

Guía de Seguridad de las TIC

CCN-STIC 845D

LUCIA – Manual de Administrador



octubre de 2020

Edita:



© Centro Criptológico Nacional, 2017

Fecha de Edición: octubre de 2020

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

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (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 (CNI), 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 (CCN) en su artículo 9.2.f).

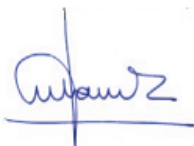
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad 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.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, 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 la comunicación (STIC) 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

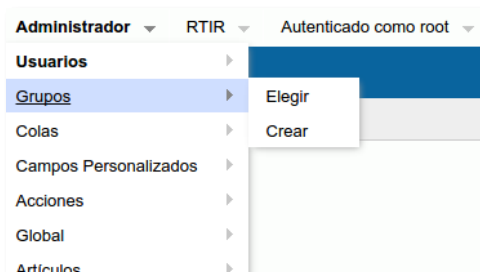
ÍNDICE

1. GESTIÓN DE GRUPOS.....	1
1.1. ATRIBUTOS DE UN GRUPO.....	1
1.2. META INFORMACIÓN DE LOS GRUPOS	1
1.3. ORGANIZACIÓN DE GRUPOS.....	2
1.4. GRUPOS DE SISTEMA E INTERNOS.....	2
1.5. GRUPOS DE TAXONOMÍA.....	2
1.5.1. GRUPOS DE ROL	2
1.5.2. GRUPOS DE ROL POR COLA.....	3
1.6. GRUPOS ORGANIZATIVOS.....	3
1.6.1. MIGRACIÓN DESDE LUCIA REV3.1	4
2. GESTIÓN DE USUARIOS.....	5
2.1. ATRIBUTOS DE UN USUARIO.....	5
2.2. META INFORMACIÓN DE LOS USUARIOS	6
2.3. USUARIOS POR DEFECTO EN LUCIA.....	7
3. GESTIÓN DE COLAS.....	8
3.1. CREACIÓN DE COLAS DE LUCIA.....	8
3.2. MODIFICACIÓN DE COLAS DE LUCIA.....	9
3.3. ATRIBUTOS DE UNA COLA.....	10
3.4. META INFORMACIÓN DE LAS COLAS	10
3.5. OTRAS CONFIGURACIONES.....	11
4. GESTIÓN DE PERMISOS.....	12
4.1. PERMISOS EN LUCIA.....	12
4.2. PERMISOS EN RT/RTIR	12
4.2.1. PERMISOS GLOBALES	12
4.2.2. PERMISOS A NIVEL DE OBJETO (COLAS, CAMPOS PERSONALIZADOS).....	13
4.2.3. TIPOS DE PERMISOS	13
5. USUARIOS GESTORES EXTERNOS	16
6. GESTIÓN DE LA SINCRONIZACIÓN	17
6.1. CONEXIÓN AL SERVIDOR CENTRAL	19
7. GESTIÓN DE CAMPOS PERSONALIZADOS	20
7.1. ATRIBUTOS DE UN CAMPO PERSONALIZADO.....	20
7.2. META INFORMACIÓN DE CAMPOS PERSONALIZADOS.....	21
7.3. CAMPOS PERSONALIZADOS EN LUCIA.....	21
8. GESTIÓN DE NOTIFICACIONES.....	22
9. GESTIÓN DE PLANTILLAS.....	24
10. GESTIÓN DE ARTÍCULOS	26
10.1. GESTIÓN DE CLASES	26
10.1.1. CREACIÓN DE UNA CLASE	27
10.2. GESTIÓN DE TEMAS	29

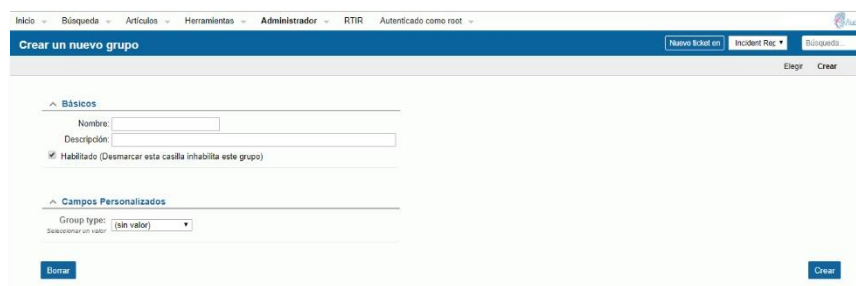
10.3. CAMPOS PERSONALIZADOS	31
11. ELIMINACIÓN DE OBJETOS.....	32
12. OTRAS CONFIGURACIONES.....	34
12.1. PERMISO DE EDICIÓN DE LA FECHA DE RESOLUCIÓN	34
12.2. IDIOMAS DISPONIBLES.....	34
13. GESTIÓN DE LA CONFIGURACIÓN.....	35
14. INSTANCIAS VSOC	36
F.A.Q. (PREGUNTAS Y RESPUESTAS FRECUENTES).....	37
ANEXO A. PERMISOS EN RT	38
ANEXO A.1. PERMISOS DE COLAS	38
ANEXO A.2. PERMISOS DE GRUPOS.....	42
ANEXO A.3. PERMISOS GLOBALES	42
ANEXO B. EXPORTACIÓN DE TICKETS EN FORMATO XML	44
ANEXO B.1. PARÁMETROS DEL SCRIPT DE EXTRACCIÓN	44
ANEXO B.2. EJEMPLOS DE USO	46
ANEXO B.3. ESPECIFICACIÓN DEL FORMATO XML	47
ANEXO C. COPIAS DE SEGURIDAD.....	50
ANEXO D. ACTUALIZACIÓN DEL CERTIFICADO DE SERVIDOR	52
ANEXO D.1. CERTIFICADOS PROPIOS AUTOFIRMADOS.....	52
ANEXO D.2. CERTIFICADOS EXTERNOS	53
ANEXO D.3. INSTALACIÓN DE CERTIFICADOS	53

1. GESTIÓN DE GRUPOS

1. Para gestionar los grupos de LUCIA es necesario identificarse en el sistema usando el usuario `root` del sistema.
2. A través del menú *Administrador* se accede a la página de gestión de grupos.



3. Al pulsar en la opción de *Crear*, se mostrará la siguiente pantalla:



4. Si se escoge la opción *Editar*, la pantalla es idéntica, con los atributos rellenos con los valores del grupo a editar.

1.1. ATRIBUTOS DE UN GRUPO

5. Para la creación de un grupo es necesario especificar el nombre del mismo y, opcionalmente, una breve descripción. Se ha de dejar marcada la opción *Habilitado*. En caso contrario, a pesar de haberse creado no podría ser utilizado. El atributo *Group type* sólo se rellena cuando se trate de un grupo especial denominado *Empresa Externa* que se tratará posteriormente en el punto 5 “Usuarios gestores externos”. Finalmente se pulsará sobre *Crear* o *Guardar Cambios*.

1.2. METAINFORMACIÓN DE LOS GRUPOS

6. Entrando en un grupo existente se encuentran disponibles los siguientes menús:
 - *Básicos*: Datos generales del grupo.
 - *Miembros*: Usuarios o grupos que pertenecen a este grupo.
 - *Pertenencias*: Grupos a los que pertenece este grupo.
 - *Permisos del grupo*: Permisos de otros grupos sobre este grupo.
 - *Permisos de usuario*: Permisos de usuarios sobre este grupo.
 - *Historial*: Histórico de acciones ejecutadas sobre este grupo.

7. Consulte el punto 1.3 para conocer las restricciones que debe tener en cuenta a la hora de modificar los grupos definidos por LUCIA.
8. Los grupos de *Empresas Externas* se tratarán posteriormente.

1.3. ORGANIZACIÓN DE GRUPOS

9. Aunque RT/RTIR no hace distinción en los grupos definidos por el usuario, en LUCIA se tratan los grupos a dos niveles diferentes¹: *Grupos de taxonomía* y *grupos organizativos*. Paralelamente existen otros *grupos de sistema* que se usan internamente por LUCIA.
10. Los *grupos de taxonomía* son una serie de grupos con permisos asignados a diferentes objetos. Dentro de estos grupos existen dos subtipos: *Grupos de rol* y *grupos de rol por cola*.
11. Los *grupos organizativos* son los grupos que cada organización u organismo puede definir para agrupar a sus usuarios.
12. La forma de trabajar y asignar permisos a los usuarios es haciéndolos miembros de estos grupos, y haciendo dichos grupos miembros de distintas combinaciones de *grupos de taxonomía*. Más detalles en el punto 1.6.

1.4. GRUPOS DE SISTEMA E INTERNOS

13. Se trata de ciertos grupos especiales definidos para tareas específicas del sistema.
14. Estos grupos no deben modificarse ni se debería añadir o eliminar usuarios de los mismos.
15. Los grupos son:
 - *LUCIA_System*
 - *REST*
 - *CronUsers*
 - *Sync*

1.5. GRUPOS DE TAXONOMÍA

1.5.1. GRUPOS DE ROL

16. Estos *grupos de rol*, cuyo nombre tiene el formato *RoleGroup_<NombreDeRol>*, contienen, en términos generales, los permisos sobre los campos necesarios para poder utilizar LUCIA.
17. Se definen cuatro roles:
 - *ReadOnly*, con permisos solo para la lectura, no modificación, de los campos personalizados.

¹ A partir de la versión LUCIA REV4.0

- *CreationTeam* (solo en LUCIA Central), *DutyTeam* y *ExternalVisibility*, idénticos a este nivel pero necesarios para separar privilegios a nivel de colas, con permisos para modificar los campos personalizados.
- *Rest* similar a los tres anteriores, pero dedicado a los usuarios que interactúan con LUCIA a través de la interfaz REST.

1.5.2. GRUPOS DE ROL POR COLA

18. Estos grupos asignan privilegios específicos para cada cola concreta de LUCIA, en base al rol que tuvieran (ver 1.5.1). Su nombre tiene el formato *RoleQueueGroup_<NombreDeRol>_<NombreDeCola>*.
19. Aquí los roles sí que tienen una diferenciación mucho más clara:
 - *ReadOnly*, solo permite la consulta de tickets en la cola y sus comentarios.
 - *CreationTeam* (solo en LUCIA Central), con permisos para creación y modificación de tickets.
 - *DutyTeam*, con los permisos para crear, modificar, comentar y ser propietario de tickets.
 - *ExternalVisibility*, similar a *DutyTeam* pero específico para que compañías externas puedan acceder a tickets específicos a los que normalmente no tendrían acceso.
 - *Rest*, con los permisos necesarios para que los usuarios de tipo *rest* puedan interactuar (crear, modificar, comentar) con los tickets de LUCIA.

1.6. GRUPOS ORGANIZATIVOS

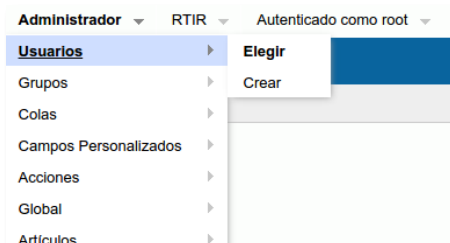
20. Estos son los grupos definidos por cada organismo/organización para gestionar el acceso de los diferentes usuarios a las colas y tickets.
21. Pueden crearse tantos como se consideren necesarios, y con el nombre que se desee, procurando no interferir con las nomenclaturas de los *grupos de taxonomía*.
22. Los usuarios operadores serán miembros de estos grupos. Por mantener un orden y simplificar el mantenimiento y gestión de grupos y usuarios, se desaconseja encarecidamente añadir usuarios directamente a los *grupos de taxonomía*.
23. Para asignar unos permisos u otros a dichos grupos de usuario, bastará con hacerles miembros de los diferentes grupos de taxonomía. Por ejemplo, un grupo podría ser miembro de los grupos *RoleQueueGroup_DutyTeam_Incident Reports – ORGANISMO*, *RoleQueueGroup_DutyTeam_Investigations – ORGANISMO* y *RoleQueueGroup_ReadOnly_Incidents – ORGANISMO*, si deseásemos que los operadores de dicho grupo tengan total control sobre las colas de investigaciones y reportes de incidentes de *ORGANISMO* pero solo lectura de sus incidentes.

1.6.1. MIGRACIÓN DESDE LUCIA REV3.1

24. Esta estructura de grupos se ha introducido con *LUCIA REV4.0* y difiere de la definida en versiones anteriores, requiriendo un proceso de migración.
25. Esta migración se intenta realizar de forma automática en la medida de lo posible durante el proceso de instalación. Todos estos grupos anteriores, a excepción de los *grupos de sistema* existentes (e.g., *LUCIA_System*), se migrarán como *grupos organizativos*. Sin embargo, si se habían hecho cambios específicos en alguno de los grupos existentes en *LUCIA REV3.1* es posible que sea necesario revisar manualmente la nueva configuración.

2. GESTIÓN DE USUARIOS

26. Para gestionar los usuarios de LUCIA es necesario identificarse en el sistema usando el usuario `root`.
27. A través del menú *Administrador* se accede a la página de gestión de usuarios.



28. Al hacer clic en la opción de *Crear*, se muestra la siguiente pantalla:

29. Si se escoge la opción *Editar* o se selecciona un usuario ya creado, la pantalla es idéntica pero los atributos ya contienen los valores de los atributos del usuario que se está editando.
30. Nota: Para todo usuario no perteneciente al sistema que interactúe con LUCIA, por ejemplo, enviando un correo y por tanto generando un *Reporte de Incidente* o a los destinatarios de una *Investigación*, por defecto se creará automáticamente usuario limitado. Este usuario no podrá acceder al sistema y se utiliza internamente para relacionar los tickets en los que se encuentre involucrado.

2.1. ATRIBUTOS DE UN USUARIO

31. Una vez cumplimentados los atributos obligatorios y aquellos que se estimen oportunos de los atributos opcionales, se debe pulsar el botón *Crear* o *Guardar Cambios*.

