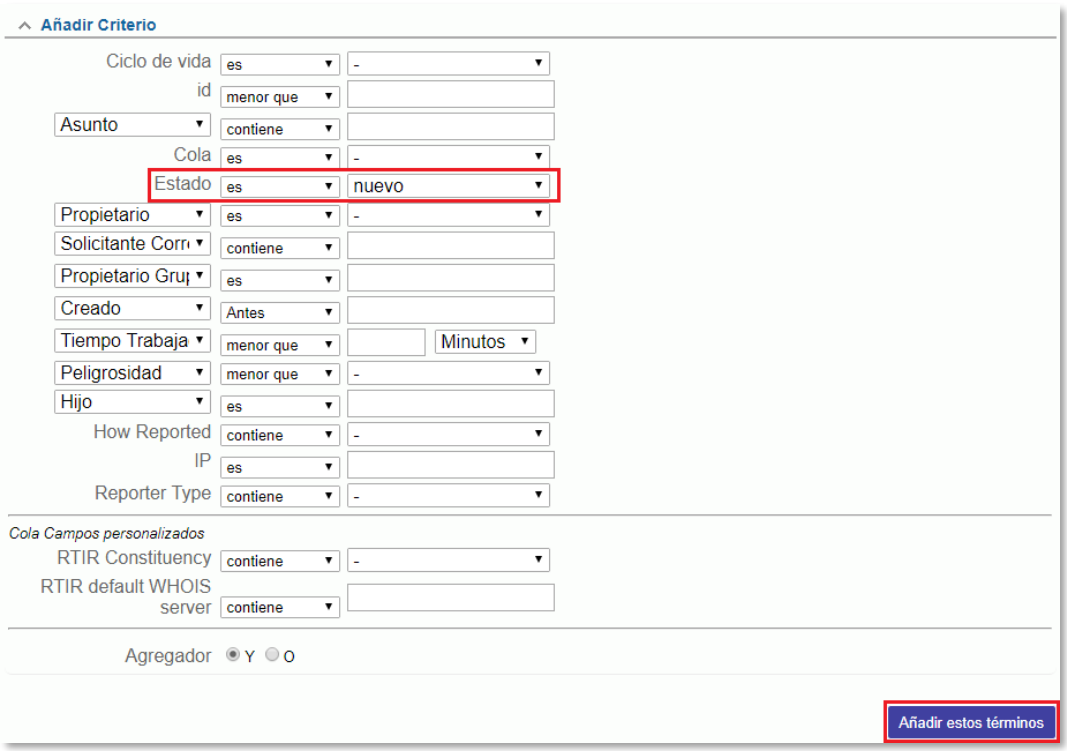
– Seleccionar en los criterios añadidos *AND Queue = 'Incident Reports – NOMBRE_VISIBILIDAD'* y pulsar en este orden los botones: *abajo, derecha e Y/O*.



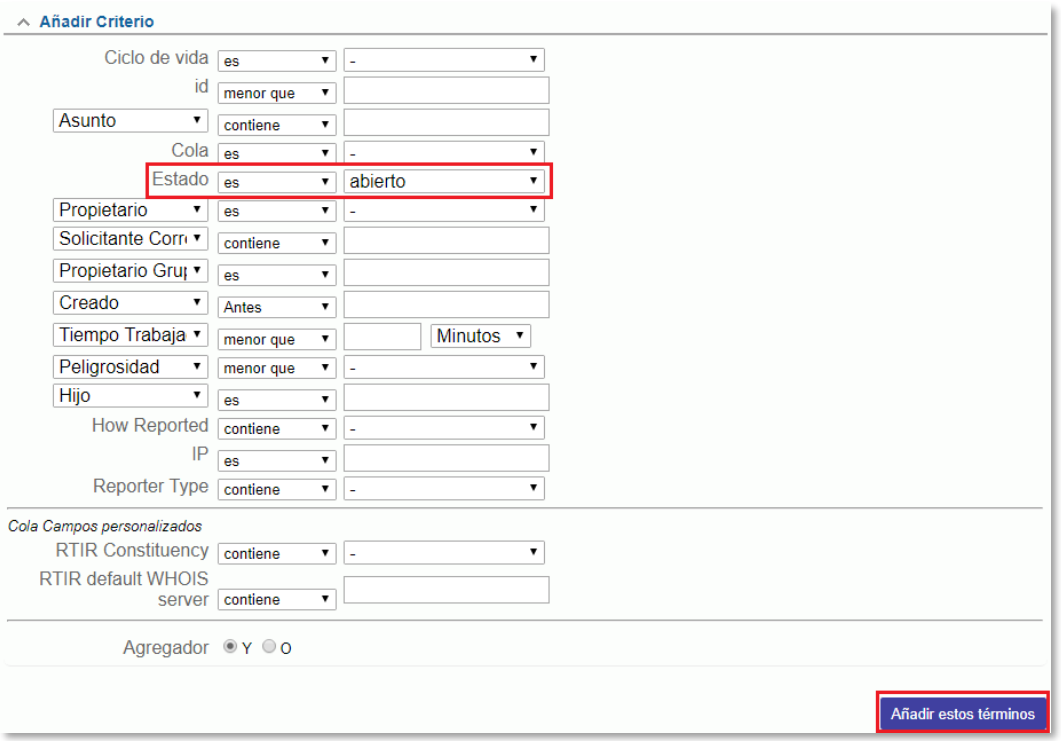
– Resultando la siguiente consulta:

– Seleccionar en los criterios añadidos *Owner = 'nombre_usuario'*.

