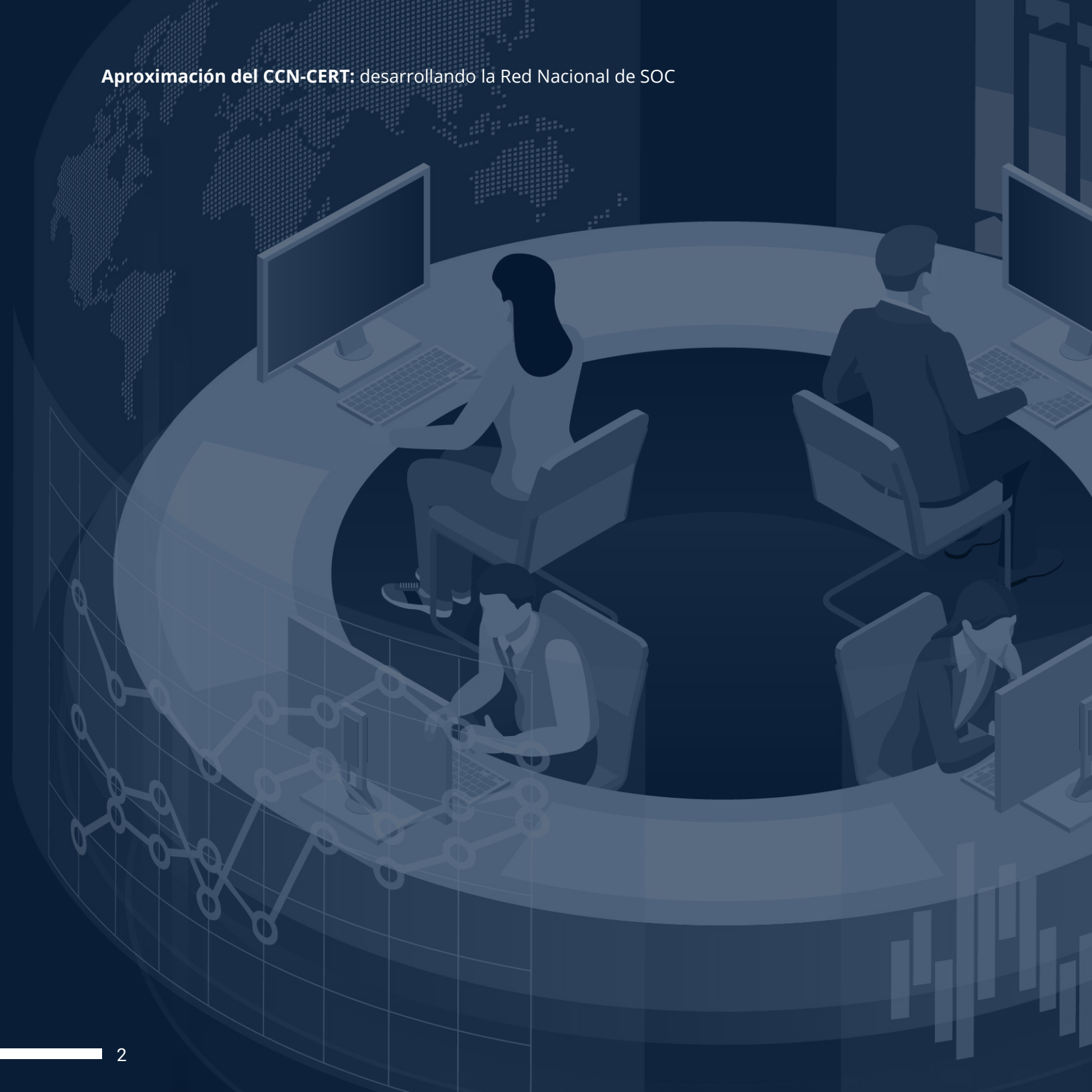
APROXIMACIÓN DEL CCN-CERT:

desarrollando la Red Nacional de SOC

Red Nacional de SOC

OCTUBRE **2021**



ÍNDICE

centro criptológico nacional

1. CERT/CSIRT VS SOC

Los términos CERT[1] o CSIRT[2] son acrónimos del inglés que se emplean indistintamente para definir a los Equipos de Respuesta a Incidentes de Seguridad de la Información.