32. Cuadro de Identidad:

- *Nombre de usuario*: Es el único campo requerido junto con la contraseña, puede ser desde un nombre descriptivo hasta una dirección de correo.
- *Correo*: En el caso de que el usuario quiera recibir notificaciones del sistema, tales como correos o comentarios de los casos, se debe establecer una dirección. Dicha dirección no debe existir previamente en el sistema².
- *Nombre real*: Nombre del usuario completo. Es interesante sobre todo para aquellos usuarios que vayan a gestionar casos desde la plataforma, ya que puede llegar a ser usado por el sistema para establecer el origen (*from*) de los mensajes o reflejar quién ha hecho modificaciones en los casos.

33. Cuadro de Control de acceso: Define los derechos básicos del usuario en el sistema:

- *Permitir a este usuario acceder a RT*: Permite al usuario acceder al sistema a través del interfaz web.

Un usuario creado automáticamente al interactuar con LUCIA tendrá este permiso habilitado, pero al no tener una contraseña definida no podrá acceder. Si se define una contraseña, el usuario solo podrá ver la vista de RT *SelfService*, una interfaz reducida que sólo lista los tickets de los que el usuario es *Solicitante*.

Para cualquier usuario, si se elimina este permiso el usuario quedará deshabilitado no pudiendo ni acceder ni interactuar con LUCIA.

- *Asignar a este usuario permisos adicionales (Privilegiado)*: Este derecho convierte a un determinado usuario en privilegiado, lo cual le da acceso a la interfaz web completa, permitiendo además poder darle permisos sobre las distintas colas de RT. Ser usuario privilegiado no significa ser usuario root del sistema.

2.2. METAINFORMACIÓN DE LOS USUARIOS

34. Para cada usuario existente se encuentran disponibles los siguientes menús:

- *Básicos*: Datos generales del usuario.
- *Pertenencias*: Grupos a los que pertenece el usuario directa o indirectamente.
- *Historial*: Histórico de las acciones realizadas sobre el usuario.
- *RT de un vistazo*: Disposición de la página de inicio en LUCIA.
- *Paneles en el menú*
- *Claves privadas*: Claves PGP del usuario (deshabilitado en la versión actual).
- *Resumen de usuario*: Resumen de los datos del usuario.

35. Como se mencionaba en el punto 1.6 “Grupos organizativos”, los usuarios que vayan a gestionar tickets de LUCIA deberán pertenecer a uno o varios *grupos*

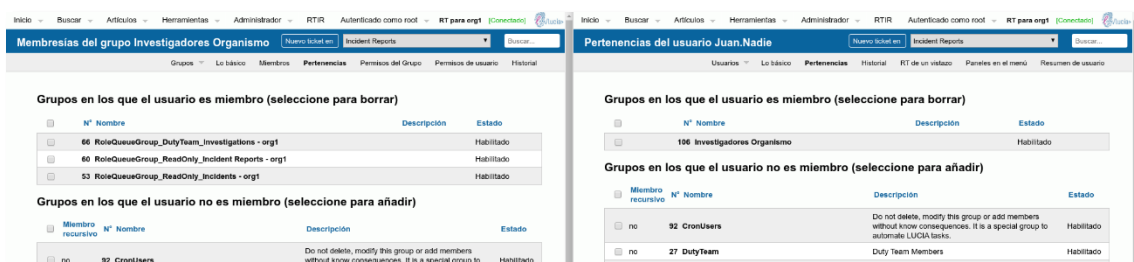
² Un truco para asignar a dos usuarios la misma dirección de correo consiste en definirla directamente en la base de datos `rt4` sobre la tabla `Users`.

organizativos para acceder a dichos tickets. En ningún caso deberán pertenecer directamente a *grupos de sistema* o de *taxonomía*.

36. Los *usuarios de sincronización* y los *usuarios del sistema* (grupo *LUCIA_System*), al ser generados automáticamente, ya son establecidos al grupo correspondiente y no han de ser modificados.

2.3. USUARIOS POR DEFECTO EN LUCIA

37. Con la instalación de LUCIA se crean los usuarios *rest* y *rtcronuser* de forma automática que no han de ser modificados bajo ningún concepto para no alterar el correcto funcionamiento de la herramienta.
38. La contraseña de *rtcronuser* no puede ser modificada porque dicho usuario está asociado a un usuario del sistema con el mismo nombre.
39. Existe un usuario *operador* que se crea con la instalación. Por defecto, no tiene visibilidad sobre ninguna cola puesto que no está asignado a ningún grupo. Si desea que tenga visibilidad sobre los Incidentes y/o notificaciones SAT-INET, SAT-SARA y/o SAT-ICS, se debe añadir su pertenencia a los grupos correspondientes (ver punto 1.5).
40. En el siguiente ejemplo se muestra cómo el usuario ha sido añadido a un grupo con permisos para crear y modificar investigaciones pero solo consultar reportes e incidentes de la visibilidad *org1*:



3. GESTIÓN DE COLAS

41. Desde LUCIA REV4.0 la agrupación de tickets, permisos, etc., queda definida a nivel de cola, abandonándose el concepto de *visibilidad (constituency)* que queda relegado a una mera forma de clasificación organizativa de colas.

3.1. CREACIÓN DE COLAS DE LUCIA

42. Las colas de LUCIA engloban una serie de propiedades y procesos para su correcto funcionamiento. Aunque es posible realizar la mayoría de los pasos desde la interfaz de usuario, se recomienda utilizar los mecanismos proporcionados a través de LUCIA para ello.
43. Estos procesos, además de crear las colas en sí, crearán una serie de *grupos de taxonomía* (ver punto 1.5.2) y asignarán los campos específicos de LUCIA, entre otras acciones.
44. En LUCIA REV4.0 la creación de colas se realiza a través de ficheros de configuración/especificación y la utilidad `run-commands`.
45. La definición de colas se puede hacer a través bien de ficheros YAML³ o de ficheros JSON⁴. Estos ficheros contienen en su primer nivel una lista (*array*) de objetos con dos atributos:
- Una clase (propiedad **class**) con un valor concreto `RT::Extension::Lucia::Core::Service::Commands::CreateAndSetupLuciaQueue`
 - Los argumentos (propiedad **args**) específicos para la cola a crear:
 - **queue_name**: (Obligatorio) El nombre de la cola a crear/modificar.
 - **queue_lifecycle**: (Obligatorio) El ciclo de vida de la cola (uno de los valores `LUCIA_incident_reports`, `LUCIA_investigations`, `LUCIA_SAT_incidents` o `LUCIA_incidents`).
 - **organization_id**: (Obligatorio) El nombre identificativo del organismo responsable de esta cola⁵.
 - **queue_description**: Descripción opcional (pero recomendado) para la cola.
 - **synchronization**: Para colas sincronizables (solo ciclos de vida de incidentes) se definen sus propiedades en este bloque:
 - **notification_email_address**: Dirección de correo a utilizar para las notificaciones relacionadas con tickets de esta cola (en notificación a terceros; consultar guía CCN-STIC 845A, Manual de usuario)

³ <https://yaml.org/spec/1.1/>

⁴ <https://www.json.org/json-en.html>

⁵ Puede variar para instancias con varios organismos, como las instancias VSOC. Ver apartado 14, "Instancias VSOC".

46. En el siguiente ejemplo YAML se puede ver la configuración de tres colas diferentes: Una de *incidentes*, una de *reportes de incidente* y una de *investigaciones*. Puede usarse como plantilla si se desea definir manualmente nuevas colas de LUCIA.

YAML: colas.yml

```
- class: RT::Extension::Lucia::Core::Service::Commands::CreateAndSetupLuciaQueue
  args:
    queue_name: "Incidents - ORGANISMO"
    queue_lifecycle: "LUCIA_incidents"
    organization_id: "ORGANISMO"
    queue_description: "Cola de incidentes de ORGANISMO"
    synchronization:
      notification_email_address: "incidentes@organismo.org"

- class: RT::Extension::Lucia::Core::Service::Commands::CreateAndSetupLuciaQueue
  args:
    queue_name: "Incident Reports - ORGANISMO"
    queue_lifecycle: "LUCIA_incident_reports"
    organization_id: "ORGANISMO"
    queue_description: "Cola de reportes de incidentes de ORGANISMO"

- class: RT::Extension::Lucia::Core::Service::Commands::CreateAndSetupLuciaQueue
  args:
    queue_name: "Investigations - ORGANISMO"
    queue_lifecycle: "LUCIA_investigations"
    organization_id: "ORGANISMO"
    queue_description: "Cola de investigaciones de ORGANISMO"
```

47. Para aplicar estas definiciones, se utilizará la utilidad Perl `run-commands` incluida con LUCIA (asumiendo que la definición está en un fichero `colas.yml`)

bash

```
perl -I/opt/rt4/lib \
/opt/rt4/local/plugins/RT-Extension-Lucia-Core/sbin/run-commands colas.yml
```

3.2. MODIFICACIÓN DE COLAS DE LUCIA

48. Los atributos generales de la cola (aquellos definidos en RT; detallados en el punto 3.3) pueden editarse desde el propio RT/RTIR⁶. Se puede acceder a su edición desde el menú *RT* → *Administrador* → *Colas* → *Elegir*, seleccionando la cola correspondiente en el listado.
49. Los atributos específicos de LUCIA necesitarán cambiarse desde un terminal. Para ello habrá que editar un fichero similar al de definición de colas con los atributos que queramos modificar, identificando por nombre la cola a modificar (Nota: No se debe modificar el ciclo de vida). Por ejemplo, si quisiéramos modificar la dirección de correo de notificación en la cola de incidentes del ejemplo en el punto anterior:

YAML: cambiosCola.yml

```
- class: RT::Extension::Lucia::Core::Service::Commands::CreateAndSetupLuciaQueue
  args:
    queue_name: "Incidents - ORGANISMO"
    queue_lifecycle: "LUCIA_incidents"
    organization_id: "ORGANISMO"
    synchronization:
      notification_email_address: "notificacion.incidentes@organismo.org"
```

⁶ Requerirá un usuario con los permisos para modificar colas, como puede ser el usuario *root*.

bash

```
perl -I/opt/rt4/lib \  
/opt/rt4/local/plugins/RT-Extension-Lucia-Core/sbin/run-commands cambiosCola.yml
```

3.3. ATRIBUTOS DE UNA COLA

50. Los atributos generales disponibles son:

- *Nombre de la cola*: Nombre descriptivo. Debe ser corto.
- *Descripción*: Breve descripción de la cola.
- *Ciclo de vida (Lifecycle)*: Identifica el tipo de ticket por cola. Se utilizan los valores ⁷ *LUCIA_incidents*, *LUCIA_SAT_incidents*, *LUCIA_incident_reports* y *LUCIA_investigations*.
- *Etiqueta de asunto*: Es la etiqueta que se utilizará para crear el *Asunto* de los tickets de la cola, los cuales tendrán un asunto como el siguiente: *[ETIQUETA #idcaso]*. Si no se establece ningún valor utilizará el establecido por defecto en el sistema: *[NombreInstancia #idcaso]*. Se recomienda no modificar este valor si va a haber una comunicación por correo electrónico entre instancias (como es el caso por ejemplo de la notificación a terceros).
- *Orden de clasificación*: Orden en el que se clasifica la cola.
- *Dirección de respuesta*: Dirección de correo que utilizará el sistema para enviar los mensajes de correo de los tickets.
- *SLA (Service Level Agreement)*: Actualmente deshabilitado.
- *Dirección de respuesta y Dirección de comentario*: Direcciones de correo que utilizará el sistema para enviar las respuestas y los comentarios de los tickets.
- *RTIR Constituency (Visibilidad)*: Visibilidad a la que se le asigna la cola. Actualmente en desuso para LUCIA.

3.4. METAINFORMACIÓN DE LAS COLAS

51. Entrando en una cola existente se encuentran disponibles los siguientes menús:

- *Básicos*: Datos generales de la cola.
- *Observadores*: Son usuarios o direcciones de correo electrónico que recibirán actualizaciones del caso por correo. Pueden establecerse en *Cc* o *Admin Cc*, siendo la única diferencia que los *Admin Cc* podrán modificar los tickets.
- *Plantillas*: Plantillas personalizadas para esta cola.
- *Acciones*: Scripts de RT que aplicarán sobre tickets de esta cola.
- *Campos Personalizados*: Campos personalizados para los tickets de esta cola.
- *Permisos del grupo*: Permisos de los grupos sobre los tickets de la cola.

⁷ Desde LUCIA REV4.0. Previamente se utilizaban los definidos por RTIR *incidents*, *incident_reports* e *investigations*.

- *Permisos de usuario*: Permisos de los usuarios sobre los tickets de la cola.
- *Historial*: Histórico de acciones sobre la cola.
- *Valores por defecto*: Permite reiniciar los campos personalizados al valor por defecto

3.5. OTRAS CONFIGURACIONES

52. Adicionalmente será necesario aplicar otras configuraciones sobre las colas:

- *Correo electrónico*: Para operaciones de notificación será necesario configurar dos direcciones de correo para notificaciones internas en los parámetros de configuración `%lucia_rtbase_email_address_for_queue`⁸ y `%lucia_rtbase_email_address_alias_for_queue`⁹ (los originales y sus alias, respectivamente). Estos parámetros por defecto se definen en los ficheros `/opt/rt4/local/etc/lucia_rtbase_email_address_for_queue_Config.pm` y `/opt/rt4/local/etc/lucia_rtbase_email_address_alias_for_queue_Config.pm`. Ambas direcciones no pueden ser iguales (por una imposición de diseño para evitar bucles en algunos clientes de correo la dirección de origen y destino no pueden coincidir; de ahí la necesidad de utilizar alias de las cuentas).

⁸ En LUCIA REV3.1 y anteriores: `%LuciaTicketCategoryEmailAddresses`.