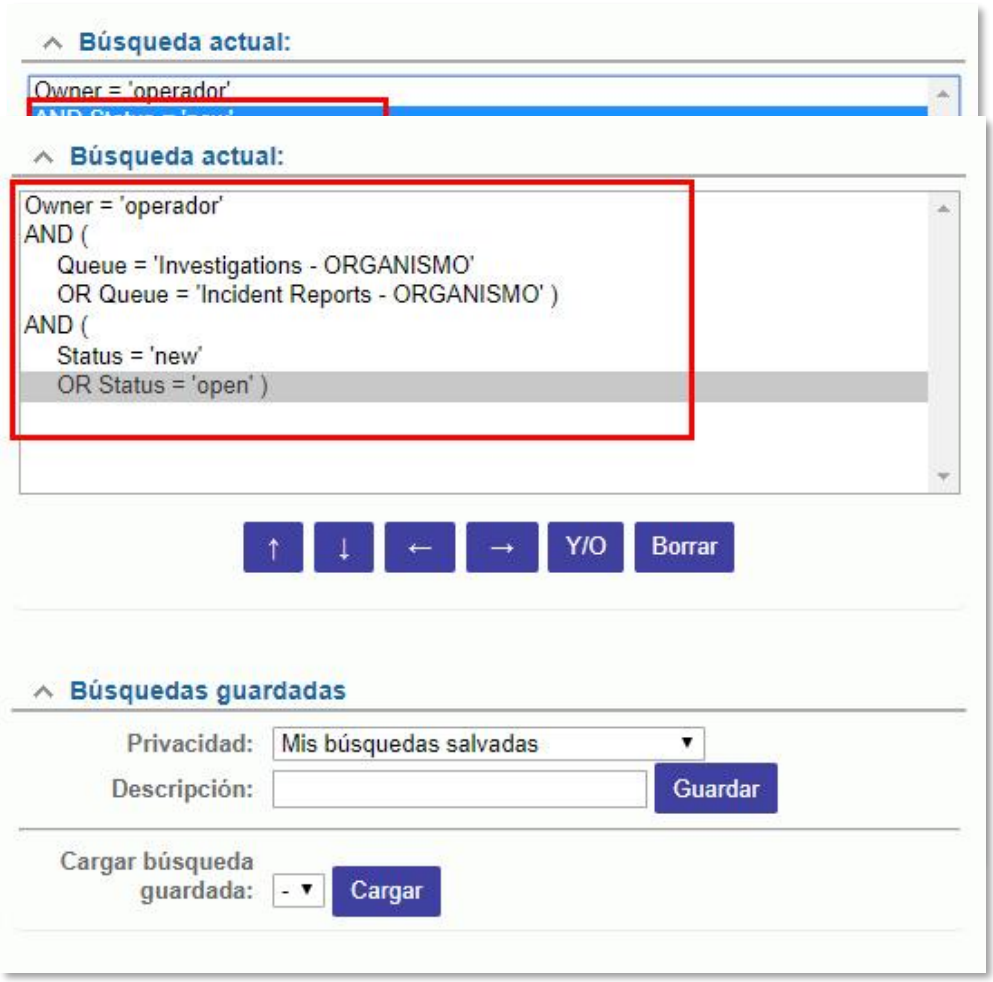
– Seleccionar el criterio *'Estado' 'es' 'nuevo'* y pulsar en *'Añadir estos términos'*.



– Seleccionar el criterio *'Estado' 'es' 'abierto'* y pulsar en *'Añadir estos términos'*.



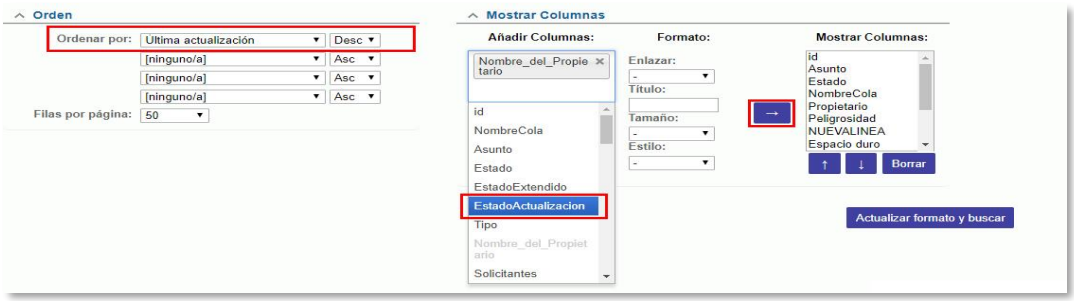
– Seleccionar el criterio *AND Status = 'new'* y pulsar en el botón *derecha*.



– Seleccionar el criterio *AND Status = 'open'* y pulsar en el siguiente orden los botones *abajo, abajo, derecha e Y/O*.

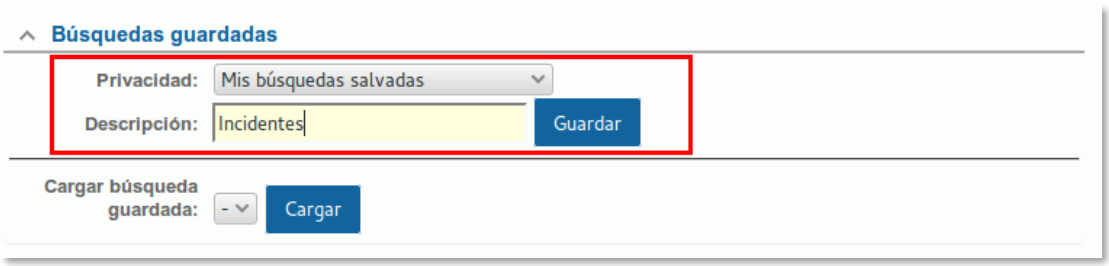
– Dando como resultado la siguiente consulta:

– Seleccionar en Orden el campo *Última actualización* y *Desc*. A su vez, se debe incluir entre las columnas a mostrar el campo *'EstadoActualizacion'*. Se pueden borrar aquellas columnas a mostrar que se consideren innecesarias.



