Sistema de Alerta Temprana

SAT-INET 2.0

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

ÍNDICE

1. INTRODUCCIÓN

Los incidentes de seguridad a los que están expuestos los sistemas de la Administración Pública española son cada día más numerosos y, a través de Internet, más fáciles de llevarse a cabo y de propagarse. Código dañino y/o espía instalado en los equipos de un Organismo, gusanos que intentan extenderse por la red y comunicarse con servidores externos para enviar información o para destruir, bloquear o modificar datos almacenados, ataques contra los servicios web de un ente público… En general, este tipo de ataques y especialmente los de código dañino han experimentado un crecimiento exponencial en los últimos años, superando muchas veces a las capacidades de detección tradicionales.

Disponer de una visión holística y distribuida de los riesgos y amenazas que se producen en los distintos organismos, frente a una visión centrada en el tráfico de una única organización, permite mejorar de una forma muy importante las capacidades de detección de tráficos "anómalos" que, de otro modo, podrían pasar desapercibidos.

Esta visión global permite, no sólo detectar incidentes de forma temprana generando las contramedidas más adecuadas para atajar su impacto de la forma más rápida posible, sino que además permite limitar la propagación del incidente a través de la red e identificar el impacto sobre otros organismos y/o dominios.

Por este motivo, desde el año 2008 la Capacidad de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) viene desarrollando un Sistema de Alerta Temprana (SAT) para la detección de incidentes y anomalías que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país que permite realizar acciones preventivas, correctivas y de contención. En un primer momento, este servicio comenzó su desarrollo con la monitorización de la Red de Intercomunicación de todos los organismos de la Administración Pública española, SARA (SAT-SARA). Posteriormente, ya en el año 2010, el servicio se extendió a los accesos de Internet de las distintas administraciones (SAT-INET) y durante 2016 comenzó el desarrollo del servicio de monitorización de los sistemas de control industrial que están en operación en infraestructuras del Sector Público (SAT-ICS).

A través de este servicio, el Centro Criptológico Nacional, en colaboración con el organismo adscrito, puede detectar multitud de tipos de ataque, evitando su expansión, respondiendo de forma rápida ante el incidente detectado y, de forma general, generar normas de actuación que eviten futuros incidentes. Al tiempo, y gracias al almacenamiento de un número progresivo de eventos, es posible contar con una panorámica completa y veraz de la situación de los sistemas de las administraciones públicas españolas que posibilite una acción preventiva frente a las amenazas que sobre ellas se ciernen.

2. ¿QUÉ ES EL SISTEMA DE ALERTA TEMPRANA SAT-INET?

El Sistema de Alerta Temprana (SAT) de Internet es un servicio desarrollado e implantado por la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico de Internet del Organismo adscrito. Su misión es detectar patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico, sin centrarse en el análisis del contenido del tráfico que no sea relevante en la detección de una amenaza.

Para su puesta en marcha es necesaria la implantación de una **sonda individual** en la red del Organismo, que se encarga de detectar y recolectar la información de seguridad más relevante y, después de un primer filtrado, enviar estos eventos de seguridad hacia el **sistema central** que realiza una correlación entre los distintos elementos y entre los distintos dominios (organismos). Inmediatamente después, el Organismo adscrito recibe los correspondientes avisos y alertas sobre los incidentes detectados.

La sonda es un servidor dedicado que funciona como un sistema de detección de intrusos (IDS – *Intrusion Detection System*) y que incorpora varias herramientas de detección y monitorización, tanto de código abierto como comerciales, y que cuenta con dos interfaces de red diferenciados:

- Interfaz de análisis: recibe una copia del tráfico del organismo para analizar. Este interfaz solo lee el tráfico fuera de línea, sin modificarlo en ningún momento, y sólo aquel que es necesario para desarrollar su función.
- Interfaz de gestión: conecta a través de Internet de forma segura con el sistema central de monitorización/correlación, haciendo uso de la infraestructura del Organismo o de una conexión independiente.