⁹ En LUCIA REV3.1 y anteriores: `%LuciaTicketCategoryEmailAddressesAliases`.

4. GESTIÓN DE PERMISOS

53. Los permisos permiten a un usuario, grupo o rol (todos los usuarios, usuarios privilegiados, propietarios, observadores...) del sistema hacer algún tipo de acción. Los permisos se pueden establecer en varios niveles, a nivel de toda la instancia de LUCIA, o bien a nivel de cada uno de los objetos (cola, campo personalizado, etc.). Hay que tener en cuenta también que la tabla de permisos para un usuario se construye desde los más restrictivos a los más generales, es decir, si un usuario tiene permiso de acceso a los valores de los campos personalizados a nivel global, incluso cuando a nivel de un determinado campo personalizado no se le otorguen permisos, el usuario podrá ver y modificar dichos valores en los casos en los que se aplique ese campo personalizado.

4.1. PERMISOS EN LUCIA

54. Como se indicaba en el punto 1.6 “Grupos organizativos”, para la gestión específica de permisos sobre LUCIA la recomendación es agregar *grupos organizativos* como miembros de los *grupos de taxonomía* gestionados por LUCIA.

4.2. PERMISOS EN RT/RTIR

55. Con la instalación de LUCIA no es necesario modificar los permisos globales, por grupos o por usuarios. Basta con hacer que los grupos y usuarios creados manualmente pertenezcan a uno de los grupos predefinidos.

56. No obstante, a continuación, se describe el funcionamiento interno.

4.2.1. PERMISOS GLOBALES

57. La gestión de permisos a nivel global es accesible a través de *Administrador* → *Global* → *Permisos del Grupo* para gestionar permisos a grupos. Aunque se recomienda la gestión de permisos a nivel de grupos, para gestionar permisos globales a usuarios, se accede a través de *Administrador* → *Global* → *Permisos de Usuario*.

4.2.1.1. PERMISOS PARA BÚSQUEDAS

58. Para permitir a los usuarios gestionar sus búsquedas personalizadas (almacenarlas, cargarlas y borrarlas), se deben conceder los siguientes permisos, repartidos en las tres pestañas existentes, al grupo *Privilegiado* desde *Administrador* → *Global* → *Permisos del Grupo*:

- *LoadSavedSearch*: Permitir carga de búsquedas guardadas.
- *CreateSavedSearch*: Permitir la creación de búsquedas guardadas.
- *ShowSavedSearches*: Ver búsquedas guardadas.
- *EditSavedSearches*: Crear, modificar y eliminar búsquedas almacenadas.

4.2.1.2. PERMISOS PARA MODIFICACIÓN DEL PROPIO USUARIO

59. Para permitir a los usuarios modificar sus propios datos (incluyendo su contraseña) se debe conceder el siguiente permiso, situado en la pestaña *Permisos para el staff*, al grupo *Privilegiado* desde *Administrador* → *Global* → *Permisos del Grupo*:

- *ModifySelf*: Modificar la propia cuenta RT.

4.2.2. PERMISOS A NIVEL DE OBJETO (COLAS, CAMPOS PERSONALIZADOS)

60. La gestión de permisos de usuarios o grupos o de roles en estos casos, es necesario acceder al objeto sobre el que requiere gestionar los permisos, por ejemplo a una cola determinada. En el menú del objeto existen dos opciones *Permisos de Grupos* y *Permisos de usuarios*.

4.2.3. TIPOS DE PERMISOS

61. Una vez seleccionado una de las dos opciones (usuario o grupo), se accede a la página que permite establecer los permisos, en este caso para otorgar *Permisos de Grupo*. En esta página a la izquierda se pueden seleccionar los tres tipos de objetos a los que puede conceder permisos divididos en tres niveles:

- *Sistema*:
 - *Todos*: Todos los usuarios del sistema.
 - *Privilegiado*: Usuarios privilegiados independientemente de que estén o no en un grupo.
 - *No Privilegiado*: Usuarios no privilegiados del sistema
- *Roles*:
 - *AdminCc*
 - *Cc*
 - *Propietario*
 - *Solicitante*

- *Usuarios y Grupos de usuarios:* el primer caso aparece cuando estemos otorgando permisos a grupos y el segundo cuando lo estemos haciendo a usuarios.

62. En la parte central de la página se muestran los permisos que se pueden otorgar divididos en 3 categorías:

- *Permisos generales:* Permiten realizar acciones básicas sobre la cola y los tickets, como por ejemplo crear un caso, hacer un comentario, responder un caso, ver los valores de los campos personalizados, ver la cola...

RT para CCN-CERT

Modificar permisos de usuario para la cola Incidents

Nuevo caso en Incidents

Colas Básicos Observadores Plantillas Acciones Campos Personalizados Permisos del Grupo Permisos de usuario Historial

USUARIOS

AÑADIR USUARIO

Añadir derechos para este usuario

Privilegios generales Privilegios para el staff Privilegios para los administradores

☐ Comentar sobre los casos	CommentOnTicket
☐ Crear casos	CreateTicket
☐ Responder a los casos	ReplyToTicket
☐ Validarse como solicitante de caso o CC del caso o cola	Watch
☐ Ver cola	SeeQueue
☐ Ver resumen del caso	ShowTicket
☐ Ver valores de campos personalizados	SeeCustomField

Guardar Cambios

- *Permisos para el personal:* Son los permisos que dan derecho a realizar sobre los tickets acciones de gestión, como por ejemplo modificar los campos personalizados, o modificar el ticket (tiempos, estados), poseer un ticket, apropiarse de un ticket asignado a otro usuario, apropiarse de tickets que no estén asignados a nadie y ver los comentarios del ticket.

RT para CCN-CERT

Modificar permisos de usuario para la cola Incidents

Nuevo caso en Incidents

Colas Básicos Observadores Plantillas Acciones Campos Personalizados Permisos del Grupo Permisos de usuario Historial

USUARIOS

AÑADIR USUARIO

Añadir derechos para este usuario

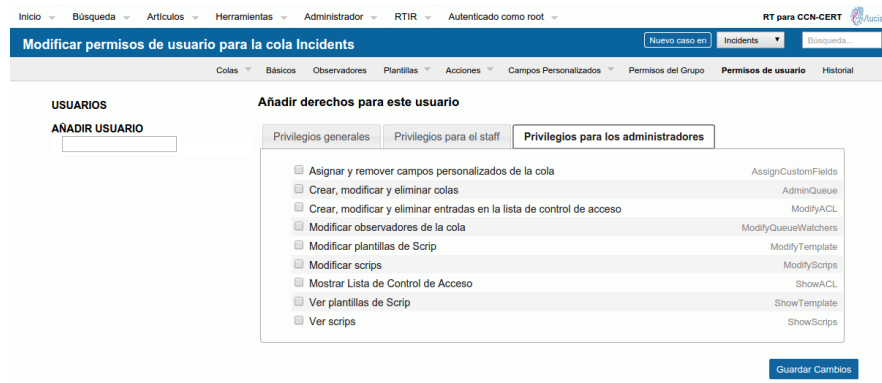
Privilegios generales Privilegios para el staff Privilegios para los administradores

☐ Borrar casos	DeleteTicket
☐ Casos propios	OwnTicket
☐ Coger casos	TakeTicket
☐ Modificar casos	ModifyTicket
☐ Modificar valores de campo personalizado	ModifyCustomField
☐ Modify ticket owner on owned tickets	ReassignTicket
☐ Robar casos	StealTicket
☐ Transferir mensajes fuera de RT	ForwardMessage
☐ Validarse como AdminCc del caso o cola	WatchAsAdminCc
☐ Ver comentarios privados del caso	ShowTicketComments
☐ Ver detalles de los mensajes de correo saliente y sus destinatarios	ShowOutgoingEmail

Guardar Cambios

- *Permisos de administrador:* Son los permisos que permiten realizar acciones de administración sobre la cola, en este ejemplo, o sobre un campo personalizado en el caso en el que se esté definiendo permisos sobre campos personalizados. Algunas de estas acciones permiten asignar nuevos campos personalizados,

crear/modificar/borrar la cola y modificar las acciones que se ejecutan sobre la cola.



- *Ciclo de vida de permisos*: En el caso en el que se defina un ciclo de vida personalizado para una cola, se pueden definir permisos especiales, permiten definir qué y quién no puede pasar un caso de un estado a otro de ese ciclo de vida. En estos casos muestra una nueva pestaña llamada *Cambio de estados*, con la cual se definen los permisos.
63. Para asignar los permisos a un determinado usuario, grupo o rol, se marcan en la parte izquierda sobre qué rol se desea aplicar dicho permiso y en la ventana central marcar los permisos para posteriormente hacer clic en *Guardar Cambios*.

5. USUARIOS GESTORES EXTERNOS

64. En LUCIA, el concepto *Usuario Gestor Externo* es un usuario sobre el que se desea dar acceso a alguno de los tickets creados manteniendo oculto el resto. Por ejemplo, una empresa subcontratada que brinda apoyo en la resolución de ciertos incidentes a un organismo pero que el organismo no quiere que vea el resto de los incidentes.
65. Para crear un nuevo gestor externo, se creará un *grupo organizativo* nuevo, estableciendo el valor de su campo *Tipo de grupo* a *Compañía externa*, y seleccionando la clase de LUCIA adecuada en el campo *Clase de LUCIA* (solo los grupos que coincidan en su *Clase de LUCIA* con la establecida para una cierta cola podrán ser seleccionables como gestores externos de los tickets de dicha cola; por ejemplo, una cola con una *clase de LUCIA SATINET* solo podrá ser externamente gestionada por miembros de compañías externas para la clase SATINET).
66. El siguiente paso sería, como con cualquier *grupo organizativo*, asignarlo como miembro de los *grupos de rol por cola* de interés (**importante: aquellos con rol ExternalVisibility**)
67. Todos aquellos usuarios miembros de dicho grupo y que hayan sido seleccionados en el campo *Visibilidad externa* de un ticket podrán acceder a dicho ticket.

6. GESTIÓN DE LA SINCRONIZACIÓN

69. La sincronización en LUCIA sólo afecta a las colas de Incidentes propios del Organismo y las colas del SAT. El resto de colas, pertenecientes a IR e INV que se creen no se sincronizan.
70. Por defecto y aunque una cola de incidentes de LUCIA se haya creado como sincronizable, será rechazada desde el servidor. Contacte con el CCN-CERT para solicitar que se habilite su sincronización.
71. Para la *sincronización unidireccional de metadatos de los incidentes propios* del organismo, se sincronizan todos los campos excepto *Visibilidad externa, Recordatorios, Campaña, Origen de la Amenaza, ficheros adjuntos, comentarios y campos personalizados añadidos por el organismo*; es decir, permite el envío de incidentes de forma aséptica.
72. Para la *sincronización bidireccional de los incidentes del SAT*, la sincronización es completa de todos los campos de los tickets Incidente excepto *Visibilidad externa, Recordatorios, Campaña, Origen de la Amenaza, Requiere intervención del CCN-CERT y campos personalizados añadidos por el organismo* dado que no existen en la instancia LUCIA Central.

	Unidireccional (propios)	Bidireccional (SAT)
Asunto	✓	✓
Creado	✓	✓
Comienzo	✓	✓
Fecha Límite	✓	✓
Actualizado	✓	✓
Recordatorios		
Propietario	Se envía pero no se replica en el otro extremo	Se envía pero no se replica en el otro extremo
Cola	Se envía pero no se replica en el otro extremo	Se envía pero no se replica en el otro extremo
Peligrosidad y Peligrosidad estimada	✓	✓
Estado	✓	✓
Descripción	✓	✓
IP	✓	✓
Situación	✓	✓
Tipo de Notificación	✓	✓

	Unidireccional (propios)	Bidireccional (SAT)
Tipo de organismo	✓	✓
Clase del Ciberincidente	✓	✓
Tipo del Ciberincidente	✓	✓
Nivel de clasificación	✓	✓
Fiabilidad	✓	✓
Origen de la amenaza		
Campaña		
Reglas de Detección	✓	✓
Visibilidad externa		
¿Afecta al RGPD?	✓	✓
Notificar a AGPD	✓	✓
Notificar al CNPIC	✓	✓
Categoría del sistema según ENS	✓	✓
Requiere intervención del CCN-CERT	✓	
Resolución	✓	✓
Recursos invertidos	✓	✓
Impacto	✓	✓
Causa del incidente	✓	✓
Incidencias durante la Resolución	✓	✓
Número de Sistemas/Usuarios Afectados	✓	✓
Tiempo trabajado	✓	✓
GUID del ticket	✓	✓
Otros campos		
Adjuntos		✓
Comentarios		✓

73. En cualquier caso, se excluyen de la sincronización los *Reportes de Incidentes e Investigaciones* generadas desde la instancia del organismo.
74. En caso de que se den problemas con la sincronización de una determinada acción, tras varios reintentos el sistema avisa del error mediante el envío de un correo con información sobre el fallo a la dirección configurada durante la instalación en el parámetro `OwnerEmail` del fichero `/opt/rt4/etc/RT_SiteConfig.pm`.
75. Estas peticiones fallidas se reintentarán automáticamente cada minuto o cuando se realice alguna otra operación sincronizable (e.g., editar un incidente en una cola sincronizable).
76. Recuerde consultar las notas en el apartado 13 cuando aplique los cambios. Estos cambios de configuración pueden requerir, además, el reinicio de otros servicios de sincronización.

```
bash
```

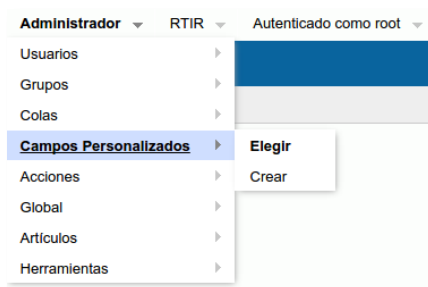
```
systemctl restart lucia_sync_client.service
```

6.1. CONEXIÓN AL SERVIDOR CENTRAL

77. Para conectar al servidor central necesitará configurar los siguientes parámetros:
 - `lucia_sync_client_server_url`: La URL del servidor de sincronización (<https://lucia-rest.ccn-cert.cni.es/sync/>)
 - `lucia_sync_client_rest_user`: El nombre del usuario registrado en el servidor para las operaciones de sincronización.
 - `lucia_sync_client_rest_password`: La contraseña del usuario registrado en el servidor para las operaciones de sincronización.