Estos equipos están enfocados desde sus orígenes en 1988[3] a la gestión de incidentes y tienen la responsabilidad de coordinar y respaldar la respuesta ante cualquier evento de estas características que sufra la Comunidad a la que da servicio. Son entidades organizativas situadas, en la mayoría de los casos, de forma **externa** a la propia organización y tienen un **carácter transversal**, puesto que abordan toda la problemática de un incidente, incluyendo los aspectos legales y normativos, su relación con otros equipos y organizaciones **(coordinación)**, así como su implicación en la ciberseguridad general.

Sin olvidarse, por supuesto, de las actividades posteriores al incidente y diseñadas para prevenir y mitigar futuros ataques.

Al abordar un incidente, el CERT/CSIRT tiene una **visión global** del mismo y puede buscar ataques basados en Indicadores de Compromiso (IOC), reglas definidas y con análisis del tráfico exterior; investigar las **tácticas, técnicas y procedimientos del atacante** (TTP) llegando a su origen e, incluso, aportar vacunas genéricas. Todo ello, abstrayéndose de las particularidades de cada organización.

---

1. Guía CCN-STIC 401. CERT. *Computer Emergency Response Team*. Organización especializada en responder inmediatamente a incidentes relacionados con la seguridad de las redes o los equipos. También publica alertas sobre amenazas y vulnerabilidades de los sistemas. En general tiene como misiones elevar la seguridad de los sistemas de los usuarios y atender a los incidentes que se produzcan.

2. CSIRT *Computer Security Incident Response Team*. Una organización que coordina y apoya la respuesta a los incidentes de seguridad que involucran a sitios dentro de una circunscripción definida". [R2350] (Véase: CERT, FIRST, incidente de seguridad). [RFC4949:2007]

3. En 1988, y ante lo que se consideró el primer gran ciberataque de la historia (gusano Morris), el Departamento de Defensa de Estados Unidos encargó a la Universidad Carnegie Mellon, en Pittsburgh, la creación de un equipo capaz de hacer frente a este nuevo tipo de amenazas. El resultado fue la constitución del primer CERT de la Historia y el registro de la marca. En la actualidad, solo las empresas instaladas en Estados Unidos necesitan un acuerdo con esta entidad para el uso de este acrónimo (https://www.sei.cmu.edu/our-work/cybersecurity-center-development/authorized-users/).

Estos CERT/CSIRT son instrumentos útiles para la **coordinación nacional e internacional** y como último recurso ante emergencias o crisis apoyando a las organizaciones con personal experto y herramientas específicas, pero no pueden resolver la gestión diaria de la ciberseguridad en las organizaciones.

Por su parte, el **Centro de Operaciones de Seguridad**, COS, aunque más conocido, por sus iniciales en inglés, SOC[4], tiene un ámbito de actuación más amplio dentro de una organización y está centrado en su funcionamiento diario.

En este caso, sí son **equipos internos** y entre sus funciones, además de incluir la respuesta al incidente, se encuentran la **prevención, detección, respuesta y recuperación** de los sistemas tras un ciberataque.

Dicho de otro modo, los SOC vienen a ser un centro de mando para los equipos de ciberseguridad IT de una organización. Son responsables de supervisar y proteger la tecnología, la red, servidores, aplicaciones y hardware.

Los esfuerzos de monitorización de un SOC se extienden más allá de la respuesta a un incidente.

Deben vigilar y analizar de **forma constante** las redes y los sistemas para detectar intrusiones y anomalías en tiempo real, parametrizar al atacante (mediante IOCs) e implantar medidas concretas para su mitigación. Todo ello compartiéndolo con su CERT/CSIRT de referencia para evitar la propagación a otras entidades similares a la suya.

Aunque en ocasiones las definiciones puedan ser difusas y muchos servicios puedan estar superpuestos, los CERT/CSIRT suelen actuar de coordinadores de los diferentes SOC.