El despliegue de la sonda se realiza del siguiente modo:

- Instalación de la sonda en el Organismo y configuraciones necesarias en la **electrónica de red** para enviar hacia la sonda el tráfico a analizar.
- La **conexión entre la sonda y el sistema central** se realiza siempre de forma **segura**, a través del establecimiento de un túnel cifrado. Esta conexión puede realizarse a través de salida a Internet del Organismo adscrito o a través de una salida dedicada hacia Internet. El establecimiento de este túnel cifrado se inicia desde la sonda hacia el sistema central, no siendo necesaria ninguna infraestructura adicional por parte del organismo para el establecimiento de túneles cifrados.
- La sonda se **gestiona** completamente **desde el CCN-CERT**, no siendo necesaria la realización de tareas de administración por parte del personal del Organismo. Eventualmente se solicitaría apoyo al Organismo en el caso que fuera necesaria la realización de tareas puntuales que no pudieran realizarse de manera remota.
- De forma general, salvo que se pacte otra cosa, la sonda vigilará el **tráfico de Internet** de la red corporativa del Organismo y el de las DMZ's de servicios que el organismo ofrezca a Internet. Con los eventos recibidos se realiza una correlación avanzada de eventos en el sistema central, permitiendo la detección de ataques hacia los distintos organismos adscritos al sistema o la presencia de código dañino en estas redes.

- La **gestión**, **actualización y mantenimiento** del **sistema central** está a cargo del CCN-CERT, que lleva a cabo tareas de administración, maduración de las reglas de detección e inclusión de nuevas funcionalidades y herramientas. De hecho, periódicamente se realiza la integración de numerosas reglas de detección, propias y externas, completando y ampliando la inteligencia del servicio y su capacidad de detección. Las reglas propias son generadas a partir de la información obtenida durante la investigación de otros incidentes de seguridad y a partir de la información recibida de otros organismos con los que se mantiene un intercambio de información referente a incidentes de seguridad.
- Los usuarios pueden acceder en tiempo real a **información relevante** de los eventos generados por la sonda de su organismo y a informes periódicos a través de un portal accesible en Internet, y a la información de los incidentes de seguridad notificados a través de la herramienta LUCIA. Cada Organismo puede ver exclusivamente los eventos e informes relacionados con su red monitorizada.

2.1 SAT-INET 2.0

Durante el tiempo en el que se ha venido prestando el servicio del Sistema de Alerta Temprana SAT-INET, desde que iniciara su andadura en 2010, se ha identificado la necesidad de evolucionar el modelo centralizado inicial de recolección y correlación de eventos por sus limitaciones en las capacidades de escalado si se monitoriza un número elevado de fuentes, sobre todo por la necesidad de consumo de ancho de banda entre las sedes remotas y el sistema central al querer integrar fuentes de eventos en el sistema provenientes de otros sistemas de seguridad perimetral de los que dispusiera el organismo.

Estas necesidades han quedado cubiertas con la evolución del Sistema de Alerta Temprana **SAT-INET** a la **versión 2.0**, que permite desplegar de manera distribuida capacidades de recolección de eventos y de correlación avanzada en la red del organismo, de manera complementaria al despliegue de la sonda, de cara a poder integrar otras fuentes de eventos de otros dispositivos de seguridad perimetral del organismo.

De este modo, el SAT 2.0 tiene la capacidad de funcionar con un **modelo de correlación distribuida**, en el que los eventos de la sonda y de otros sistemas de seguridad se recolecten y correlen en origen, eliminando la necesidad de utilización de un gran ancho de banda entre la red del organismo y el sistema central del SAT-INET, que realizará una correlación de segundo nivel utilizando solamente alertas previamente correladas para identificar amenazas que afecten de forma coordinada a varias fuentes.