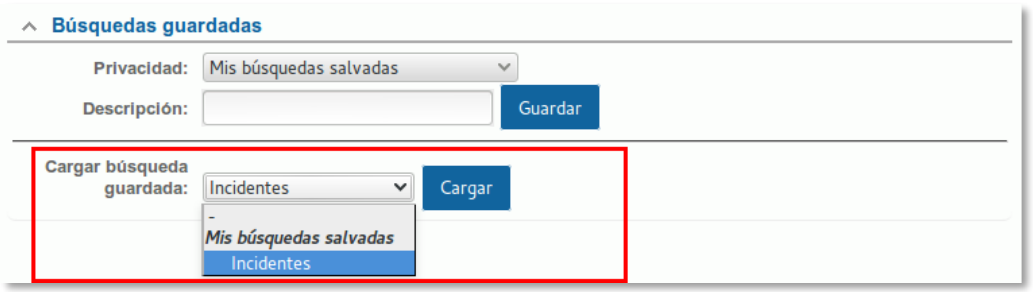
82. Para mayor comodidad, las consultas pueden ser almacenadas para reutilizarse en cualquier momento. Para ello, una vez definidos los criterios, pulsar en el botón *"Añadir estos términos"* para incorporarlos en la ventana *"Búsqueda actual"* tantas veces como se requiera.

83. Una vez definida, se debe guardar la consulta en la sección destinada a tal efecto, seleccionando dentro del desplegable *Privacidad* el valor *"Mis búsquedas salvadas"* incluyendo una descripción.



84. Para cargar una búsqueda ya existente, se debe seleccionar en el desplegable *'Cargar búsqueda guardada'* y pulsar en el botón *"Cargar"*.

85. Para poder utilizar las búsquedas guardadas es necesario que el administrador de LUCIA así lo haya configurado previamente.



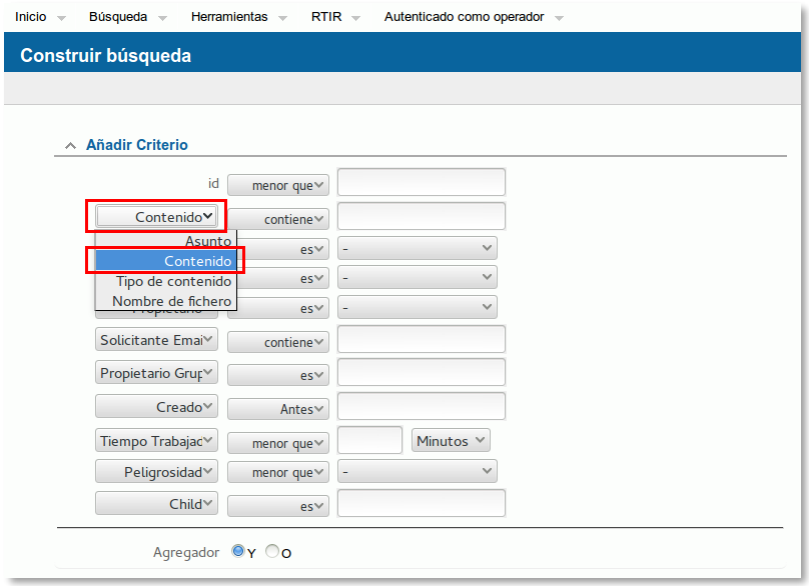
7.4.1. BÚSQUEDAS POR CONTENIDO[8]

86. Las búsquedas por contenido, como su nombre indican, buscan dentro del contenido del ticket tanto en su texto inicial como en los comentarios.

87. Para hacer esta búsqueda, es necesario que exista un índice en base de datos el cual se reconstruye automáticamente cada veinte minutos, procesando 150 tickets en cada pasada. Es por ello que un ticket recién creado no aparecerá en los resultados de búsqueda hasta que haya sido indexado.

[8] Disponible a partir de la actualización LUCIA REV2.3

88. Para realizar búsquedas por contenido en los tickets, se deberá seleccionar el campo *'Contenido'* en el desplegable correspondiente al construir la consulta.



89. Las búsquedas por contenido son de tipo booleano con las siguientes características:
    - Sólo se pueden buscar palabras cuya longitud sea de al menos 3 caracteres.
    - No distingue entre mayúsculas y minúsculas.
    - Se pueden añadir ciertos caracteres especiales al principio o al final de las palabras a buscar. A continuación, se listan todos los caracteres especiales existentes:

Carácter	Significado
`+palabra`	*palabra* debe estar presente en cada resultado devuelto.
`-palabra`	*palabra* no debe estar presente en los resultados.
`@distancia`	Todas las palabras no distan unas de otras más palabras de lo especificado. Las palabras a buscar han de ir entrecomilladas y, a continuación, el operador `@distancia`.
`>` `<`	Se usan para cambiar la contribución de una palabra a la relevancia de los resultados. El operador `>` incrementa su contribución y el operador `<` la decrementa.
`( )`	Los paréntesis agrupan palabras en subexpresiones. Estos grupos pueden anidarse.
`~palabra`	Al comienzo de una palabra indica que los resultados que tengan esa palabra han de presentarse con menos relevancia, es decir, se mostrarán al final, pero no serán excluidos como lo serían con el símbolo '-'.

*	Carácter comodín. Al revés que el resto, se añade al final de la palabra. Esto devolverá aquellos resultados que contengan palabras que empiezan por los caracteres especificados.
" "	Entrecomillar palabras hace que se busquen literalmente. Los caracteres incluidos que no sean letras no serán tenidos en cuenta.
Sin operador	Por defecto, si no hay otro símbolo, las palabras pueden estar, mostrando primero los resultados que más coincidencias tengan (los más relevantes).

90. A continuación, se muestran algunos ejemplos de búsqueda utilizando los operadores anteriormente descritos:

    `Mercurio Venus`

    Devuelve los resultados que contengan al menos una de las dos palabras.

    `+Mercurio +Venus`

    Devuelve los resultados que contengan las dos palabras.

    `+Mercurio Venus`

    Devuelve los resultados que contengan *Mercurio*, pero presenta con más relevancia los que además contienen *Venus*.