4. CCN-STIC 401. SOC. Security Operation Center. Un Centro de Operaciones de Seguridad (COS) es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet. Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos.

A su vez, pueden recibir información del CERT y complementarla con información interna de su despliegue y, de esta forma, detectar nuevas relaciones.

En resumen, y aunque en ocasiones las definiciones de uno y otro término puedan ser difusas y muchos servicios puedan estar superpuestos, los CERT/CSIRT suelen actuar de coordinadores de los diferentes SOC.

Principales características

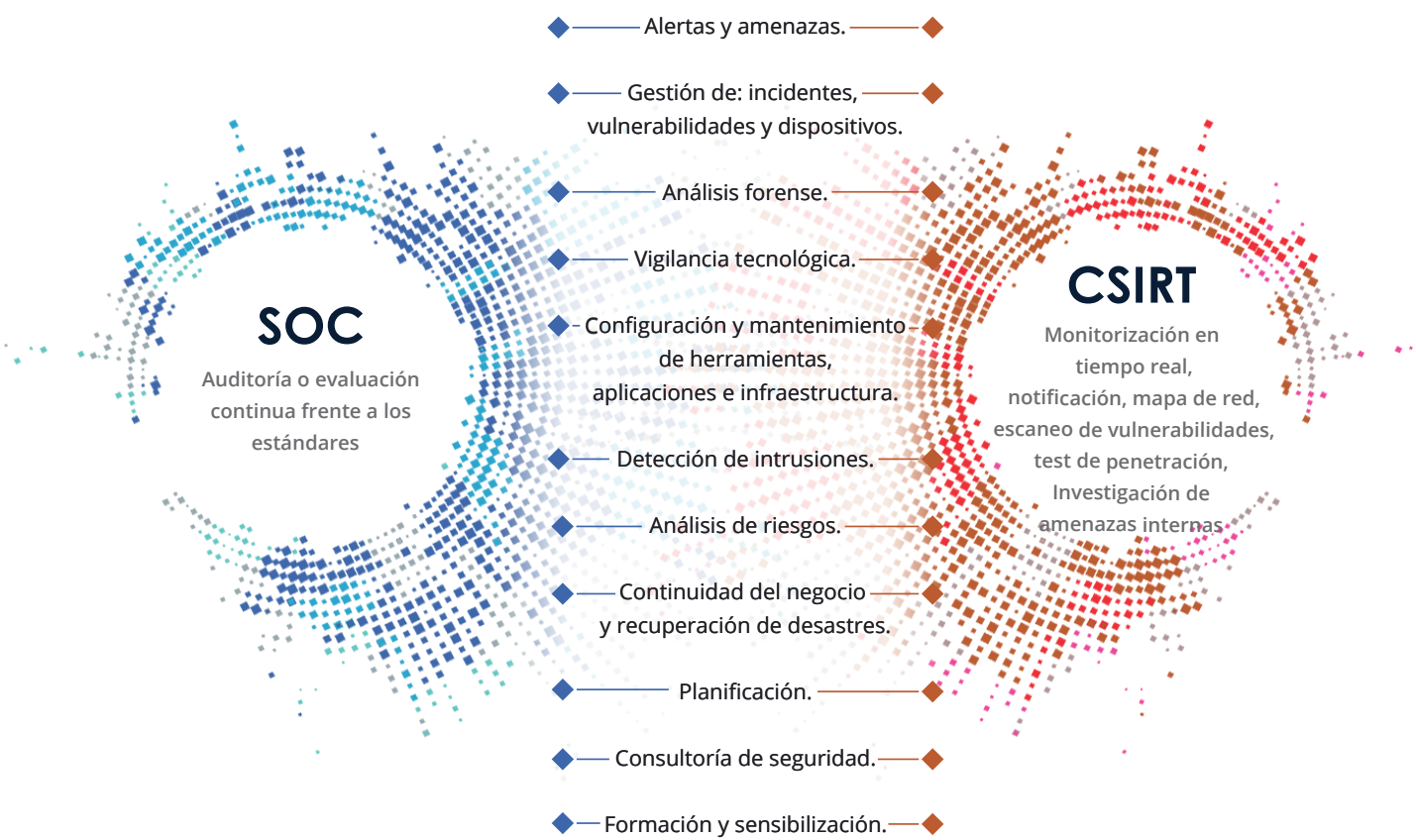
CERT/CSIRT

- Gestión de incidentes.
- Equipo externo.
- Investigación TTPs, origen incidente, vacunas.
- Transversal a todas las áreas.
- Visión global de fuentes externas a la organización.
- Coordinación nacional o internacional.