Para la puesta en marcha en un organismo del modelo de correlación distribuida es necesario el **despliegue** en la red del Organismo **de otros servicios de manera complementaria** al despliegue de la **sonda individual.** Estos servicios complementarios forman parte de la herramienta GLORIA del CCN-CERT y su implementación consistirá en el despliegue de los siguientes servicios:

- Servicio de recolección y almacenamiento, modelado y centralización de eventos de seguridad[1]. Este servicio recogerá los eventos provenientes de la sonda del SAT-INET y de los sistemas de seguridad perimetral que se integrasen en el sistema[2].
- Servicio de correlación compleja de eventos de seguridad. Este servicio desarrollará y parametrizará correladores de eventos especializados para aplicación en diferentes dominios de la detección y de la protección, adaptándose a las particularidades del entorno.

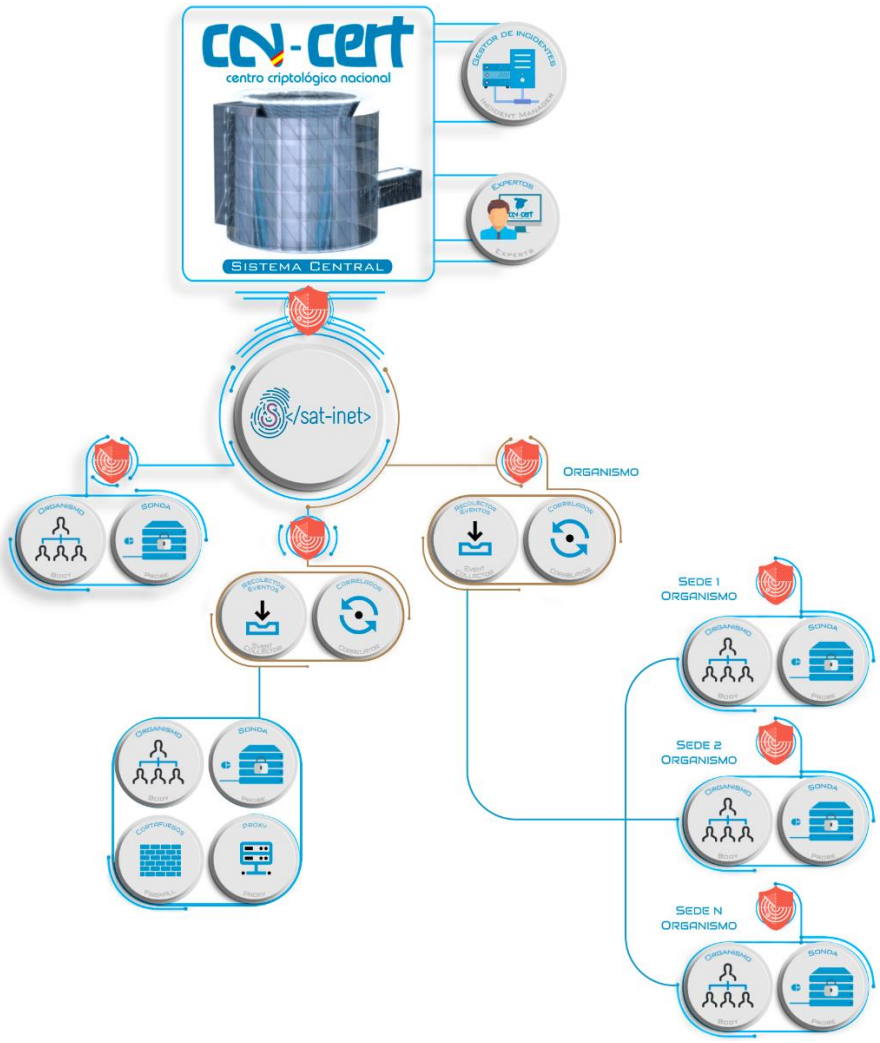

Figura 1. Arquitectura SAT-INET 2.0

[1] Dependiendo del número de eventos por segundo (EPS) a integrar en el sistema, podría variar el número de máquinas a desplegar dedicadas a la recolección y almacenamiento. Serán necesarios trabajos de análisis y definición de alcance con el organismo para definir la arquitectura a desplegar.

