GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 844

# ANEXO III: CREACIÓN DE FICHERO DE INCIENTES PROPIOS EN CASO DE NO TENER INSTANCIA DE LUCIA


Octubre 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.10.15 11:14:13 +02'00'



NIPO: 083-19-023-3

Fecha de Edición: octubre 2018

# 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.

Octubre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

# 1. FORMATO PARA LA CREACIÓN DEL XML DE INCIDENTES PROPIOS EN CASO DE NO DISPONER DE INSTANCIA PROPIA DE LUCIA PARA SU IMPORTACIÓN EN INES

1. Uno de los beneficios de tener una instancia propia de LUCIA, es la facilidad para la carga de incidentes en INES (propios del organismo, SAT-INET y SAT-SARA) mediante la exportación de los mismos en formato XML.

Los incidentes procedentes del Sistema de Alerta Temprana (SAT) se remitirán desde el CCN-CERT a finales de cada año tras su extracción del sistema LUCIA Central, sin embargo, no se disponen de los datos de incidentes propios, por lo que el organismo deberá cargarlos manualmente en INES.

Para facilitar los cálculos, el organismo tiene la posibilidad de crear su propio fichero en formato XML de incidentes propios ya sea manualmente o por transformación de la salida de los datos exportados de su gestor de incidentes si se dispone de uno (*OTRS, REMEDY, ServiceDesk*,…).

El fichero de datos XML deberá contener texto plano sin formato, tener extensión .xml y que cumpla la siguiente estructura:

```
<LUCIA constituency="ORGANISMO" date_start="2016-01-01 01:00:00">
    <TICKET>
        <date_created>FECHA_DC</date_created>
        <date_starts>FECHA_DS</date_starts>
        <date_resolved>FECHA_DR</date_resolved>
        <status> VALOR_STA</status>
            <cyber_incident_classification>VALOR_CIC</cyber_incident_classific
        ation>
        <impact>VALOR_IMP</impact>
    </TICKET>
    ….La estructura <TICKET> se repetirá tantas veces como incidentes a cargar….
</LUCIA>
```

El significado y posibles valores de la estructura XML es la siguiente:

- Parámetros de la etiqueta *<LUCIA>*:
  - *ORGANISMO*: Nombre del organismo. Cualquier valor de texto es válido siempre que no contenga las cadenas *SATINET* o *SATSARA*.
  - *2016*: Año de los datos a cargar.

- Campos de la estructura *<TICKET>*:
  - *FECHA_DC*: Fecha de creación (o alta en el sistema) del incidente en formato *YYYY-MM-DD HH:MM:SS*
  - *FECHA_DS*: Fecha de detección del incidente por el organismo en formato *YYYY-MM-DD HH:MM:SS*. Si se desconoce este valor, debe inicializarse al valor por defecto *1970-01-01 01:00:00*

- *FECHA_DR*: Fecha de resolución del incidente en formato *YYYY-MM-DD HH:MM:SS*. Si el incidente se encuentra en estado *abierto*, debe inicializarse al valor por defecto *1970-01-01 01:00:00*

- *VALOR_STA*: Estado del incidente. Los posibles valores son:
  - abierto: La gestión de incidente continúa en proceso.
  - resuelto: La gestión de incidente se encuentra finalizada.

- *VALOR_CIC*: Clasificación del incidente. Los posibles valores (respetando mayúsculas, espacios y acentos) son:
  - Código dañino
  - Compromiso de información
  - Contenido abusivo
  - Disponibilidad
  - Fraude
  - Intrusiones
  - Política de seguridad
  - Obtención de información
  - Otros

- *VALOR_IMP*: Impacto del incidente. Los posibles valores (respetando mayúsculas, espacios y acentos) son:
  - I0 – Irrelevante
  - I1 – Bajo
  - I2 – Medio
  - I3 – Alto
  - I4 - Muy Alto
  - I5 - Crítico

Los criterios empleados en la clasificación del incidente (VALOR_CIC) e impacto (VALOR_IMP) se definen en la Tabla 1 (Clasificación de los ciberincidentes) y Tabla 4 (Criterios de determinación del nivel de impacto) de la guía CCN-STIC-817 respectivamente. El organismo debe mapear los valores que se encuentren definidos en su gestor de incidentes para calcular su equivalencia con los definidos en las mencionadas tablas