7. GESTIÓN DE CAMPOS PERSONALIZADOS

78. A la gestión de los campos personalizados se accede a través del menú *Administrador* → *Campos Personalizados*.



79. Al hacer clic en la opción de *Crear*, se mostrará la siguiente pantalla:

80. Si se escoge la opción *Editar*, la pantalla es idéntica, pero los atributos aparecen rellenos con los valores del campo.

81. Para que un campo personalizado esté disponible para el objeto deseado (habitualmente colas), se seleccionará el objeto desde el menú *Administración*, en los detalles del objeto seleccionado, en la página *Campos Personalizados*, y por último marcando el campo que nos interese añadir al objeto y pulsando *Enviar*.

7.1. ATRIBUTOS DE UN CAMPO PERSONALIZADO

82. Los atributos a rellenar son los siguientes:

- **Nombre:** Nombre del campo.
- **Descripción:** Breve descripción del campo.
- **Tipo:** Tipo de valor que recogerá el campo.
- **Tipo de visualización:** El elemento de interfaz que se utilizará para introducir/seleccionar el valor. Solo disponible para campos personalizados ya creados (i.e., en su edición, no en su creación).
- **Aplica a:** Tipo de objeto que podrá disponer del campo.
- **Validación:** Expresión regular de formato.

- *Vincular valores a:* Convertir valores de este campo a hipervínculos a otro servicio.
- *Incluir página:* Incluir contenido de otro servicio web al mostrar este campo.
- *Las categorías se basan en:* Campo en el que se basan las categorías. Solo disponible para campos personalizados ya creados (i.e., en su edición, no en su creación) de tipo seleccionable (seleccionar un valor o selección múltiple).
- *Por defecto valor:* Valor por defecto que tiene el campo. Solo disponible para campos personalizados ya creados (i.e., en su edición, no en su creación) de tipo seleccionable (seleccionar un valor o selección múltiple).
- *Valores:* Valores que tiene el campo. Solo disponible para campos personalizados ya creados (i.e., en su edición, no en su creación) de tipo seleccionable (seleccionar un valor o selección múltiple).

7.2. META INFORMACIÓN DE CAMPOS PERSONALIZADOS

83. Editando un campo personalizado existente se tienen accesos a:

- *Básicos:* Datos generales del campo.
- *Permisos del Grupo:* Permisos de los grupos sobre el campo.
- *Permisos de Usuario:* Permisos de los usuarios sobre el campo.
- *Aplica a:* Objetos a los que aplica el campo.

7.3. CAMPOS PERSONALIZADOS EN LUCIA

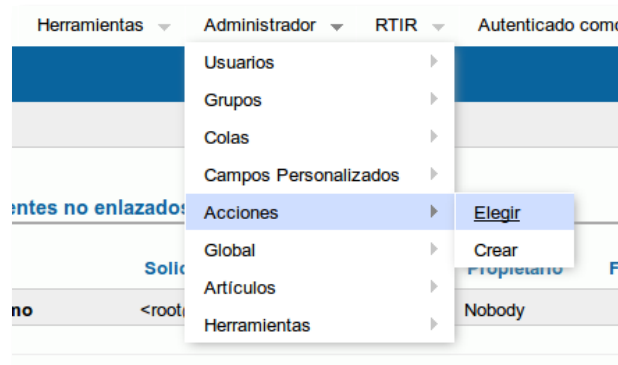
84. Con la instalación de LUCIA se crean una serie de atributos o campos personalizados que no han de ser modificados bajo ningún concepto para no alterar el correcto funcionamiento de la herramienta. Para que la sincronización sea coherente, los valores de los campos de las distintas instancias de LUCIA han de ser comunes.
85. La única modificación permitida sobre los que se ofrecen inicialmente es añadir o quitar valores a los campos *Campaña (Campaign)* y *Origen de la Amenaza (Threat Source)*, puesto que no serán sincronizados entre instancias dado que sus valores difieren.

8. GESTIÓN DE NOTIFICACIONES

86. Por defecto, LUCIA está configurada para notificar automáticamente las siguientes acciones tanto a la cuenta de correo configurada en el sistema como al propietario:

Acción	Scrip asociado
Creación de un Reporte de Incidente o Investigación	<i>[Lucia] Send Create Investigation or Incident report Notification</i>
Creación de un Incidente propio	<i>[Lucia] Send Create ORG Incident Notification</i>
Creación de un Incidente SAT	<i>[Lucia] Send Create SAT Incident Notification</i>
Comentario en un Reporte de Incidente o Investigación	<i>[Lucia] Send Comment Investigation or Incident report Notification</i>
Comentario en un Incidente propio	<i>[Lucia] Send Comment ORG Incident Notification</i>
Comentario en un Incidente SAT	<i>[Lucia] Send Comment SAT Incident Notification</i>
Cierre de un Reporte de Incidente o Investigación	<i>[Lucia] Send Close Investigation or Incident report Notification</i>
Cierre de un Incidente propio	<i>[Lucia] Send Close ORG Incident Notification</i>
Cierre de un Incidente SAT	<i>[Lucia] Send Close SAT Incident Notification</i>
Autocierre de un Incidente propio	<i>[Lucia] Send AutoClose ORG Incident Notification</i>
Autocierre de un Incidente SAT	<i>[Lucia] Send AutoClose SAT Incident Notification</i>
Reapertura de un Incidente propio	<i>[Lucia] Send Reopen ORG Incident Notification</i>
Reapertura de un Incidente SAT	<i>[Lucia] Send Reopen SAT Incident Notification</i>
Reasignación de un Incidente	<i>[Lucia] Send Owner Change Notification</i>

87. Los Scripts que ejecutan estas acciones son accesibles desde el menú *Administrador* → *Acciones* → *Elegir*:



88. Cada una de estas acciones lleva asociada una plantilla de correo que puede ser editada para personalizar el correo enviado.
89. A su vez, estos *scripts* pueden ser deshabilitados para evitar el envío de estas notificaciones. Para ello se debe seleccionar uno en concreto, desmarcar la casilla *Activar* y guardar los cambios.

^ Básicos

Descripción: [Lucia] Send Create INCIDENT INC Notification

Condición: [Lucia] CreateINCIDENTTicket

Acción: [Lucia] SendNotification

Plantilla: Autoreply INCIDENT INC in HTML

Aplica a: Incidents

☒ Activar (Desmarcar esta caja desactiva este scrip)

90. Por defecto estas notificaciones están deshabilitadas¹⁰ para el propietario del incidente, pudiendo llegar a darse el caso de que un usuario reciba dos correos electrónicos para el mismo evento en caso de que su cuenta pertenezca a una lista de distribución configurada como destinatario de incidentes además de tener su correo asociado en LUCIA.
91. Si se desea habilitar o deshabilitar este comportamiento, habrá que establecer a verdadero (para habilitar) o falso (deshabilitar) las notificaciones con el parámetro `$lucia_rtbase_enable_notify_owner`:

Perl

```
Set($lucia_rtbase_enable_notify_owner, 0); # Deshabilitar
Set($lucia_rtbase_enable_notify_owner, 1); # Habilitar
```

¹⁰ Hasta LUCIA REV3.1 estaba habilitado por defecto. Las instancias actualizadas a LUCIA REV4.0 desde LUCIA REV3.1 tendrán habilitado este comportamiento y deberá deshabilitarse explícitamente si así se desea.

9. GESTIÓN DE PLANTILLAS

93. Desde LUCIA REV4.0 las plantillas propias de LUCIA vienen definidas a través del propio código del aplicativo. Tan solo es necesario invocar esta definición desde el cuerpo de la plantilla. La forma que tienen es similar a la siguiente:

Perl/HTML

```
{RT::Extension::Lucia::RtBase::Manager->Instance()->BuildTemplate("LUCIA Create Incident in HTML", $Ticket, $Transaction);}
```

94. Aunque la edición es sencilla, las plantillas de LUCIA llevan incrustado código Perl por lo que hay que tener especial atención en las modificaciones que se realizan. El resto es lenguaje HTML.
95. Una modificación que se recomienda hacer, aunque no es obligatoria, es el pie de firma en las plantillas si se quieren personalizar. De esta manera, se puede incluir información adicional de contacto con el organismo o términos legales en cada notificación que envíe LUCIA por correo electrónico, incluyendo dicho fragmento al final de la plantilla deseada. Por ejemplo:

Perl/HTML

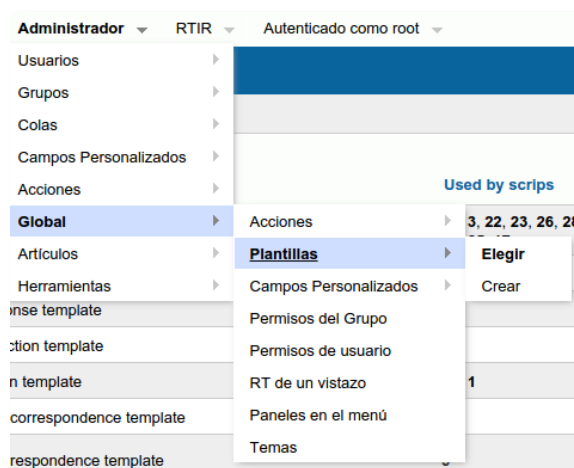
```
{RT::Extension::Lucia::RtBase::Manager->Instance()->BuildTemplate("LUCIA Create Incident in HTML", $Ticket, $Transaction);}
```

<p>

Aviso legal: Este mensaje contiene información CONFIDENCIAL. Si ha recibido este mensaje por error, debe saber que su lectura, copia, uso o divulgación están prohibidos por la Ley. Por ello, le rogamos que nos lo comunique inmediatamente por esta misma vía y proceda a su destrucción. Muchas gracias.

</p>

96. La gestión de las plantillas se realiza accediendo a través del menú *Administrador* → *Global* → *Plantillas*.



97. Las plantillas suministradas por LUCIA de este modo son:

- *LUCIA Admin Comment* y *LUCIA Admin Comment in HTML*
- *LUCIA Autoreply Incident report in HTML*

- *LUCIA Autoreply Investigation in HTML*
- *LUCIA Autoresolved Incident in HTML*
- *LUCIA Changed Owner in HTML*
- *LUCIA Commented Incident in HTML*
- *LUCIA Commented Investigation or Incident report in HTML*
- *LUCIA Correspondence in HTML*
- *LUCIA Create Incident in HTML*
- *LUCIA Create Investigation or Incident report in HTML*
- *LUCIA Reminder Incident in HTML*
- *LUCIA Reopen Incident in HTML*
- *LUCIA Resolved y LUCIA Resolved in HTML*
- *LUCIA Resolved Incident in HTML*
- *LUCIA Resolved Investigation or Incident report in HTML*
- *LUCIA Transaction y LUCIA Transaction in HTML*

10. GESTIÓN DE ARTÍCULOS

99. Los artículos son una forma 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.

100. Internamente se organizan en clases y temas.

10.1. GESTIÓN DE CLASES

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

102. Se puede acceder a la sección de clases desde *Administrador* → *Artículos* → *Clases*.



103. Inicialmente vienen creadas 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.

104. Toda clase consta de los siguientes campos:

- *Nombre de la clase*
- *Descripción*

105. En la pantalla de edición de la clase aparecen también las siguientes opciones:

- *Habilitado*: si está activada

- 'Todos los artículos en esta clase deberían estar listados en un desplegable': si los artículos de esta clase se mostrarán en un desplegable a la hora de responder a los tickets

106. Además, existen unos seleccionables que indican qué partes del artículo serán incluidos en el cuerpo del mensaje. Por defecto vienen seleccionados todos, pero puede editarse desde la configuración de la clase:

- *Incluir nombre del artículo*: Si se debe incluir el nombre del artículo
- *Incluir resumen del artículo*: Si se debe incluir la breve descripción del artículo
- *Incluir campo personalizado 'Response'*
 - *Título*: Si se debe incluir el título del campo (en este caso *Response*)
 - *Valor*: Si se debe incluir el contenido del campo *Response*

107. El campo personalizado *Response* viene incluido en las clases *CCN-CERT* y *ORGANISMO*, pero no es un campo que venga por defecto en una nueva clase.

10.1.1. CREACIÓN DE UNA CLASE

108. Para crear una nueva clase se hará a través de *Administrador* → *Artículos* → *Clases* → *Crear*.

109. Se deben introducir los valores antes descritos y a continuación *Crear*.

110. Como se ha indicado, el campo *Response* no viene añadido por defecto. Para añadirlo, hay que ir a la ficha *Campos Personalizados*:

111. Seleccionarlo y dar a *Enviar*.

Editar campos personalizados para Nueva clase

Nuevo caso en Incident Repc...

Clases Básicos Temas Campos Personalizados Permisos del Grupo Permisos de usuario Aplica a

Campos Personalizados Seleccionados

Campos Personalizados No Seleccionados

#	Nombre	Agregado	Tipo	Pattern	Estado
☒	14 Response	CCN-CERT, ORGANISMO, Templates	Rellenar en un area de texto		Habilitado

Enviar

112. Se recomienda establecer las opciones de qué incluir para dicho campo desde la pestaña *Básicos*:

Modificar la clase Nueva clase

Clases **Básicos** Temas Campos Personalizados

Nombre de la clase: Nueva clase

Descripción:

☒ Habilitado (al desactivar esta casilla se deshabilitará esta clase)

☐ Todos los artículos en esta clase deberían estar listados en un desplegable de la página de respuesta al ticket

Cuando se inserten artículos de esta clase en los correos:

- ☒ Incluir nombre del artículo
- ☐ Incluir resumen del artículo
- ☒ Incluir campo personalizado "Response"
 - ☐ Título
 - ☒ Valor

113. Se pueden añadir otros campos personalizados específicos para artículos, tal y como se indica en el apartado 10.3.

114. Además, para que los artículos se muestren para todas o una determinada cola, se debe marcar desde la pestaña *Aplica a*:

Inicio Búsqueda Artículos Herramientas Administrador RTIR Autenticado como root

RT para ORGANISMO

Modificar objetos asociados para Nueva clase

Nuevo caso en Incident Repc...