[2] Dentro del servicio del Sistema de Alerta Temprana SAT-INET se integrarán los eventos provenientes del cortafuegos perimetral y del servidor proxy. La integración de otros eventos de seguridad provenientes de otros dispositivos de seguridad perimetral o de otros sistemas de la organización podrían suponer un coste a asumir por el organismo para los trabajos de consultoría, integración y configuración.

3. BENEFICIOS APORTADOS A LOS ORGANISMOS ADSCRITOS

El Sistema de Alerta Temprana SAT-INET tiene como principal función la **detección temprana en el caso que se produzca un incidente de seguridad**, para que puedan aplicarse las medidas necesarias de contención y de eliminación de la amenaza y poder evitar que el intento de ataque sea fructífero o, en su caso, minimizar el posible impacto. Ofrece **ventajas significativas con independencia de que se tenga una solución de monitorización desplegada** (siendo compatible con ella) o no. En este último caso, permite desplegar una solución gestionada por un equipo de expertos y que incorpora las últimas tecnologías.

En general, las ventajas para cualquier organización podrían resumirse en las siguientes:

- Acceso al mayor conjunto de **reglas de detección**, tanto propias como externas, integradas por el equipo de expertos del CCN-CERT que permite la detección de un mayor número de amenazas.
- **Detección** de todo tipo de ataques e incidentes, incluyendo **detección avanzada interdominio** (detección temprana de un incidente que se haya replicado en otro de los dominios monitorizados).
- **Correlación**. El sistema central no solo detecta incidentes importantes de forma individual, sino que se pueden detectar eventos mucho más complejos que pueden involucrar a distintos dominios.
- **Información** de gran valor para los responsables TIC de las administraciones públicas, que pueden ver en tiempo real el estado de su red con respecto a la seguridad, así como acceder a informes estadísticos.
- **Soporte a la resolución de incidentes**. Como CERT Gubernamental/Nacional español, el CCN-CERT ofrece a todos los organismos su colaboración para una detección, contención y eliminación de cualquier ataque que pueda sufrir a sus sistemas.

4. PREGUNTAS MÁS FRECUENTES –FAQ-

4.1 ¿Qué es una sonda?

La sonda es un servidor de alto rendimiento que permite el análisis del tráfico de la red del Organismo adscrito, la generación de eventos específicos de seguridad y su envío de forma segura al sistema central. Consta de los siguientes elementos:

- La interfaz de gestión, que se conecta a la red del Organismo para enviar al sistema central del SAT los eventos generados por la sonda.
- Los interfaces de análisis, que reciben el tráfico a analizar y que no tienen dirección IP, siendo totalmente transparentes a la red.
- Un Sistema de Detección de Intrusiones de Red (IDS), con reglas de detección específicas de diferentes fuentes y de creación propia.
- Un recolector de los eventos detectados para su envío al Sistema Central. Este agente inicialmente estará configurado para el análisis de los eventos generados por las distintas herramientas de detección que se incorporen.

4.2 ¿Dónde se instala una sonda?

La sonda puede implantarse en distintos puntos de la red dentro de la infraestructura del Organismo, siendo siempre recomendable que el tráfico que reciba haya sido ya filtrado por los dispositivos de seguridad perimetral del Organismo.

Además, esta sonda puede estar conectada a distintas redes para realizar una monitorización diferenciada, siempre que existan diversas interfaces de red disponibles en el servidor para llevar a cabo esta tarea.

En cada caso se estudiará junto con el Organismo cual es la situación ideal donde realizar la instalación de la sonda.