SOC

- Prevención, monitorización, vigilancia, contención y recuperación.
- Equipo interno, trabajo in situ Vigilancia diaria y constante.
- Área IT. Redes, equipos y sistemas.
- Visión específica de la organización.

Servicios ofrecidos normalmente por un SOC y un CSIRT



2. ¿POR QUÉ UN SOC AHORA?

Hace ya más de 20 años que se acuñó el concepto de SOC. Desde entonces se ha ido interiorizando de manera progresiva y en paralelo al desarrollo de las amenazas y la tecnología. Hoy ya nadie niega la necesidad de disponer, en tiempo casi real, de un panorama consolidado de amenazas, de un conjunto de medios que permita reaccionar de forma rápida ante un ciberincidente, y de capacidades suficientes de detección de las nuevas amenazas.

La proliferación de vulnerabilidades[5] desconocidas para el fabricante (Día 0) o recién publicadas (Día 1)[6] y la sistematización de su explotación por grupos organizados, no deja más opción que desarrollar estos SOC en las organizaciones.

La Unión Europea no ha sido ajena a esta realidad. En el año 2013 se publicó la Estrategia de Ciberseguridad de la Unión Europea.

Tras esta, posteriormente, en 2016, con la publicación de la Directiva NIS en (2016/1148) se insta a los gobiernos a mejorar las capacidades nacionales de ciberseguridad impulsando los CSIRT nacionales, a incrementar la cooperación en la UE obligando a la notificación de ciberincidentes e impulsar la aplicación de medidas de seguridad.

Tras dos años de funcionamiento de las transposiciones nacionales de la directiva NIS y de lo establecido en la estrategia de 2013, la UE está trabajando en una evolución de la citada Directiva, conocida como NIS 2.0.

5. Vulnerabilidad: CCN-STIC 401. Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza.
6. Vulnerabilidad DIA 1. Vulnerabilidades cuya resolución acaba de publicar el fabricante pero que tienen posibilidad de explotación inmediata por parte de un atacante con resultado de elevación de privilegios, denegación de servicio o explotación de código en remoto entre otros impactos. La actualización de la tecnología se debe hacer de forma inmediata.

La Comisión Europea propone crear una red de centros de operaciones de seguridad en toda la UE, coordinados adecuadamente con la red de CERT/CSIRT, y dotará de financiación a este tipo de proyectos.

Finalmente, en diciembre de 2020 se publicó la nueva Estrategia de Ciberseguridad para le Década Digital de la UE[7] donde señala que *las redes y los sistemas informáticos requieren una vigilancia y un análisis constantes para detectar intrusiones y anomalías en tiempo real*. El texto continúa: *este tipo de centros son vitales para recopilar registros y aislar los acontecimientos sospechosos que ocurren en las redes de comunicación que vigilan*.

Por este motivo, la Comisión propone crear una **red de centros de operaciones de seguridad en toda la UE**, que coordinados adecuadamente con la red de CERT/CSIRT contribuirá a apoyar la mejora de los centros existentes y el establecimiento de otros nuevos, así como la formación y el desarrollo de capacidades del personal que trabaja en estos centros. El órgano ejecutivo europeo dotará de financiación a este tipo de proyectos.

7. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

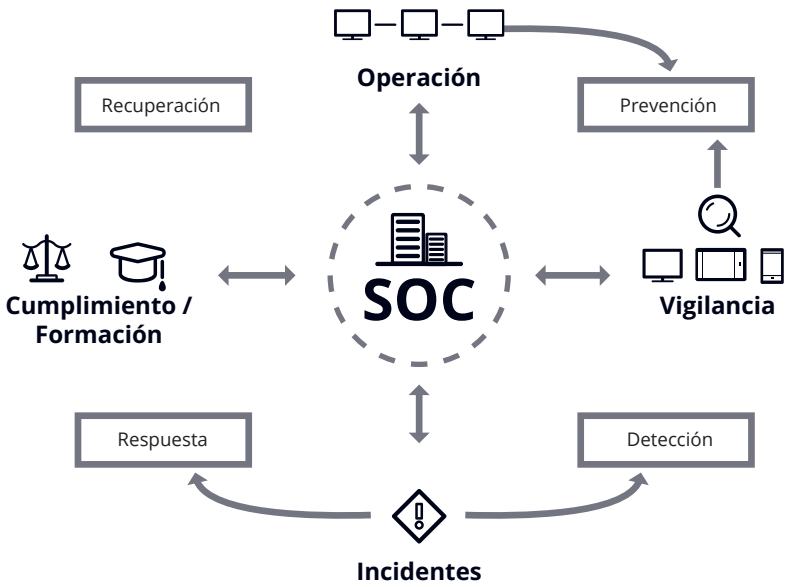
3. EJES Y FUNCIONES DE UN SOC

La situación de cada organización es diferente: objetivos, usuarios, infraestructura, dimensión, etc. De ahí que, a la hora de desplegar un SOC, cada eje y función deba personalizarse acorde a los objetivos y el grado de madurez de esta.

Las dimensiones de la organización es otro factor fundamental a tener en cuenta. Esta dimensión estará directamente relacionada con la entidad del SOC que podrá desplegar todos los pilares o solo algunos, e incluso mantener alguno en modo virtual.

No obstante, podemos concretar cuatro grandes ejes (Operación, Vigilancia, Incidentes y Cumplimiento/Formación) sobre los que pivotar un SOC, asociados cada uno de ellos a las funciones básicas que deben tener este tipo de centros: **prevención, detección, respuesta y recuperación** de los sistemas tras un ciberataque.

Eje y funciones de un SOC

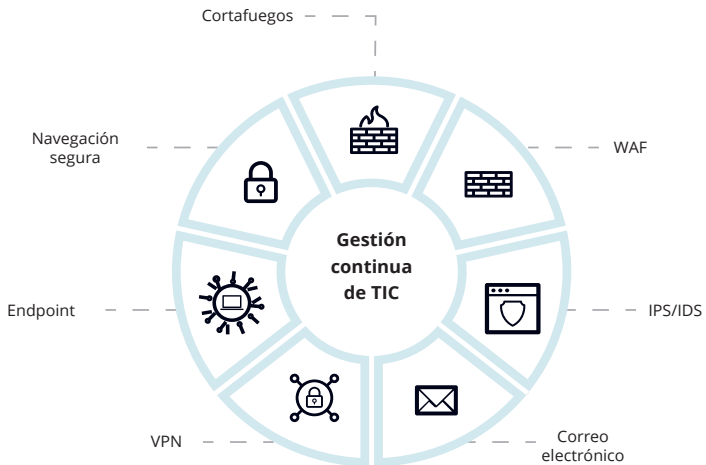


3.1 OPERACIÓN. Prevención

Corresponde a la gestión diaria de aquellos elementos TIC que proporcionan seguridad a la organización: cortafuegos, WAF[8], IPS/IDS[9], correo electrónico, acceso remoto (VPN[10]), seguridad del Endpoint[11], navegación segura, prevención de fuga de datos, etc.

Aunque en numerosas ocasiones la gestión rutinaria de todos estos aspectos lo realiza el equipo TIC de la organización, ajeno al SOC, su traspaso y supervisión por parte del centro de operaciones y su personal con conocimientos de seguridad será una garantía para la mejor administración de las redes y sistemas.

Todo ello dependerá de la entidad y madurez de la organización y de si se recurre a una empresa externa para proporcionar seguridad. En este caso es muy frecuente que sean profesionales con conocimiento de seguridad quienes gestionen los elementos TIC.