Clases Básicos Temas Campos Personalizados Permisos del Grupo Permisos de usuario **Aplica a**

Aplicar globalmente

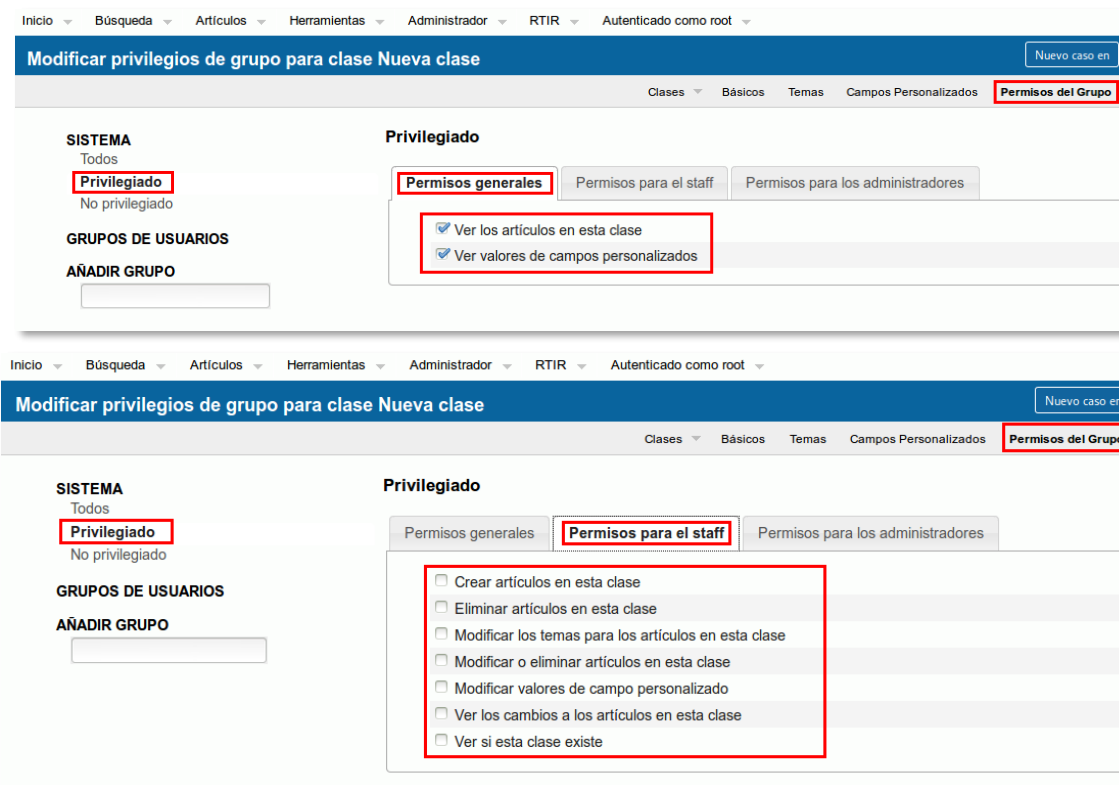
☒ marque esta casilla para aplicar esta clase globalmente a todas las colas.

Colas seleccionadas

Colas no seleccionadas

#	Nombre	Descripción	Dirección	Peligrosidad	DefaultDueIn	Ciclo de vida	Etiqueta de asunto	Estado
☐	3 Incidents		-/-	0-0	0	Incidents		Habilitado
☐	4 Incident Reports		-/-	0-0	0	Incident_reports		Habilitado
☐	5 Investigations		-/-	0-0	0	Investigations		Habilitado

115.Y, por último, se deberán dar los siguientes permisos a los *Usuarios privilegiados* o *grupos organizativos* correspondientes sobre dicha clase desde la pestaña *Permisos de Grupo*:



Inicio ▾ Búsqueda ▾ Artículos ▾ Herramientas ▾ Administrador ▾ RTIR ▾ Autenticado como root ▾

Modificar privilegios de grupo para clase Nueva clase Nuevo caso en

Clases ▾ Básicos Temas Campos Personalizados **Permisos del Grupo**

SISTEMA
 Todos
Privilegiado
 No privilegiado

GRUPOS DE USUARIOS
 AÑADIR GRUPO

Privilegiado

Permisos generales Permisos para el staff Permisos para los administradores

☒ Ver los artículos en esta clase
☒ Ver valores de campos personalizados

Inicio ▾ Búsqueda ▾ Artículos ▾ Herramientas ▾ Administrador ▾ RTIR ▾ Autenticado como root ▾

Modificar privilegios de grupo para clase Nueva clase Nuevo caso en

Clases ▾ Básicos Temas Campos Personalizados **Permisos del Grupo**

SISTEMA
 Todos
Privilegiado
 No privilegiado

GRUPOS DE USUARIOS
 AÑADIR GRUPO

Privilegiado

Permisos generales **Permisos para el staff** Permisos para los administradores

☐ Crear artículos en esta clase
☐ Eliminar artículos en esta clase
☐ Modificar los temas para los artículos en esta clase
☐ Modificar o eliminar artículos en esta clase
☐ Modificar valores de campo personalizado
☐ Ver los cambios a los artículos en esta clase
☐ Ver si esta clase existe

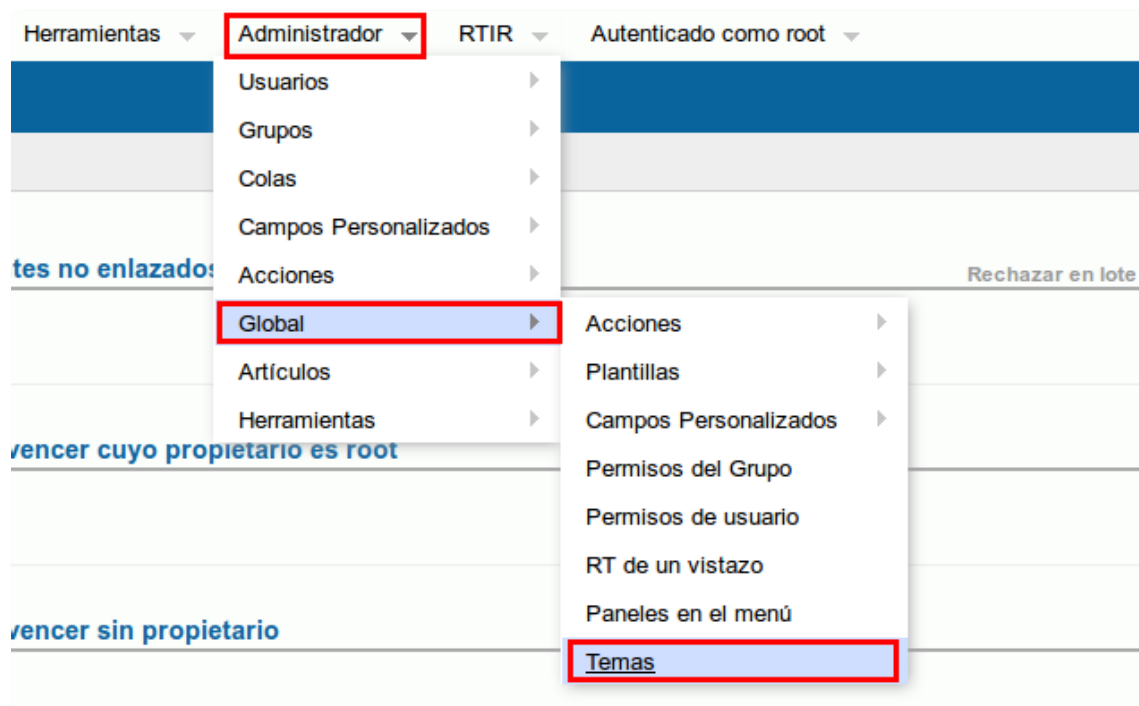
10.2. GESTIÓN DE TEMAS

116.Los temas son otra forma de organizar los artículos. Se pueden entender como una especie de etiquetas para los artículos.

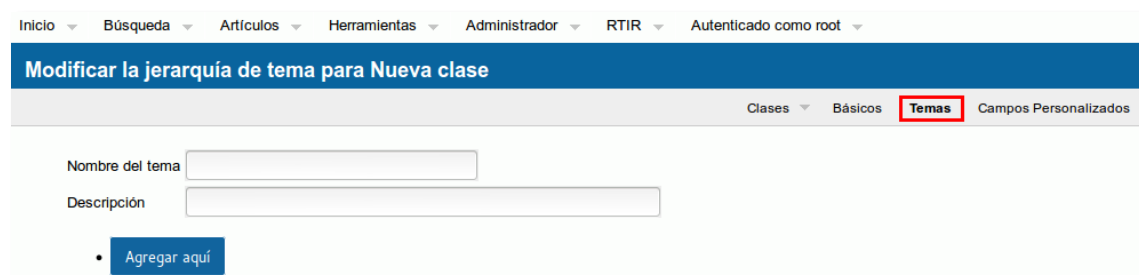
117.Los temas pueden ser de dos tipos:

- *Globales*: aplicables a los artículos de cualquier clase
- *De clase*: aplicables a los artículos de una clase

118. Los temas globales están disponibles para todos los artículos; y cada artículo podrá estar relacionado con temas tanto globales, como específicos de su clase. Pueden ser creados desde *Administrador* → *Global* → *Temas*.

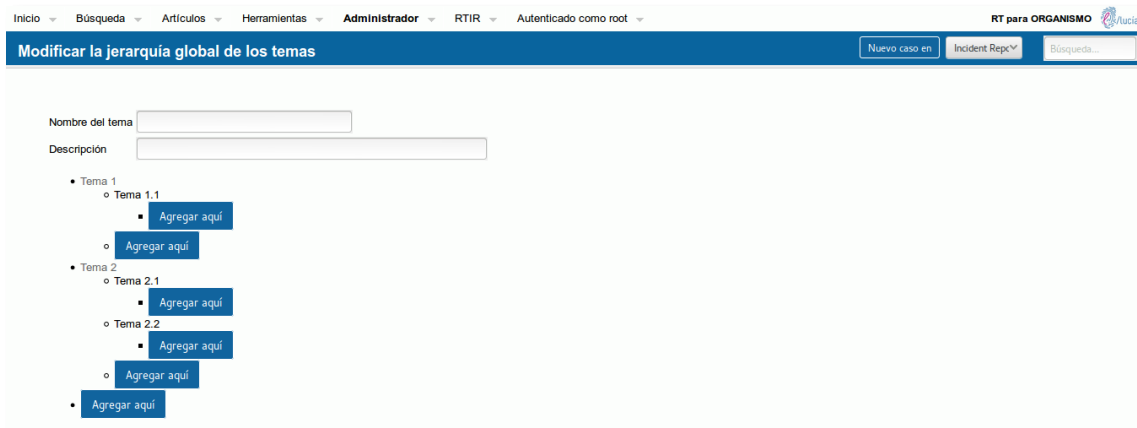


119. Los temas de clase son específicos de esa clase.



120. Todos los temas contienen un nombre y, opcionalmente, una descripción. Además, se organizan jerárquicamente, lo que permite la creación de árboles temáticos que

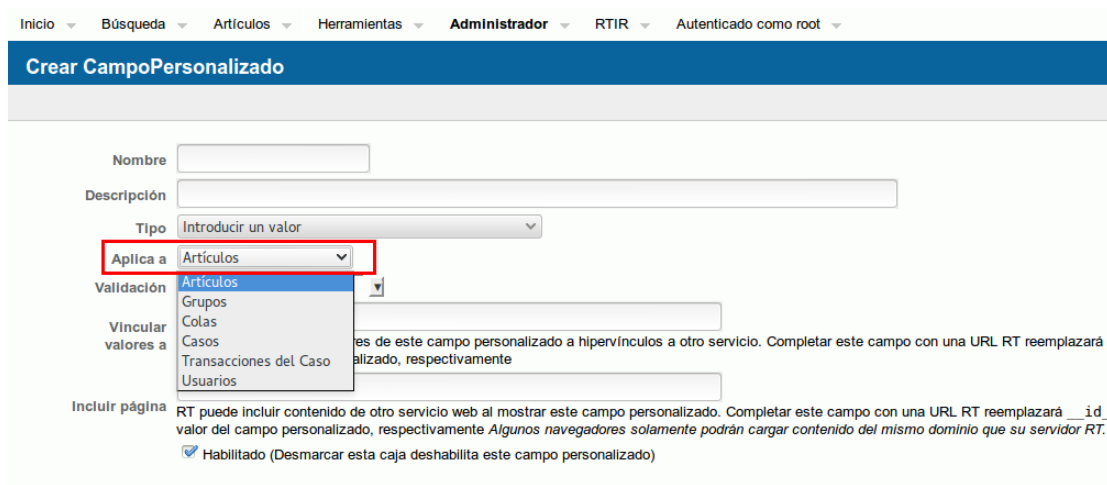
se mostrarán en la creación de artículos para poder seleccionar el o los temas a los que aplica dicho artículo.