4.3 ¿Qué características debe tener el servidor?

Los requerimientos hardware del servidor para el adecuado funcionamiento de la sonda son los siguientes:

	Mínimos	Recomendados
Procesador	Procesador multinúcleo de 8 cores	Procesador multinúcleo de 16 cores
Memoria	16 GB de memoria RAM	
Almacenamiento	2 Discos Duros 146GB SAS, en RAID 1 (Espejo)[3]	
Red	Interfaz/ces de análisis (tantas como redes a analizar): tarjeta/s de red	

[3] La capacidad de los discos duros es meramente orientativa. El servidor deberá disponer de una capacidad mínima que permita la instalación del sistema operativo, de las aplicaciones necesarias y que asegure el almacenamiento de eventos generados por la sonda durante un periodo de tiempo razonable para el correcto funcionamiento del sistema.

	Gigabit Ethernet de tecnología Intel (driver e1000e o igb)
	Interfaz de gestión: tarjeta de red Gigabit Ethernet con distinto driver que la/s interfaz/ces de análisis (p.e. Broadcom…)
Soporte Óptico	Lector DVD (requerido únicamente para la instalación)
Sistema Operativo	Hardware compatible con CentOS 7.3 (Instalado por el CCN-CERT)

Los **organismos interesados** en adscribirse a este SAT, **deberán disponer de un servidor** que cumpla al menos con los requerimientos mínimos. La **instalación** del sistema operativo, de todas las aplicaciones necesarias y de la securización de la plataforma **se realizará por personal técnico del CCN-CERT** en el momento de la instalación de la sonda en el Organismo.

De manera alternativa, la instalación podrá realizarse directamente por el Organismo con apoyo remoto del personal técnico del CCN-CERT. En estos casos se entregará al organismo una imagen de instalación y un manual para que éste pueda llevar a cabo la instalación de la sonda y, una vez llevadas a cabo estas tareas, el personal técnico del CCN-CERT realizará, mediante acceso remoto a la misma, las tareas de finalización de la instalación y de integración en el sistema central del SAT.

4.4 ¿Quién realiza la gestión de la sonda?

La gestión y administración de la sonda se realiza por el personal técnico del CCN-CERT, para mantener un sistema lo más homogéneo posible. Entre las tareas de gestión y administración se incluyen la actualización diaria de las reglas de detección, actualizaciones de sistema operativo, actualización de las aplicaciones, aplicación de parches de seguridad de sistema operativo y de aplicaciones, particularización de las reglas de detección, etc.

4.5 ¿Qué es el sistema central?

El sistema central es el encargado de la recolección de la información proveniente de las distintas sondas y de la correlación de eventos para detectar incidentes de seguridad.

GLORIA es la herramienta que se encuentra desplegada en el sistema central para desarrollar estas tareas y está compuesta por diferentes elementos:

- Recolector de eventos. Es el encargado de recibir los eventos que provienen de los diferentes sistemas a analizar y de enviarlos al bus de eventos del que se nutre el siguiente elemento.
- Motor de correlación. Es el encargado de procesar la información que llega al bus de eventos. Este elemento del sistema implementa reglas de correlación que son las que deciden si se genera o no una alerta en respuesta a los eventos recibidos.
- Consola única de operador. Es la que permite el análisis de las alertas generadas tras la correlación de los eventos recibidos por el sistema.
- Cuadro de mando activo. Es el que presenta información relativa a los procesos monitorizados y permite la visualización de indicadores.

4.6 ¿Quién monitoriza el sistema central?

La gestión, actualización y mantenimiento del sistema central está a cargo del CCN-CERT, que, con un equipo de expertos en seguridad de la información, lleva a cabo tareas de administración, maduración de las reglas de detección y de correlación e inclusión de posibles nuevas fuentes de detección.

4.7 ¿Cómo se envían los eventos al sistema central?