    `+Mercurio –Venus`

    Devuelve los resultados que contengan *Mercurio* y que no contengan *Venus*.

    `+Mercurio ~Venus`

    Devuelve los resultados que contengan *Mercurio*, pero presenta con menos relevancia los que además contienen *Venus*.

    `+Mercurio +(>Venus <Tierra)`

    Devuelve los resultados que contienen las palabras *Mercurio* y *Venus*, o *Mercurio* y *Tierra* (en cualquier orden), pero muestra *Mercurio Venus* con más relevancia que *Mercurio Tierra*.

    `Merc*`

    Devuelve los resultados que empiecen por *merc*.

    `“Mercurio Venus”`

    Devuelve los resultados que contienen literalmente *Mercurio Venus*.

7.5. COMENTAR Y RESPONDER

91. Hay dos maneras con las que añadir información a un ticket: comentando y respondiendo. Un comentario permanece oculto al solicitante, mientras que una respuesta es pública y se manda por correo. Ambos textos aparecerán en el historial del ticket. Para ejecutar estas acciones, se hace desde el menú *Acciones* del propio ticket o desde el propio historial.

92. Cuando se ejecuta cualquiera de estas dos acciones se permite agregar adjuntos, actualizar el propietario y el tiempo trabajado en el ticket. Asimismo, se pueden

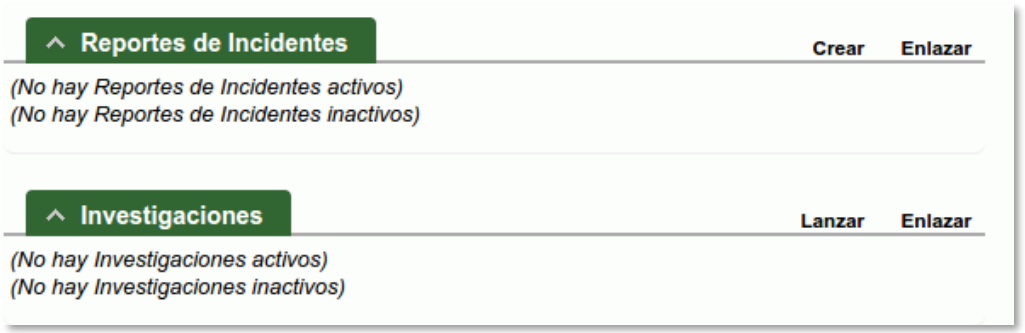
incluir direcciones de correo en *Cc* y *Bcc*, pero sólo recibirán esta actualización del ticket, no las futuras.

7.6. ENLAZAR

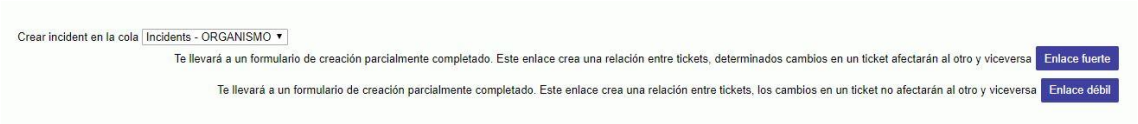
93. Para enlazar un Reporte de Incidente o una Investigación a un Incidente, se debe ir a la vista del ticket y editarlo. Una vez ahí, se selecciona la opción *'Enlazar'* y el o los tickets deseados, y finalmente en *'Enlazar'*.

94. Para que el usuario tenga la opción de enlazar, debe ser el propietario del ticket.

95. En el caso de tratar con un Incidente, el proceso se hará desde la propia vista del ticket, haciendo clic en *'Enlazar'*:



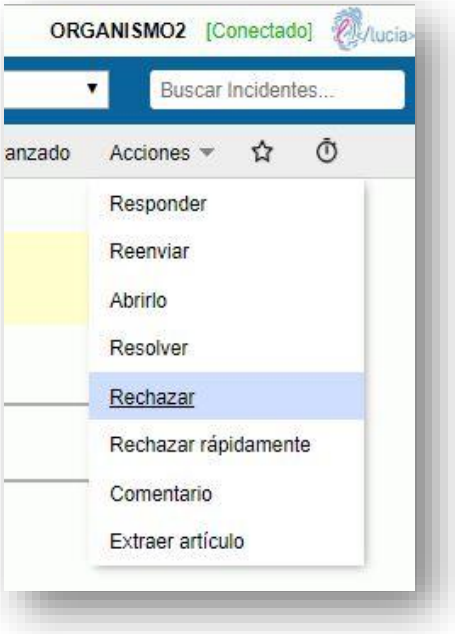
96. Existen dos tipos de enlace entre incidentes y reportes/investigaciones: Enlace débil y enlace fuerte. En el enlace débil, los cambios realizados sobre un ticket no afectan al otro y viceversa. En el enlace fuerte, los cambios realizados sobre un ticket afectan al otro y viceversa.



97. Una vez se haya seleccionado dicha opción, se mostrará un listado con los tickets a enlazar, se seleccionará el o los tickets deseados y se pulsará finalmente en *'Enlazar'*.

7.7. RECHAZAR Y ABANDONAR

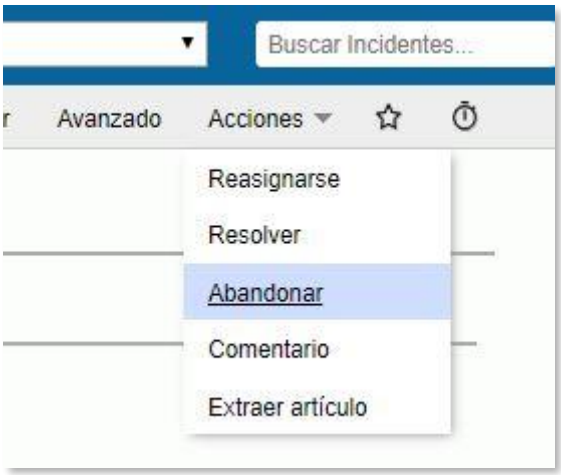
98. Un Reporte de Incidente puede ser rechazado de dos maneras: mediante las acciones *'Rechazar'* y *'Rechazar rápidamente'*.