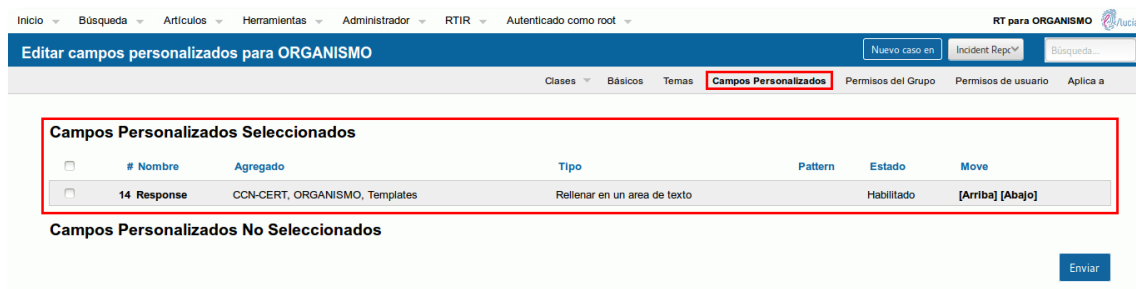
10.3. CAMPOS PERSONALIZADOS

121. Los artículos no tienen un “cuerpo” único, sino que tienen relacionados campos personalizados. Las clases inicialmente creadas tienen incluido el campo *Respuesta* (*Response*).

122. Si se crean nuevas clases, se les puede añadir más campos personalizados que deben haber sido creados indicando que se desea que apliquen a Artículos.



123. Una vez creados los campos, habría que ir a la clase, hacer clic en *Campos Personalizados* y añadirlos.



11. ELIMINACIÓN DE OBJETOS

124.NOTA: Para eliminar incidentes sincronizados, debe utilizar el campo Delete Incident/Borrar Incidente, solo visible por el superusuario.

125.Eliminar objetos, usuarios o tickets, por defecto se encuentra deshabilitado en los menús de LUCIA por ser una práctica no recomendable. No obstante, a continuación, se indican los pasos para permitir eliminar ciertos tickets o usuarios desde la línea de comandos del servidor. El único uso que debe darse a esta funcionalidad es la de eliminación de contenidos creados a modo de pruebas o durante las pruebas de conectividad.

126.La eliminación se hace mediante la herramienta `rt-shredder`. Ésta permite eliminar objetos de base de datos filtrando los elementos mediante un lenguaje similar al de consulta de base de datos.

127.NOTA: Por defecto y como medida de seguridad, la herramienta `rt-shredder` elimina un máximo de diez objetos por ejecución, por lo que es posible que el comando se deba ejecutar varias veces si la consulta supera ese límite. Mediante el argumento `limit`, se permite la modificación de ese límite.

128.La sintaxis del comando `rt-shredder` es:

```
bash
/opt/rt4/sbin/rt-shredder --plugin 'Objeto=arg1,value1;arg2,value2'
```

129.A continuación, se muestran algunos ejemplos:

- Eliminar el ticket 3 de la cola *Incident Reports* - *ORGANISMO*:

```
bash
/opt/rt4/sbin/rt-shredder \
--plugin 'Tickets=query,Queue="Incident Reports - ORGANISMO" and id=3'
```

- Eliminar el ticket 9 de la cola *Incidents* - *ORGANISMO* con sus tickets asociados:

```
bash
/opt/rt4/sbin/rt-shredder \
--plugin 'Tickets=query,Queue="Incidents - ORGANISMO " and id=9;with_linked,TRUE'
```

- Eliminar el usuario habilitado *Prueba*:

```
bash
/opt/rt4/sbin/rt-shredder --plugin 'Users=status,enabled;name,Prueba'
```

130.Cada eliminación que se vaya ejecutar necesita una confirmación:

```
Next 2 objects would be deleted:
RT::Ticket-9 object
```

```
RT::Ticket-4 object
Do you want to proceed? [y/N]
```

131.En el caso de que los criterios introducidos no encuentren ningún resultado, aparecerá el siguiente mensaje:

```
Objects list is empty, try refine search options
```

132.Para obtener más información, se pueden consultar la lista los diferentes *plugins* disponibles en la herramienta con el comando:

```
bash
/opt/rt4/sbin/rt-shredder --plugin list
```

133.Para ver la sintaxis de cada uno de ellos, se ha de ejecutar el comando:

```
bash
/opt/rt4/sbin/rt-shredder --plugin help-NombrePlugin
```

12. OTRAS CONFIGURACIONES

134. En este apartado se recogen configuraciones de LUCIA no englobables en ninguno de los apartados anteriores, aunque no por ello deben ser obviadas, pues pueden resultar de utilidad.

12.1. PERMISO DE EDICIÓN DE LA FECHA DE RESOLUCIÓN

135. Por defecto, LUCIA sólo deja editar la fecha de resolución a usuarios con el permiso *SuperUser*, como por ejemplo *root*. Para modificar este comportamiento y permitir modificar esta fecha a cualquier usuario con permiso de edición sobre el ticket, se editará el parámetro `$lucia_core_allow_modify_resolved` estableciéndolo a `1` (verdadero):

```
Perl
#...
Set($lucia_core_allow_modify_resolved, 1); # Allow to modify the Resolved date
#...
```

12.2. IDIOMAS DISPONIBLES

136. RT por defecto carga las traducciones de todos los idiomas disponibles. Esto supone un fuerte impacto al rendimiento durante la inicialización, especialmente en herramientas de consola. Se puede limitar el conjunto de idiomas a cargar a través del parámetro de configuración `@LexiconLanguages`. En el siguiente ejemplo se limita al castellano y al inglés:

```
Perl
#...
Set(@LexiconLanguages, qw(es en)); # Castellano (es) e inglés (en)
#...
```

13. GESTIÓN DE LA CONFIGURACIÓN

137. La mayoría de los parámetros de configuración se encuentra en ficheros del sistema de ficheros de RT.

138. Existen varios ficheros y directorios donde se pueden establecer las configuraciones:

- `/opt/rt4/etc/RT_Config.pm`: El fichero base de configuración de RT. Se desaconseja encarecidamente su edición, en favor de otras alternativas de configuración.
- `/opt/rt4/etc/RT_SiteConfig.pm`: El fichero base de configuración específica de un sitio de RT.
- `/opt/rt4/etc/RT_SiteConfig.d/*.pm`: Ficheros auxiliares de configuración específica de un sitio de RT. Es una forma complementaria a `/opt/rt4/etc/RT_SiteConfig.pm` de establecer la configuración.
- `/opt/rt4/local/plugins/**/etc/*_Config.pm`: Ficheros de configuración específicos de las diferentes extensiones de RT. No se recomienda su modificación ya que muchos de ellos pueden ser sobrescritos en posteriores actualizaciones de las extensiones.
- `/opt/rt4/local/etc/*_Config.pm`: Ficheros de configuración específicos de la instalación local individual. Esta es la forma recomendada de configuración de las instancias.

139. NOTA IMPORTANTE: Para que RT detecte los cambios en cualquier fichero de configuración, se deben ejecutar los siguientes comandos:

```
bash
rm -rf /opt/rt4/var/mason_data/obj
service httpd restart
```

14. INSTANCIAS VSOC

141. Se trata de instancias propias especiales donde varios organismos comparten una única instancia. Conceptualmente es similar al concepto de *tenencia múltiple* (*multitenancy*).
142. A partir de LUCIA REV4.0 es posible gestionar este tipo de instancias a través de un control de acceso a las colas bien estructurado mediante *grupos organizativos* (ver apartado 1, especialmente el sub-apartado 1.6). Cada organismo tendrá el número de *grupos organizativos* que necesite. Mientras estos no tengan acceso (siendo miembros de *grupos de taxonomía* y/u *organizativos* de otro organismo), existirá compartimentación y por tanto podrán convivir en una única instancia.
143. Para poder segmentar posteriormente los tickets en su gestión global, es importante que las colas tengan asociado el valor correcto con el nombre/identificador del organismo **organization_id** (ver apartado 3.1, “Creación de colas de LUCIA”). Se trata de una clasificación intermedia, más fina que segmentar por instancia (las instancias VSOC están compartidas por varios organismos), pero no tanto como segmentar por cola (un organismo tiene o puede tener varias colas).

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

¿Cuáles son los campos del ticket que se sincronizan desde la instancia local del organismo al nodo central de LUCIA del CCN-CERT?

La lista de campos sincronizados, tanto para la sincronización unidireccional como bidireccional, viene detallada en el punto 6, “Gestión de la sincronización”.

¿Está permitido añadir campos personalizados nuevos?

Sí, aunque el poder añadir nuevos campos personalizados requiere la modificación de todos los *grupos de rol* relevantes (existentes y futuros) para que tengan permiso de lectura y/o edición sobre esos campos.

¿Está permitido modificar campos personalizados existentes?

No. Los campos personalizados predefinidos (excepto *Campaña* y *Origen de la Amenaza*) no se deben modificar en ninguna circunstancia, pues han de tener coherencia y homogeneidad con la instancia LUCIA Central. Actualmente se encuentran debidamente alineados con la CCN-STIC 817 por lo que no es necesaria su modificación.

¿Qué es el campo *Origen de la Amenaza*?

Este campo no sincronizado es para uso del propio organismo puesto que su punto de vista de la amenaza no tiene por qué ser el mismo en todas las instancias. Por ejemplo, en LUCIA Central puede ser *China* o *Rusia* y para el organismo un sistema específico, grupo de usuarios, etc.

¿Qué es el campo *Campaña*?

Este campo no sincronizado es para uso del propio organismo puesto que su punto de vista de la amenaza no tiene por qué ser el mismo en todas las instancias. Por ejemplo, en LUCIA Central puede almacenar información de uso exclusivo del CCN como, por ejemplo, una campaña de ransomware específica.

ANEXO A. PERMISOS EN RT

144. RT consta de diferentes objetos: Tickets, Colas, Grupos, Acciones (Scripts), Plantillas, Campos personalizados, Usuarios, Grupos... Cada objeto tiene unos permisos asociados. Para poder realizar una acción en concreto sobre un objeto, un usuario debe tener los permisos adecuados. Por ejemplo, si se desea crear un ticket en la cola A, el usuario deberá tener el permiso *CreateTicket* sobre la cola A (o sobre todas las colas). Otros permisos, como por ejemplo *AdminGroup*, no están ligados a una cola.
145. En RT los permisos pueden tener un contexto global (aplican a todo el sistema), un contexto de grupo (aplican sólo a ese grupo) o un contexto de cola (aplican sólo a esa cola). Todos los objetos tienen un contexto. Por ejemplo, si la Acción A es una acción global, se pueden conceder permisos a los usuarios en un contexto global.
146. Cada permiso puede estar ligado a un contexto y la interpretación de ese permiso puede ser diferente en cada contexto. Por ejemplo, el permiso *AdminQueue* en dos colas diferentes puede ser dado a diferentes grupos de usuarios, mientras que en un contexto global da privilegios sobre todas las colas.
147. A continuación se detallan los permisos más relevantes de RT.

ANEXO A.1. PERMISOS DE COLAS

148. Los siguientes permisos pueden ser concedidos a usuarios de RT en el contexto de una cola:
- ***AdminQueue***
Un usuario con este permiso puede administrar colas en RT.
Si un usuario posee este permiso en el contexto global, podrá crear y deshabilitar cualquier cola y cambiar todas las propiedades de las colas. Si lo posee en un contexto de cola, el usuario podrá cambiar las propiedades de esa cola (esto incluye deshabilitarla).
 - ***CommentOnTicket***
Un usuario con este permiso puede añadir comentarios a un ticket.
Este permiso puede ser concedido en el contexto global o en un contexto de cola. Por defecto, este permiso es concedido al grupo *Todos (Everyone)*.
Un usuario puede también comentar en un ticket si tiene el permiso *ModifyTicket*.
 - ***CreateTicket***
Un usuario con este permiso puede crear un ticket en una cola. También es necesario para mover un ticket de una cola a otra.
Este permiso puede ser concedido a usuarios y grupos en el contexto global o de cola.

Por norma general, debería ser concedido al grupo *Todos*, para que incluso un usuario desconocido pueda crear un *Reporte de Incidente* enviando un correo electrónico.

- ***ModifyCustomField***

Este permiso es necesario para establecer valores en los campos personalizados en cualquier momento, incluso en la creación de un ticket. Permite al usuario asociar un valor existente de un campo personalizado a un objeto (ticket, usuario, etc.)

- ***ModifyQueueWatchers***

Un usuario con este permiso puede modificar (añadir o quitar) observadores de cola pero no permite al usuario modificar los observadores de tickets individualmente.

Este permiso puede ser concedido a usuarios en el contexto global o de cola.

Si se quiere que los usuarios puedan añadirse o quitarse ellos mismos como observadores, se deben usar los permisos *Watch* y *WatchAsAdminCC*.

- ***ModifyTemplate***

Un usuario con este permiso puede crear, borrar y modificar plantillas.

Para tener disponible el acceso a través de *Administración* → *Global* → *Plantillas* es necesario el permiso *ShowConfigTab*.

Para modificar una plantilla existente es necesario el permiso *ShowConfig*.

- ***ModifyTicket***

Un usuario con este permiso puede hacer cambios genéricos en un ticket: modificar cualquier valor de un campo –personalizado o no– del ticket, enlazar o desenlazar tickets (el usuario necesita este permiso en ambos tickets).

Este permiso puede ser concedido en el contexto global o de cola.

Este permiso permite ejecutar un gran número de acciones, pero existen otros permisos para ciertas de estas acciones:

- *CommentOnTicket* para comentar en un ticket.
- *ReplyToTicket* para responder a un ticket.
- *Watch* y *WatchAsAdminCc* para que un usuario se añada o quite como observador del ticket.

Existen también algunas restricciones:

- Para mover un ticket a otra cola, es necesario que el usuario tenga los permisos *SeeQueue* y *CreateTicket* en la cola destino. El propietario actual perderá la propiedad del ticket si no tiene el permiso *OwnTicket* en la cola destino.