El transporte de los eventos se realiza de forma cifrada a través de un túnel cifrado por la salida de Internet del Organismo hacia el Sistema Central, con lo que la confidencialidad e integridad de los envíos queda garantizada. La conexión entre la sonda individual y el sistema central se puede establecer de dos formas:

- Conexión de la sonda a Internet a través de la infraestructura de Internet del Organismo adscrito.
- Conexión directa de la sonda a una conexión a Internet independiente de la red del Organismo.

4.8 ¿Qué información se envía al sistema central?

Las sondas únicamente envían hacia el sistema central alertas generadas tras la detección de algún tipo de evento, definidos en las reglas de detección integradas en el sistema, y que responden a patrones de tráfico potencialmente dañinos o de comportamientos conocidos de determinado tipo de código dañino.

En **ningún momento se realiza un envío del tráfico de Internet del Organismo** hacia el sistema central, manteniéndose así la privacidad en las comunicaciones.

En el caso de haberse desplegado en el Organismo capacidades de correlación distribuida, hacia el sistema central se enviarán las alertas generadas tras la correlación de las diferentes fuentes de información, no llegando a enviar siquiera los eventos generados por las diferentes fuentes, quedando estos eventos almacenados en el equipo desplegado en el organismo encargado de la recepción de eventos en el entorno distribuido.

4.9 ¿Qué tipo de ataques puede detectar el servicio SAT-INET?

La sonda es capaz de detectar todo tipo de ataques, siempre que se encuentren parametrizados en las reglas de detección desplegadas en el sistema, y dar una respuesta rápida y eficaz ante cualquier incidente. Sin embargo, el trabajo de detección se centrará principalmente en detectar la presencia de código dañino en las redes de las organizaciones y en la detección de intentos de intrusión sobre estas redes.

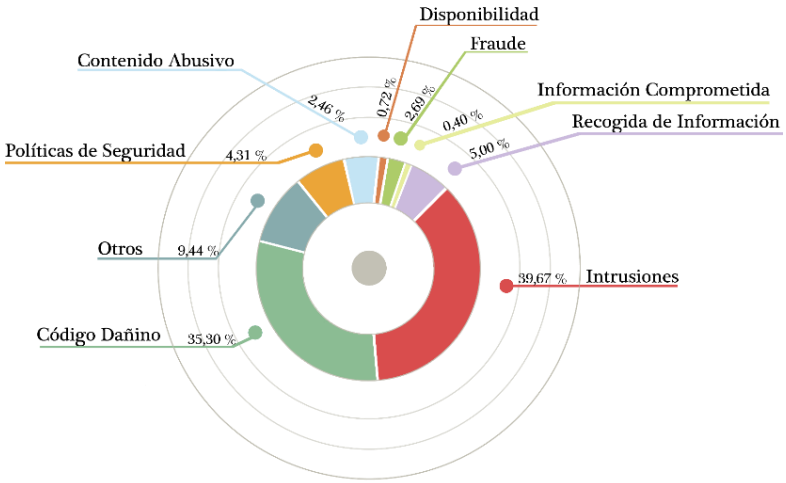

Figura 2. Clasificación de los incidentes notificados en 2017

4.10 ¿Qué es el portal SAT?

El portal del SAT de Internet es el lugar en el que el personal TIC del Organismo adscrito puede visualizar en tiempo real los eventos generados por su sonda y que han sido enviados al sistema central. Además, permite acceder a estadísticas e informes sobre el servicio ofrecido por este Sistema de Alerta Temprana.

En un futuro permitirá también acceder a la herramienta LUCIA, para la gestión de los incidentes que hayan sido detectados por la sonda y comunicados al organismo, y a la herramienta REYES, para agilizar la consulta de información durante la labor de análisis de los incidentes notificados.

El acceso a este portal se ofrece al personal TIC una vez se realiza la instalación de la sonda y el Organismo queda adscrito al SAT de Internet.