Operación

8. Web Application Firewall.
9. IPS: Intrusion Prevention System / IDS: Intrusion Detection System: Sistemas de prevención y detección de instrusiones.
10. VPN: Virtual Private Network. Red Privada Virtual.
11. Endpoint: sistema de seguridad al "final" de la estructura de red (los equipos conectados a la red de una organización: portátiles, móviles, etc.).

3.2 VIGILANCIA. Prevención

La evaluación y vigilancia permanente de todos los recursos que tenemos expuestos o con posibilidad de ser atacados (superficie de exposición y estado de la seguridad) es una actividad crítica en cualquier organización. Por ello, es preciso tratar las deficiencias de seguridad que pueden ser:

- **Técnicas** (bugs, configuraciones erróneas, servicios activos inesperados, puertas traseras, etc.).
- **Humanas** (falta de concienciación, inexperiencia, formación inadecuada, etc.).
- **De procedimiento** (inexistencia de documentación, acciones incorrectas o fuera de procedimiento definido, ausencia de verificaciones, etc.).
- **Legislativas/normativas** (desviación frente a los requisitos definidos como de obligado cumplimiento).

El desarrollo de las amenazas y la evolución de la superficie de exposición hace necesaria la realización de auditorías, así como inspecciones técnicas de forma periódica.

El desarrollo de las amenazas y la evolución de la superficie de exposición hace necesaria la realización de **auditorías**, así como **inspecciones técnicas** de forma periódica.

Vigilancia

3.3 INCIDENTES. Detección y repuesta

La comunicación de los incidentes a través de la herramienta LUCIA del CCN-CERT que permite comunicar los incidentes directamente a los actores involucrados y a los órganos administrativos que, por ley, es preciso notificar.

La gestión de incidentes pasa por una detección y respuesta eficiente. Para ello es preciso el análisis de los registros y evidencias generadas por las diferentes fuentes que, en el caso de los SOC, al estar desplegados in situ pueden actuar sobre los sistemas comprometidos de forma mucho más rápida.

Algunos de los controles y medidas de detección recomendables son:

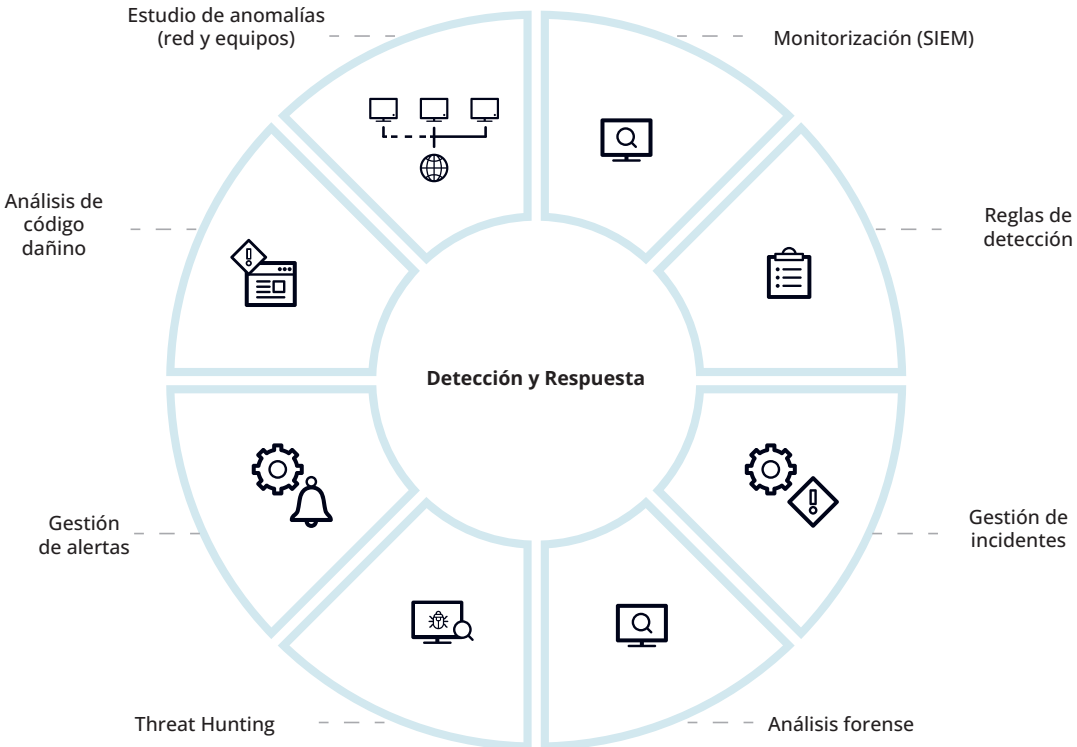
- Monitorización y correlación de eventos (SIEM).
- Inclusión de reglas de detección desde los puntos finales al perímetro externo.
- Gestión de incidentes y análisis forense.
- Búsqueda de amenazas ocultas (Threat Hunting). Gestión de alertas, incluidas las AntiDDoS.
- Análisis de código dañino.
- Estudio de anomalías en la red o en el comportamiento de equipos y usuarios.