99. *'Rechazar'* permite incluir información del trabajo realizado previo al rechazo y enviar un comentario o una respuesta para indicar la causa de esta acción.

100. Al *'Rechazar rápidamente'* el ticket pasa a ser automáticamente rechazado, sin necesidad de confirmación, ni posibilidad de incluir información al ticket.

101. Los Incidentes, en vez de ser rechazados, pueden ser abandonados.



102. Al *'Abandonar'* un Incidente permite escoger el estado final de los Reportes asociados y qué Investigaciones pasan a estar resueltas.

7.8. BORRAR TICKET

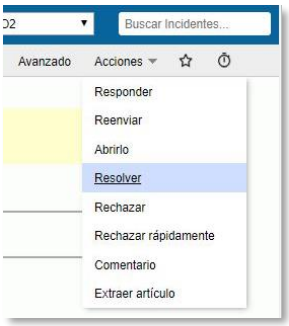
103. El Borrado solo está permitido en tickets propios.

104. Para borrar un ticket debemos situarnos en la página *'Mostrar'* del ticket y en el menú superior pulsar en *"Editar"*.

105. A continuación, marcamos la casilla de borrado y guardamos los cambios.

7.9. RESOLVER (CERRAR) TICKET

106. Para resolver un ticket, se hará clic en la acción *'Resolver'*.



107. Si se necesita documentar las acciones o el cierre o adjuntar ficheros, debe realizarse mediante el botón *'Comentar'* que se encuentra en la sección *'Histórico'* de la vista *'Mostrar'*.

108. Al resolver tickets Incidentes, se muestran también los campos de Resolución para ser cumplimentados y los tickets asociados (Reportes de Incidentes e Investigaciones) que requieren ser marcados también como resueltos (por defecto se cerrarán todos).

109. Recuerde que en el caso de cierre de Incidentes es importante cumplimentar cierta información según lo exige el ENS (consulte el apartado 5.4 "Resolver (cerrar) un Incidente" para más información).

110. Para mayor comodidad, estos campos son los mismos que aparecen en la sección *"Resolución"* de la edición del ticket Incidente, por lo que no es necesario llegar hasta la página de resolución para cumplimentarlos.

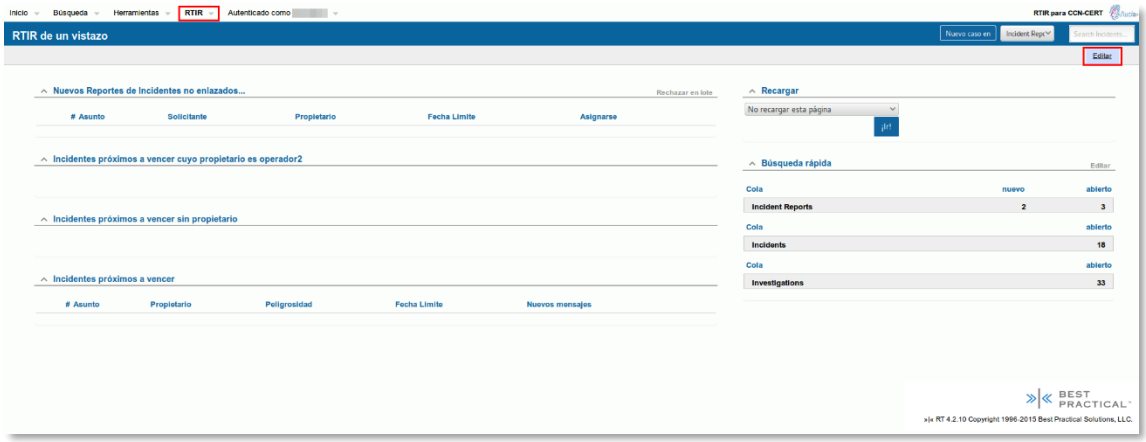
111. Los Incidentes resueltos no se muestran en el panel de inicio ni en el de RTIR. No obstante, pueden ser localizados mediante búsquedas, agregar comentarios y reabrirse si es necesario.

112.Recuerde que existen procesos automatizados que resuelven tickets de forma automática.

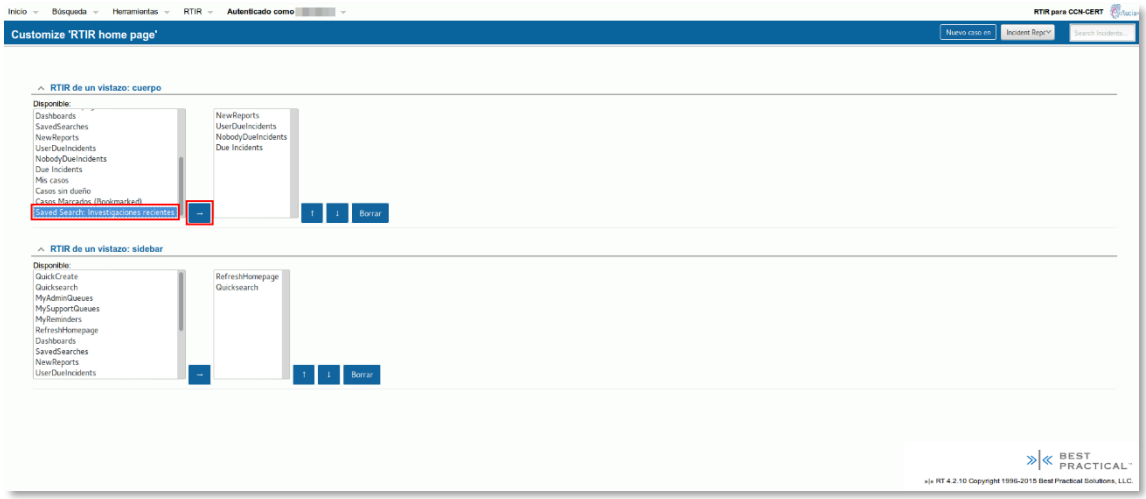
7.10. PERSONALIZAR PANELES DE RTIR

113.Las búsquedas personalizadas pueden resultar de utilidad que aparezcan en la página de inicio de RTIR.