4.11 ¿Quién tendrá acceso a la información de mi Organismo?

Únicamente tendrán acceso a la información del Organismo adscrito los responsables de la seguridad TIC seleccionados por el propio Organismo para tal efecto y los administradores del sistema, es decir, el equipo de expertos del CCN-CERT que monitoriza el sistema central de sondas. Ninguna otra persona tendrá acceso a esta información. Es importante saber que ningún Organismo tendrá acceso a la información de otros organismos adscritos y **únicamente podrá ver los eventos generados por su propia sonda y los informes periódicos de su propio organismo**, si bien sí que será usada la detección de eventos distribuida para la generación de la inteligencia del sistema de forma automatizada. En este sentido, como en todas las materias competencia del Centro Criptológico Nacional, la política a seguir será mantener en todo momento la confidencialidad de la información tratada.

4.12 ¿Quién se puede suscribir a este servicio?

Cualquier Organismo perteneciente al Sector Público, empresa pública, operadores críticos del sector público o empresas y organizaciones de interés estratégico para el país pueden adherirse al Sistema de Alerta Temprana de Internet, contactando con el CCN-CERT.

4.13 ¿Qué información voy a recibir si estoy suscrito al servicio SAT-INET?

El Organismo que esté adscrito al Sistema de Alerta Temprana SAT-INET, recibirá periódicamente informes de estado del servicio. Entre otra información, los informes incluyen el código dañino y los ataques detectados en cada Organismo, los incidentes gestionados en un período de tiempo y un listado de todos los incidentes pendientes de resolver.

Del mismo modo, anualmente recibirá un informe en el que se recogerá la actividad de la sonda durante ese periodo e indicadores que permitirán valorar tanto el servicio ofrecido por el SAT como la capacidad de respuesta del Organismo en la resolución de los incidentes de seguridad gestionados.

4.14 ¿Cómo voy a recibir la información de los incidentes?

Para la recepción de los incidentes el Organismo que esté adscrito al Sistema de Alerta Temprana SAT-INET deberá disponer de una cuenta de correo a la que enviar la notificación de los incidentes de seguridad. Esta cuenta de correo deberá ser única, por lo que se recomienda al Organismo la creación de una lista de distribución que reciba todo el personal TIC que vaya a encargarse de la investigación de los incidentes de seguridad.

La información referente a los incidentes de seguridad detectados por el personal técnico del CCN-CERT estará disponible en la herramienta LUCIA, al que tendrán acceso los responsables de seguridad de los Organismos adheridos a este servicio, donde podrán realizar el seguimiento de los incidentes notificados y donde podrán informar de las acciones llevadas a cabo para la resolución del mismo.

LUCIA es la herramienta de ticketing para la gestión de incidentes de seguridad desarrollada por el CCN-CERT (puede encontrar más información referente a LUCIA en https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/lucia.html).

Aunque la información relativa a los incidentes de seguridad notificados al Organismo se encontrarán en la herramienta LUCIA, ante la posible necesidad de intercambio de información referente a los incidentes de seguridad a través del correo electrónico, será necesario que el organismo genere un par de claves PGP/GPG para intercambiar información de manera cifrada en el caso que fuese necesario.

Una vez generadas las claves PGP/GPG asociadas a esta cuenta de correo, el Organismo deberá remitir al CCN-CERT la clave pública para poder cifrar la información que éste quisiera remitir de manera cifrada. Igualmente, el CCN-CERT proporcionará la clave pública de la cuenta de correo utilizada para la notificación de incidentes para que el Organismo pueda también enviarle información cifrada en caso necesario.

5. Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la **información clasificada** (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del **Sector Público** es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de **operadores críticos del sector público** la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

6. Punto de contacto

- Tfno. 91 283 2678 / 91 283 2251
- Web: https://www.ccn-cert.cni.es
- E-Mail: sat-inet@ccn-cert.cni.es