- ***OwnTicket***

Un usuario con este permiso puede ser el propietario un ticket. Esto significa que se le permite ser el responsable del asunto descrito en el ticket. Es un permiso que se concederá a las personas encargadas de la gestión y resolución de tickets.

Este permiso puede concederse a un usuario o grupo en el contexto global o de cola.

Normalmente, a quienes se les conceda este permiso se les concederá también *SeeQueue* en las mismas colas, aunque no es estrictamente necesario.

- ***ReplyToTicket***

Un usuario con este permiso puede responder a un ticket.

Por defecto, este permiso se le concede al grupo *Todos*. Esto se explica con el ejemplo de que un usuario externo (no privilegiado) accidentalmente cambie de dirección de correo, no podría responder a preguntas en el ticket nunca más. Aunque esto puede conllevar otros riesgos. Hay quien opta por conceder este permiso al grupo *Solicitante* en vez de *Todos*.

- ***SeeCustomField***

Este permiso permite ver el valor de campos personalizados en el ticket.

- ***SeeQueue***

Un usuario con este permiso puede ver una cola en concreto.

Este permiso puede ser concedido en el contexto global o el de cola. No es un permiso peligroso, ya que sólo permite ver, pero, además de mantener la vista inicial de usuario más limpia (con menos objetos), pueden existir razones para limitar su uso.

Este permiso no tiene nada que ver con tickets, para lo que es necesario el permiso específico *ShowTicket*.

En el caso de ser concedido estando el usuario autenticado, será necesario que inicie sesión de nuevo.

El principal efecto de este permiso es que todas las listas de colas que aparecen en la interfaz de usuario de RT contienen sólo las colas en las que el usuario tiene este permiso. Por ejemplo, la lista de estadísticas.

Dada la ubicuidad del uso de las listas de colas en RT, este permiso es necesario para realizar bastantes operaciones básicas, por ejemplo: será necesario para los operarios de una cola (quienes posean el permiso *OwnTicket*) para poder ver la cola en la que están trabajando.

- ***ShowTemplate***

Un usuario con este permiso puede ver las Plantillas y sus propiedades.

Este permiso puede ser concedido a usuarios y grupos en el contexto global o de cola.

- **ShowTicket**

Un usuario con este permiso puede ver un ticket, sus propiedades, transacciones y adjuntos.

Sólo las colas en las que el usuario tenga este permiso serán listadas en la página de búsqueda.

Este permiso puede ser concedido a usuarios y grupos en el contexto global o de cola.

- **ShowTicketComments**

Un usuario con este permiso puede ver los comentarios y sus adjuntos de un ticket.

Este permiso puede ser concedido a usuarios y grupos en el contexto global o de cola.

- **StealTicket**

Un usuario con este permiso puede pasar a ser el propietario de un ticket incluso si ya lo es otro usuario, quitándole la propiedad a éste.

Este permiso sólo puede ser utilizado por un usuario que tenga habilitado el permiso *OwnTicket*.

Este permiso puede ser concedido a usuarios y grupos en el contexto global o de cola.

- **TakeTicket**

Un usuario con este permiso puede cambiar el propietario de un ticket que no esté asignado a nadie (propietario *Nobody*).

Este permiso sólo puede ser utilizado por un usuario que tenga habilitado el permiso *OwnTicket*.

- **Watch**

Un usuario con este permiso puede añadirse o quitarse como *Solicitante* u *Observador Cc* en tickets.

Este permiso puede ser concedido a usuarios en el contexto global o de cola. En el contexto global, este permiso también permite modificar los observadores de la cola.

Los permisos *ModifyTicket* o *ModifyQueueWatchers* permiten a un usuario añadirse o quitarse igualmente, además del resto de posibilidades que ofrecen.

- **WatchAsAdminCc**

Un usuario con este permiso puede añadirse o quitarse como *AdminCC* de un ticket.

Los permisos *ModifyTicket* o *ModifyQueueWatchers* permiten a un usuario añadirse o quitarse igualmente.

ANEXO A.2. PERMISOS DE GRUPOS

149. Los siguientes permisos pueden ser concedidos a usuarios de RT en el contexto de un grupo:

- ***AdminGroup***

Un usuario con este permiso puede crear y deshabilitar grupos.

- ***AdminGroupMembership***

Un usuario con este permiso puede añadir o eliminar miembros de cualquier grupo público de RT.

- ***EditSavedSearches***

Un usuario con este permiso sobre un grupo puede editar las búsquedas guardadas de ese grupo.

El usuario debe tener también el permiso global *LoadSavedSearch* para tener acceso al sistema de guardado de búsquedas.

- ***ModifyOwnMembership***

Un usuario con este permiso puede añadirse o eliminarse a/de cualquier grupo público de RT.

- ***SeeGroup***

Un usuario con este permiso puede ver un grupo determinado.

- ***ShowSavedSearches***

Un usuario con este permiso puede ver y cargar las búsquedas guardadas de ese grupo. El usuario debe tener también el permiso *LoadSavedSearch*.

ANEXO A.3. PERMISOS GLOBALES

150. A continuación se muestran los permisos que pueden ser concedidos a usuarios de RT en el contexto global y que no han sido listados en las dos secciones anteriores.

- ***AdminAllPersonalGroups***

Un usuario con este permiso puede crear y borrar cualquier grupo de personas, modificar sus propiedades y añadir o quitar miembros de los mismos.

- ***AdminCustomField***

Un usuario con este permiso puede crear campos personalizados para una cola, añadir o eliminar valores para un campo personalizado y cambiar las propiedades de un campo personalizado.

Este permiso puede concederse a un usuario en el contexto global o de cola.

- ***AdminOwnPersonalGroups***

Un usuario con este permiso puede crear y borrar sus propios grupos de personas, modificar sus propiedades y añadir o quitar miembros de los mismos.

- ***AdminUsers***

Un usuario con este permiso puede crear, borrar, habilitar, deshabilitar y cambiar las propiedades de las cuentas de usuario. Es necesario tener también el permiso *ShowConfigTab*.

- ***CreateSavedSearch***

Un usuario con este permiso tiene acceso al sistema de guardado de búsquedas de RT. Sin este permiso, la opción *Crear una búsqueda guardada* permanecerá oculta.

Es necesario que el usuario tenga el permiso *ModifySelf* para acceder a *Mis búsquedas guardadas*.

- ***LoadSavedSearch***

Un usuario con este permiso tiene acceso al sistema de guardado de búsquedas de RT. Sin este permiso, la opción *Cargar una búsqueda guardada* aparecerá oculta.

- ***ModifySelf***

Un usuario con este permiso puede modificar varios de los valores de su perfil, incluyendo su contraseña de acceso.

- ***ShowConfigTab***

Un usuario con este permiso puede acceder a la pestaña de *Administrador*. Sin él no podrá ejercer sus permisos para modificar usuarios, grupos, colas, campos personalizados y otros objetos modificables a través de esta sección.

No obstante, no se debe confiar en este permiso para impedir el acceso a esas secciones. El usuario puede ser capaz de acceder a ellas introduciendo la url manualmente.

- ***SuperUser***

Un usuario con este permiso puede hacer cualquier cosa en RT.

ANEXO B. EXPORTACIÓN DE TICKETS EN FORMATO XML

151. LUCIA dispone de una herramienta para la extracción completa en formato XML de la información de los tickets *Incidentes* de las colas de Incidentes propios y del SAT (si se dispone de ellas). Esta extracción no aplica sobre *Reportes de Incidentes* ni *Investigaciones*.

152. El script debe ser lanzado desde línea de comandos con el usuario `root` de la instancia de LUCIA de la que se quieren obtener los tickets de la siguiente forma:

```
bash

perl -I/opt/rt4/lib \
/opt/rt4/local/plugins/RT-Extension-Lucia-Core/sbin/lucia-extraction \
--organization ORGANISMOS [--organization ORGANISMOS]... \
--status {created | resolved | created+resolved} \
{--start FECHA_INICIO --end FECHA_FIN | --year AÑO} \
[--queue-filter FILTRO [--queue-filter FILTRO]...] \
[--language {es | en}] \
[--writer {datadumper | xml} [--writer-option OPCIÓN [--writer-option OPCIÓN]...]]
```

153. Es necesario indicar que cualquier parámetro que contenga espacios, será necesario entrecomillarlo con comillas simples (') o dobles ("), como por ejemplo, en la siguiente llamada:

```
bash

perl -I/opt/rt4/lib \
/opt/rt4/local/plugins/RT-Extension-Lucia-Core/sbin/lucia-extraction \
--organization "ORG 1,ORG 2" \
--status created+resolved \
--start '2019-01-01 12:30:00' --end '2019-01-05 12:30:00' \
--writer xml
```

ANEXO B.1. PARÁMETROS DEL SCRIPT DE EXTRACCIÓN

154. **--organization ORGANISMOS:** Lo(s) organismo(s) a usar para segmentar los resultados. Solo los tickets pertenecientes a dicho(s) organismo(s) serán extraídos. *ORGANISMOS* es una lista de nombres de organismos separados por comas. Si se utiliza varias veces este parámetro, se concatenarán con comas como si fuera una única lista. Si solo se especifica un organismo, se pueden usar los comodines SQL % y ? para abarcar varios organismos (e.g., %CYL para JCYL y SACYL).

155. **--queue-filter FILTRO:** Establece filtros para las colas (se puede usar varias veces, limitando acumulativamente; si se usan dos filtros mutuamente excluyentes, no se generarán resultados). Los posibles valores de *FILTRO* son:

- **sat_class=CLASES_SAT:** Limita los resultados a colas de unas clases SAT dadas. *CLASES_SAT* es una lista de clases SAT separadas por coma. Si no se especifica ninguna, se seleccionarán las colas de incidentes propios (i.e., no-SAT) en su lugar.

- **include_multilevel**: Por defecto las colas intermedias de una jerarquía multinivel se excluyen de los resultados. Usar este filtro incluirá los tickets de colas multinivel.
 - **multilevel_only**: Establecer este filtro limitará los resultados estrictamente a las colas multinivel intermedias. Implica **include_multilevel**.
 - **include_spoc**: Por defecto las colas de notificación a terceros se excluyen de los resultados. Usar este filtro incluirá los tickets de colas de ventanilla única (i.e., notificación a terceros).
 - **spoc_only**: Establecer este filtro limitará los resultados estrictamente a las colas de ventanilla única. Implica **include_spoc**.
 - **name_like=NOMBRE**: Limita las colas explícitamente a aquellas cuyo nombre concuerde con *NOMBRE*. El formato de *NOMBRE* es el mismo usado en bases de datos SQL (% y ? son comodines). Cuando la base de datos lo soporte, *NOMBRE* no será sensible a mayúsculas y minúsculas.
 - **name_not_like=NOMBRE**: Limita las colas explícitamente a aquellas cuyo nombre **no** concuerde con *NOMBRE*. El formato de *NOMBRE* es el mismo usado en bases de datos SQL (% y ? son comodines). Cuando la base de datos lo soporte, *NOMBRE* no será sensible a mayúsculas y minúsculas.
156. **--status ESTADO**: Establece el/los estado/s usados para contrastar la ventana de tiempo. *ESTADO* es un valor entre *created*, *resolved*, o *created+resolved*.
157. **--start FECHA_INICIO**: Establece el límite inferior de la ventana de tiempo (solo se considerarán las fechas posteriores a *FECHA_INICIO*). El formato esperado de *FECHA_INICIO* es *YYYY[-MM-DD[hh:mm[:ss]]]*. Si se omiten partes, se redondeará a *YYYY-01-01 00:00:00*.
158. **--end FECHA_FIN**: Establece el límite superior de la ventana de tiempo (solo se considerarán las fechas anteriores a *FECHA_FIN*). El formato esperado de *FECHA_FIN* es *YYYY[-MM-DD[hh:mm[:ss]]]*. Si se omiten partes, se redondeará a *YYYY-12-31 23:59:59*.
159. **--year AÑO**: Si se utiliza, los argumentos **--start** y **--end** se ignorarán. El formato esperado de *AÑO* es *YYYY*. Es equivalente a usar **--start AÑO --end AÑO**.
160. **--writer FORMATO_SALIDA**: Especifica el formato para mostrar el resultado. Los valores soportados actualmente son:
- **datadumper**: Muestra la salida como una estructura de datos en formato Perl usando *Data::Dumper*. Éste será el formato usado por defecto si no se especifica este argumento.
 - **xml**: Genera la salida en formato XML (ver la especificación en Anexo B.2).
161. **--writer-option OPCIÓN**: Establece una de las opciones del formateador de salida. Las posibles opciones, así como si éstas requieren un valor o no, dependen del formateador y se especifican más abajo. Se puede usar este argumento varias veces para establecer varias opciones.

- Opciones para el formateador **xml**:
 - **dtd**: Si se establece esta opción, el DTD (descriptor de la estructura del XML generado) se incluirá en el propio documento generado para su propia validación.

162. **--language** *IDIOMA*: Intentará traducir la salida al idioma indicado. *IDIOMA* es el código internacional para el idioma deseado (e.g., es, en, etc.)