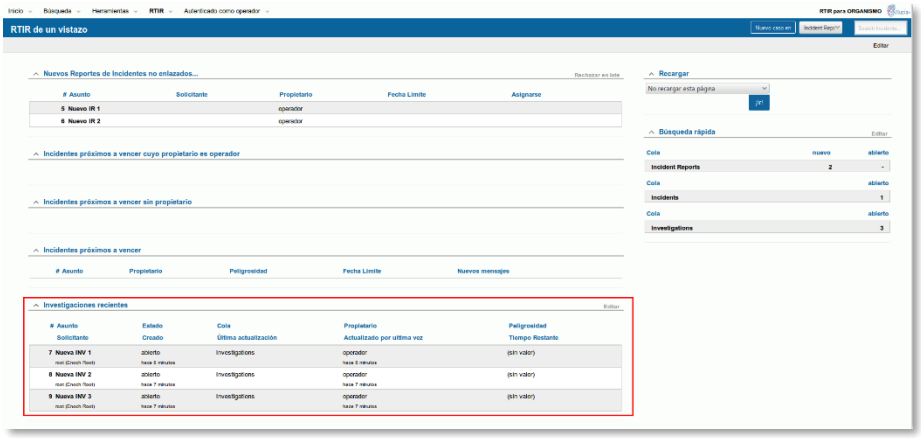
114.Para ello se debe pulsar en *'RTIR'* y después a *'Editar'*:



115.Y añadir la búsqueda guardada al panel, seleccionándola y haciendo clic en el botón identificado como una flecha a la derecha:



116.Con esto ya debe aparecer un nuevo panel con la búsqueda configurada:



7.11. ARTÍCULOS

117.Los artículos son una manera de gestionar respuestas tipo a preguntas frecuentes. En ellos se almacena un texto predefinido (u otros campos) para posteriormente ser añadidos al contenido de una respuesta o de un ticket fácilmente.

118.Internamente se organizan en clases y temas.

7.11.1. CLASES

119.Las clases son el equivalente a las colas. Todo artículo debe pertenecer a una clase.

120.Inicialmente se crean dos clases: *CCN-CERT* y *ORGANISMO*. Sobre la primera se tiene sólo permiso de lectura, pues está pensada para que el CCN-CERT distribuya su base de conocimiento a los organismos. Sobre la segunda se tiene permiso de escritura, pudiendo crear, modificar o borrar artículos.

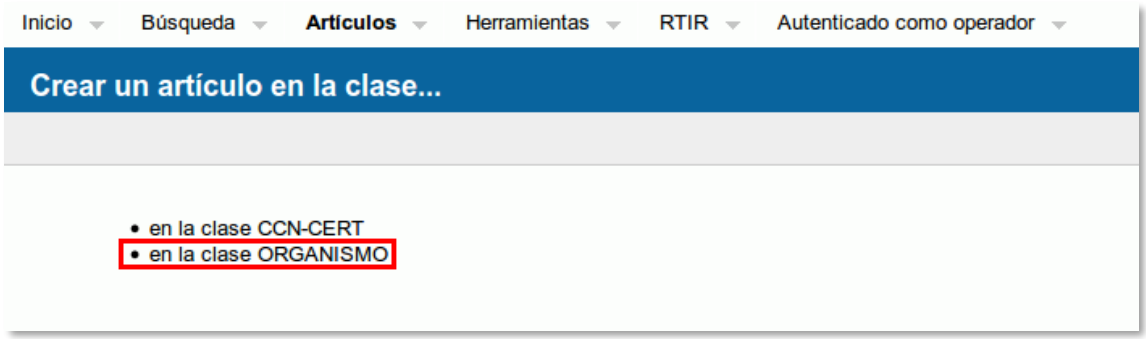
7.11.2. TEMAS

121.Los temas son otra forma de organizar los artículos. Se pueden entender como una especie de etiquetas para los artículos. Los temas globales están disponibles para todos los artículos; y cada artículo podrá estar relacionado con temas tanto globales, como específicos de su clase.

7.11.3. CREAR UN NUEVO ARTÍCULO

122.Se pueden crear nuevos artículos desde *Artículos →Crear*:

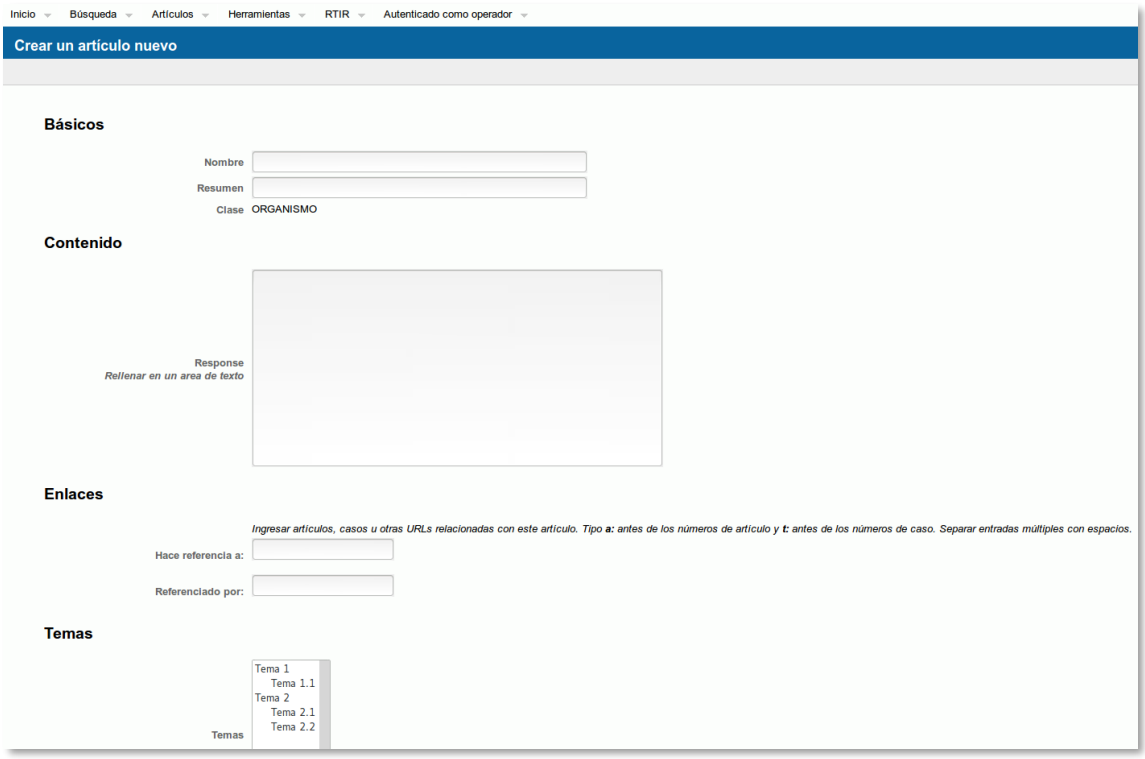
123.Acto seguido, seleccionar la clase donde se desea crear:



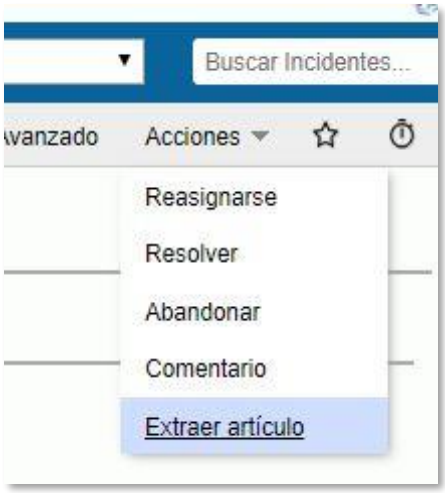
124.Aparecerá la pantalla de creación de artículos con los siguientes campos:

- Básicos
  - Nombre: Nombre del artículo
  - Resumen: Breve descripción del mismo
  - Clase: Clase donde se está creando
- Contenido
  - Response: El contenido del artículo
- Enlaces
  - Hace referencia a: Si referencia a otros tickets o artículos
  - Referenciado por: Si es referenciado por otros tickets o artículos
- Temas

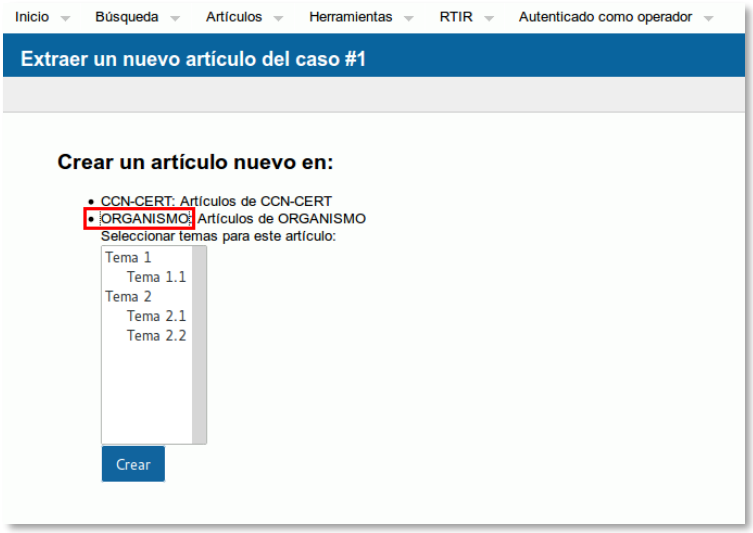
- Temas: Listado de temas asociables a este artículo



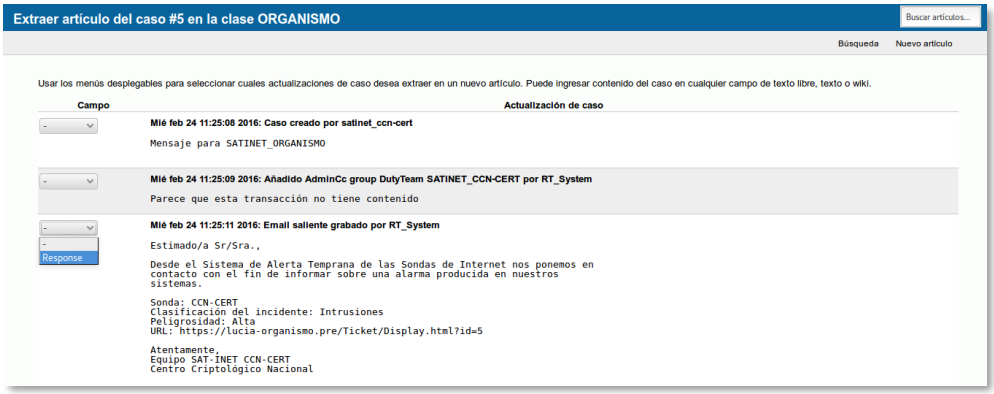
125. Otra manera de crear un artículo es generarlo a partir del cuerpo de un ticket. Para ello, existe la opción *'Extraer artículo'* desde el menú de *'Acciones'*.



126. Tras seleccionar la clase destino, se mostrarán los temas asociables al nuevo artículo a crear.



127. A continuación, se mostrarán las transacciones del ticket junto a unas casillas. Para cada una de ellas se puede seleccionar qué Campo personalizados guardará la información de dicha transacción y a continuación se crea un artículo de forma normal.