Una mejor detección y respuesta pasa por la automatización de procesos, el uso de herramientas (*véase Anexo I*) y el intercambio de información con otros SOC.

Todo ello dará lugar a la generación de casos de uso y procedimientos que marcará las actuaciones de respuesta ante un incidente en un futuro.

La comunicación de los incidentes se realizará por medio de la herramienta LUCIA del CCN-CERT. La ventaja de esta herramienta es su capacidad de comunicar los incidentes directamente a los actores involucrados y a los órganos administrativos que, por ley, es preciso notificar la existencia del incidente. Estas acciones ahorran trámites y mejoran la eficiencia de las comunicaciones entre las partes que deben estar implicadas en un incidente.

Detección y respuesta en un SOC



3.4 CUMPLIMIENTO NORMATIVO. Esquema Nacional de Seguridad

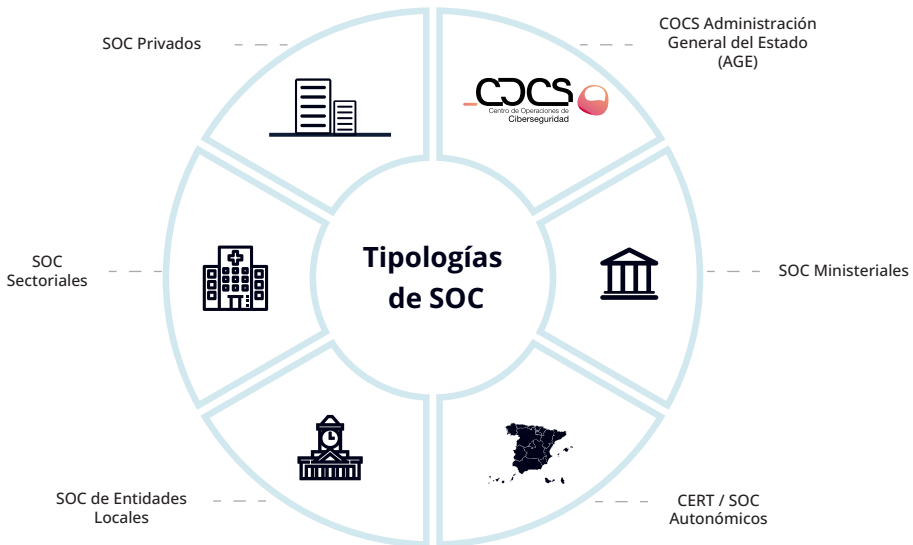
Todos los puntos anteriores deben estar basados en un marco legal que permita realizar las actuaciones necesarias de forma inmediata. En base a la experiencia del CCN-CERT, cualquier iniciativa en la creación de este tipo de estructuras debe ir acompañada de un proceso de implantación del Esquema Nacional de Seguridad (ENS)[12] como marco de referencia en medidas de seguridad a adoptar.