ANEXO B.2. EJEMPLOS DE USO

163. Extraer *cada ticket* de *ORG 1* y *ORG 2*, *creado o resuelto* durante 2019, en formato *XML*:

```
bash

perl -I/opt/rt4/lib \
/opt/rt4/local/plugins/RT-Extension-Lucia-Core/sbin/lucia-extraction \
--organization "ORG 1,ORG 2" \
--status created+resolved \
--year 2019 \
--writer xml
```

164. Extraer *cada ticket propio* (i.e., no-SAT) de *ORG 1* *creado o resuelto* durante 2019 en *colas con nombres* *"* - Lucia_ *"*, en formato *XML*, *incluyendo el DTD*:

```
bash

perl -I/opt/rt4/lib \
/opt/rt4/local/plugins/RT-Extension-Lucia-Core/sbin/lucia-extraction \
--organization "ORG 1" \
--queue-filter sat_class= \
--queue-filter "name_like=% - Lucia_%" \
--status created+resolved \
--year 2019 \
--writer xml \
--writer-option dtd
```

165. Extraer *cada ticket SAT-INET* de *ORG 2* *creado* durante *enero de 2019*, *notificado a través de ventanilla única* a esta instancia, en formato *XML*:

```
bash

perl -I/opt/rt4/lib \
/opt/rt4/local/plugins/RT-Extension-Lucia-Core/sbin/lucia-extraction \
--organization "ORG 2" \
--queue-filter sat_class=INET \
--queue-filter spoc_only \
--status created \
--start 2019-01-01 \
--end 2019-01-31 \
--writer xml
```

166. Extraer *cada ticket SAT-SARA* de *cualquier organismo*, *resuelto* durante *enero de 2019* en esta instancia (excluyendo colas multinivel y de ventanilla única), en formato *XML* y *traducido al español*.

bash

```
perl -I/opt/rt4/lib \  
/opt/rt4/local/plugins/RT-Extension-Lucia-Core/sbin/lucia-extraction \  
--organization "%" \  
--queue-filter sat_class=SARA \  
--status resolved \  
--start 2019-01-01 \  
--end 2019-01-31 \  
--language es \  
--writer xml
```

ANEXO B.3. ESPECIFICACIÓN DEL FORMATO XML

167.El formato del documento XML se compone de una cabecera opcional **!DOCTYPE** con un DTD, y un nodo raíz **LUCIA**.

168.Este nodo **LUCIA** contendrá cero o más nodos **TICKET**.

ANEXO B.3.1. EL NODO LUCIA

169.Es el nodo raíz del documento. Contiene un número arbitrario de nodos **TICKET**, además de los siguientes atributos:

- **instance**: nombre de la instancia sobre la que se ha ejecutado el script.
- **constituency**: organismos usados para filtrar la extracción.
- **queue_filters**: filtros sobre las colas usados para limitar los resultados.
- **status**: tipo de exportación: tickets creados o resueltos.
- **date_start**: fecha completa de inicio del intervalo de extracción.
- **date_end**: fecha completa de fin del intervalo de extracción.
- **date_extraction**: fecha de ejecución de la extracción

ANEXO B.3.2. LOS NODOS TICKET

170.Es la estructura que almacena la información de un ticket. Contiene varios nodos hijo con los datos del ticket, según se indica debajo.

NOTA: Los campos de la extracción indicados a continuación no aparecen ordenados en el fichero XML sino que depende de la ejecución interna de RT. Para mayor claridad, se han agrupado por categorías relacionadas.

- Relativos al incidente:
 - **id**: Identificador del ticket.
 - **subject**: El asunto del ticket.
 - **owner**: Usuario propietario.
 - **initial_priority**: Peligrosidad inicial (valor numérico)
 - **initial_priority_text**: Peligrosidad inicial (valor textual)

- **priority**: Peligrosidad (valor numérico)
- **priority_text**: Peligrosidad (valor textual)
- **status**: Estado del ticket.
- **description**: La descripción.
- **ip**: Direcciones IP relacionadas con el incidente.
- **situation**: La situación.
- **notification_type**: Tipo de notificación.
- **organization_type**: Tipo de organismo.
- **cyber_incident_classification**: Clasificación del ciberincidente.
- **type_of_cyber_incident**: Tipo de ciberincidente.
- **classification_level**: Nivel de clasificación.
- **reliability**: Fiabilidad.
- **threat_source**: Origen de la amenaza.
- **campaign**: Campaña.
- Relativos a las fechas:
 - **date_created**: Fecha de creación del ticket.
 - **date_starts**: Fecha en la que se detectó la incidencia por primera vez.
 - **date_started**: Fecha en la que el responsable ha empezado a trabajar con el ticket.
 - **date_told**: Fecha de último contacto con un agente externo.
 - **date_due**: Fecha límite de resolución.
 - **date_resolved**: Fecha de resolución o abandono¹¹.
 - **date_last_updated**: Fecha de última actualización.
- Relativos a la resolución:
 - **resolution**: Resolución.
 - **invested_resources**: Recursos invertidos en el incidente.
 - **system_category_according_to_ens**: Categoría del sistema según ENS.
 - **impact**: Impacto.
 - **incident_cause**: Causa del incidente.
 - **incidences_during_resolution**: Incidencias durante la resolución.
 - **number_of_affected_systems**: Número de sistemas afectados.
 - **affects_gdpr**: Afecta a la RGPD.

¹¹ Por defecto aparecerá 1970-01-01 01:00:00 en el valor de la etiqueta si el ticket no se ha cerrado nunca.

- **notify_agpd**: Se solicita o no notificar a la AGPD.
 - **notify_ccn_cert**: Se solicita o no notificar al CCN-CERT.
 - **notify_cnpic**: Se solicita o no notificar al CNPIC.
 - **worked_time**: Tiempo trabajado.
- Relativos a la sincronización con LUCIA Central:
- **ticket_guid**: El GUID de sincronización del ticket.

ANEXO C. COPIAS DE SEGURIDAD

171. Se recomienda usar *snapshots* para la realización de copias de seguridad debido a su sencillez y a la rapidez con la que se puede volver a un punto previo. Es especialmente crítica la creación de *snapshots* en el caso de actualizaciones de LUCIA pues se actualizan los paquetes del sistema operativo y por ello para volver a un estado previo no valdría únicamente con restaurar datos y configuración. Si no es posible la realización de *snapshots*, o bien se desea aumentar la seguridad se puede realizar adicionalmente copia de los ficheros y base de datos que componen LUCIA.

172. Antes de realizar la copia de ficheros o base de datos se recomienda parar los servicios de LUCIA para evitar incoherencias:

```
bash

systemctl disable crond
systemctl stop crond
systemctl disable httpd
systemctl stop httpd
systemctl disable postfix
systemctl stop postfix"
```

173. La realización de copia de seguridad de los ficheros debe incluir los siguientes directorios:

- `/media/lucia-data`: Contiene la instalación completa de LUCIA
- `/etc`: Configuración del sistema operativo.
- `/home`: *Home* de usuarios utilizados por LUCIA.
- `/root`: *Home* del usuario root.

174. LUCIA dispone de la herramienta `mysqldump` para la realización de volcados de la base de datos. El tamaño de la copia de seguridad depende en gran medida de la cantidad de adjuntos que tengan los tickets almacenados. Para evitar problemas en la restauración de las copias se recomienda usar el parámetro `extended-insert=false` que evita la unión de las sentencias de inserción y permite un ajuste correcto del parámetro `max_allowed_packet`. Un ejemplo de sentencia para generar el volcado correcto de la base de datos sería el siguiente:

```
bash

mysqldump -u root -p \
--extended-insert=false --single-transaction --all-databases | \
gzip -c > backup-lucia.sql.gz
```

175. La restauración de una copia de seguridad de la base de datos es un proceso que puede llevar un tiempo considerable en instancias con un número de tickets muy alto. Este tiempo se puede reducir estableciendo variando la política de sincronización a disco de mariadb. Para ello podemos modificar temporalmente los siguientes parámetros en `/etc/my.cnf` y reiniciar el servicio mysql:

```
INI: /etc/my.cnf
```

```
max_allowed_packet=100M
innodb_flush_log_at_trx_commit = 2
innodb_log_file_size = 256M
innodb_flush_method = O_DIRECT
```

Un ejemplo de sentencia de restauración de la base de datos sería el siguiente:

```
bash
```

```
gunzip < backup-lucia.sql.gz | mysql -u root -p
```

176. Una vez realizada la copia de seguridad se deben restaurar los servicios de LUCIA:

```
bash
```

```
systemctl enable httpd
systemctl start httpd
systemctl enable postfix
systemctl start postfix
systemctl enable crond
systemctl start crond
```

ANEXO D. ACTUALIZACIÓN DEL CERTIFICADO DE SERVIDOR

177.El anexo expone las instrucciones a seguir para actualizar el certificado de servidor de LUCIA, tanto para instancias que usen certificados propios autofirmados, como aquellas que utilizan certificados externos.

ANEXO D.1. CERTIFICADOS PROPIOS AUTOFIRMADOS

178.Este apartado explica cómo se debe actualizar el certificado de servidor, cuando se estén utilizando certificados propios firmados por una CA (autoridad certificadora) propia.

179.Lo primero que se debe hacer es generar una clave de servidor.

```
bash
openssl genrsa -out server.key 4096
```

180.A continuación, crear la solicitud de firma del certificado, la cual pedirá una serie de datos. Se debe poner especial atención cuando se solicite el valor del campo *Common Name*, este debe coincidir con el FQDN (p.ej. lucia.organismo.es) utilizado en la URL de servicio de LUCIA (p.ej. https://lucia.organismo.es).

```
bash
openssl req -new -key server.key -out server.csr
```

181.En este punto llega el momento de generar un certificado de servidor firmado con la CA. Se debe indicar la validez en días, así como el número de serie de certificado. Como se está actualizando el certificado, se entiende que el número de serie en este caso es '02'. Pero se debe elegir en función del número de certificados emitidos.

-days: días de validez del certificado.

-in: solicitud de firma del certificado.

-CA: parte pública del certificado de la autoridad certificadora. Puede ser encontrado en la ruta `/var/local/ca/certs/ca.crt`, aunque dependiendo de cómo se haya generado el certificado, podría encontrarse en otra ruta.

-CAkey: parte privada del certificado de la autoridad certificadora. Puede ser encontrado en `/var/local/ca/private/ca.key`, aunque dependiendo de cómo se encuentre configurada la instancia podría haber sido almacenado fuera de la propia máquina de LUCIA.

-set_serial: número de serie del certificado de servidor.

-out: nombre del certificado de servidor firmado que se quiere generar.

```
bash
openssl x509 -req -days 730 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 02 -out server.crt
```

182. Con el certificado generado y en formato crt y key, se puede proceder a la instalación.

ANEXO D.2. CERTIFICADOS EXTERNOS

183. En este apartado se explica cómo se debe actualizar el certificado de servidor en LUCIA, en el supuesto de que se dispongan de certificados externos. Es decir, certificados que se han creado y firmado fuera de la propia máquina de LUCIA.

184. Si se recibe el certificado de servidor en un único fichero pem, en el que se incluye tanto la clave privada, como el certificado, puede transformarse a formato key y crt de la siguiente manera.

185. Key:

```
bash
openssl pkey -in server.pem -out server.key
```

186. Crt:

```
bash
openssl x509 -in server.pem -outform PEM -out server.crt
```

187. Una vez se dispone del certificado de servidor en formato crt y key, se puede proceder con la instalación.

ANEXO D.3. INSTALACIÓN DE CERTIFICADOS

188. Antes de instalar los nuevos certificados es recomendable hacer una copia de los viejos. Para ello en el fichero de configuración de apache (*/media/lucia-data/etc/httpd/conf.d/rt.conf*), se encuentran dos directivas que referencian al certificado de servidor SSLCertificateFile y SSLCertificateKeyFile

```
/media/lucia-data/etc/httpd/conf.d/rt.conf
SSLCertificateFile    /media/lucia-data/etc/pki/tls/certs/server_lucia.crt
SSLCertificateKeyFile /media/lucia-data/etc/pki/tls/private/server_lucia.key
```

189. Para resguardar el certificado viejo se pueden utilizar los siguientes comandos, que harán una copia de los ficheros con extensión *'old'*

```
bash
cp /media/lucia-data/etc/pki/tls/certs/server_lucia.crt{,.old}
cp /media/lucia-data/etc/pki/tls/private/server_lucia.key{,.old}
```

190. Una vez realizadas las copias se puede proceder con la instalación del certificado de servidor.

191. Localizados los nuevos certificados de servidor en formato crt y key (*server.crt* y *server.key*), se debe establecer *server.crt* en *SSLCertificateFile* y *server.key* en *SSLCertificateKeyFile*. Al haber realizado una copia de los ficheros antiguos del certificado de servidor, se puede sobrescribir los ficheros establecidos en ambas directivas de configuración a través de estos comandos.

```
bash
```

```
cat server.crt > /media/lucia-data/etc/pki/tls/certs/server_lucia.crt  
cat server.key > /media/lucia-data/etc/pki/tls/private/server_lucia.key
```

192. Se debe asegurar que tienen los permisos necesarios

```
bash
```

```
chmod 644 /media/lucia-data/etc/pki/tls/certs/server_lucia.crt  
chmod 600 /media/lucia-data/etc/pki/tls/private/server_lucia.key
```

193. Si se dispusiera de una cadena de certificados para el certificado de servidor, esta debe especificarse en la directiva *SSLCertificateChainFile*, procurando que tenga los permisos correspondientes.

```
/media/lucia-data/etc/httpd/conf.d/rt.conf
```

```
SSLCertificateChainFile /media/lucia-data/etc/pki/tls/certs/certificate_chain.crt
```

```
bash
```

```
chmod 644 /media/lucia-data/etc/pki/tls/certs/certificate_chain.crt
```

194. A partir de la versión 2.4.8 de apache *SSLCertificateChainFile* queda obsoleto, y la cadena de certificados debe añadirse (**no** sobrescribir) en el propio crt del certificado de servidor (*server.crt*), ya que la directiva *SSLCertificateFile* será la encargada de detectar esta cadena de certificados intermedios.

195. Como apunte, en el caso de que no hubiera sido añadida anteriormente la parte pública de la CA que firma el certificado de servidor, al fichero indicado en la directiva *SSLCACertificateFile*. Esta debe ser añadida, (**no** sobrescribir) al fichero, procurando que dicho fichero tenga los permisos correspondientes.

```
/media/lucia-data/etc/httpd/conf.d/rt.conf
```

```
SSLCACertificateFile /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt
```

```
bash
```

```
chmod 644 /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt
```

196. Como último paso para la instalación de los certificados, se debe reiniciar el servicio de apache



```
bash
```

```
systemctl restart httpd
```