7.11.4. USAR UN ARTÍCULO

128. Cuando se responde o se crea un ticket, aparecen unos controles que permiten buscar artículos para incluir en la respuesta. Se pueden insertar tantos artículos como se deseen en una misma respuesta.

129. Los artículos se pueden incluir mediante su buscador, a través de su Id o utilizando el desplegable.

8. OPERACIONES AUTOMÁTICAS

8.1. NOTIFICACIONES DE CORREO

130. Toda acción ejecutada en LUCIA generará un correo de notificación a la cuenta de correo del organismo en el que aparecerá una breve información y un enlace para consultar directamente el ticket relacionado.

131. Las notificaciones de correo automáticas comprenden:

- Creación del Incidente.
- Comentarios.
- Recordatorios según la peligrosidad del Incidente y la última actualización.
- Resoluciones de tickets.
- Autocierres de Incidentes al alcanzar la fecha límite en base a la peligrosidad.

8.2. RECORDATORIOS

132. En LUCIA se encuentran programados una serie de recordatorios automáticos de Incidentes según los parámetros del ENS.

133. El envío de los recordatorios se realiza por las noches. Para cada Incidente se comprueba que desde la última actualización ha pasado un número de días según la siguiente tabla:

Situación	Sin actividad	Bajo investigación	Solicita información
Peligrosidad	**Número de días**		
Bajo	15	15	15
Medio	15	15	15
Alto	15	15	15
Muy alto	7	7	7
Crítico	3	3	3

Tabla 1: Recordatorios automáticos de incidentes, según parámetros del ENS.

8.3. AUTOCIERRES

134. LUCIA de forma automática resuelve (cierra) automáticamente Incidentes.

135. El criterio de resolución automática es el de cerrar aquellos tickets cuya *'Fecha Límite'* haya expirado.

136. El valor del campo *'Resolución'* asignado a los Incidentes mediante autocierres es *'Sin respuesta'*.

137. Un Incidente cerrado puede gestionarse mediante su búsqueda y posterior edición.

138. La fecha de cierre automática se establece partiendo de la fecha límite del ticket y en base al campo peligrosidad, añadiendo el número de días a la fecha de creación de acuerdo a la siguiente tabla:

Situación	Sin actividad	Bajo investigación	Solicita información
Peligrosidad	**Número de días**		
Bajo	15	15	15
Medio	30	30	30
Alto	45	45	45
Muy alto	120	120	120
Crítico	180	180	180

Tabla 2: Fecha límite según peligrosidad y situación del ticket para autocierres

9. NOTIFICACIÓN A TERCEROS

139. La notificación a terceros se inicia desde la instancia CENTRAL cuando detecta una de las siguientes condiciones:

   – **Notificación manual:** El incidente tiene marcado uno de los campos de notificación a terceros (bloque Normativa aplicable)

Campo	Organismo notificado	Descripción y detalles
¿Afecta al RGPD?	-	Informativo. No inicia notificación.
Notificar a AGPD	AGPD	Inicia una notificación a la AGPD. Requiere haber indicado que afecta a la RGPD (ver campo anterior).
Notificar al CNPIC	CNPIC	Inicia una notificación al CNPIC.
Categoría del Sistema según ENS	-	Informativo. No inicia notificación.
Requiere intervención del CCN-CERT	CCN-CERT	Inicia una notificación al CCN-CERT.

   – **Notificación automática:** El incidente se notifica a ciertos organismos sólo por estar asociado a organismos específicos.

140. La notificación manual generará una investigación en la instancia tercera, asociada a la copia del incidente original. Durante este paso, la investigación enviará un correo electrónico al organismo original para establecer una comunicación entre ambos. La dirección de correo usada es:

   – La establecida en el campo de configuración `default_notification_email_address` [9] si el organismo dispone de una instancia propia,

   – o la asociada al usuario por defecto de la *constituency* (e.g., `satinet_organismo-de-ejemplo_user`)

141. Si dicha cuenta está siendo *"observada"* por la instancia de LUCIA (sólo aplicable, por tanto, a instancias locales), al recibir el correo emitido por el tercero, se generará un reporte de incidente en la instancia del organismo, de modo que se establece un canal de comunicación bidireccional entre el organismo original y el tercero a través del par Reporte de incidente-Investigación (respectivamente). De no crearse el reporte (e.g., es una cuenta no observada por LUCIA o el organismo no dispone de instancia propia), la comunicación deberá llevarse por correo electrónico. Es posible que estos correos electrónicos lleven adjuntos formularios que deban rellenarse para completar la información como solicite el organismo tercero notificado.

142. La notificación automática replica automáticamente cada incidente en una determinada instancia tercera, sólo por estar vinculado el incidente a un organismo con una naturaleza concreta.

[9] Este parámetro se llamaba `$LuciaFetchmailAccount` en LUCIA REV3.1 y anteriores

143. Ambos modos de notificación son compatibles entre sí. Por ejemplo, un incidente se podría haber notificado automáticamente al CNPIC, y más tarde marcarse para su notificación manual, aplicándose las reglas de ambos (en este caso, inicialmente sólo se crearía la copia del incidente en el CNPIC, y al marcarse como notificación manual, se generaría la investigación y se establecería el canal de comunicación entre ambos organismos).

F.A.Q. (PREGUNTAS Y RESPUESTAS FRECUENTES)

En RT/RT-IR es posible unir y dividir tickets. ¿Es posible hacerlo con tickets de LUCIA?

Mientras que en RT/RT-IR es posible unir y dividir tickets, esta opción está deshabilitada para tickets de LUCIA, al no ser viable su sincronización.

Como alternativa se propone mantener todos los incidentes correlacionados vinculados a una misma investigación o investigaciones. Estos vínculos se pueden ver en un panel en los detalles del incidente.