12. Esquema Nacional de Seguridad. Conjunto de 6 principios básicos, 15 requisitos mínimos y 75 medidas de seguridad de obligada aplicación en el sector público español con tres niveles de aplicación (BASICO, MEDIO y ALTO) que proporciona la medida del nivel de seguridad de un organismo. La CCN-STIC 825 establece su relación con el estándar internacional SO/IEC 27001 e ISO/IEC 27002. https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2148-ccn-stic-825-ens--national-security-framework-27001-certifications/file.html

4. TIPOLOGÍAS DE SOC

Por lo expuesto hasta el momento, el CCN-CERT considera necesario el desarrollo de servicios horizontales de seguridad gestionados a través de SOC en diferentes ámbitos: Administración General del Estado (AGE), comunidades autónomas, entidades locales y sectoriales.

En todas las tipologías de SOC se utilizará **LUCIA**[13] para la comunicación de incidentes de seguridad debido a su capacidad de notificación a los organismos que deben estar informados y participantes en la investigación.



13. LUCIA: https://www.ccn-cert.cni.es/soluciones-seguridad/lucia.html

4.1 COCS Administración General del Estado (AGE)

Liderado por la Secretaría General de Administración Digital (SGAD), con el apoyo técnico del CCN-CERT, es uno de los grandes retos para los próximos tres años. Proporcionará servicios horizontales de seguridad a más de 105 entidades de toda la Administración y será un referente para el sector público. Este centro será financiado a través del Plan de Recuperación, Transformación y Resiliencia.

El CCN-CERT brindará apoyo a este Centro con su personal además de ofrecer sus herramientas[14] para la detección de ciberataques. Entre otras:

Sistema de Alerta Temprana, SAT, que proporciona alerta y avisos ante posibles incidentes. Con ello se aumentará las capacidades de detección del COCS-AGE.

CLAUDIA, solución de endpoint para la detección de malware complejo y movimientos laterales.

MicroCLAUDIA, protección frente al ransomware.

CARMEN, intensificará la detección de APT o malware sofisticado en la red interna de los organismos.

14. Soluciones del CCN-CERT: https://www.ccn-cert.cni.es/soluciones-seguridad.html

4.2 SOC Ministeriales

Como experiencia previa, el CCN está impulsando la implantación de SOC en diferentes Ministerios que serán reemplazados o complementados por el COCS AGE. Es el caso de los Centros de Operaciones de Seguridad desarrollaos en el Mº de Justicia, Defensa e Interior.

El primero de ellos, el SOC de la **Administración de Justicia**, en funcionamiento desde 2019, ha servido al CCN-CERT para parametrizar, aprender y conocer los recursos económicos y humanos necesarios para ofrecer estos servicios.

En este caso, el CCN-CERT además del apoyo de su personal, ofrece las siguientes herramientas:

ANA[15] seguimiento de auditorías y control sobre las correcciones que se realizan en las vulnerabilidades detectadas.

CLAUDIA para realizar vigilancia de los equipos y poder mejorar las capacidades de detección.

CARMEN en la lucha contra grupos de espionaje o malware sofisticado.

15. https://www.ccn-cert.cni.es/soluciones-seguridad.html

4.3 CERT / SOC Autonómicos

En estos momentos existen centros de estas características en Andalucía (ANDALUCIA-CERT), Cataluña (ACC), Comunidad Valenciana (CSIRT-CV), Galicia (CSIRT.gal), Región de Murcia (CSIRT CARM) y País Vasco (Basque Cybersecurity Center).

A ellos se unen otros organismos autonómicos que ofrecen parcialmente este tipo de servicios, como Madrid, y otros que están en periodo de implantación.

Sea cual fuere la situación, el CCN-CERT pretende seguir impulsando la constitución de CERT/SOC autonómicos.

REYES, solución para compartir los diferentes indicadores de ataques entre los CERT/CSIRT y SOC autonómicos, potenciando la velocidad de intercambio y mejorando las tareas de detección (véase Anexo I).

Mediante REYES se puede compartir los diferentes indicadores de ataques entre los CERT/CSIRT y SOC autonómicos, potenciando la velocidad de intercambio y mejorando las tareas de detección.

4.4 SOC de Entidades Locales

En España existen 8.131 municipios, de los cuales solo 63 tienen más de cien mil habitantes y la inmensa mayoría (7.715) poseen una población inferior a 20.000. Desarrollar las capacidades que requiere un SOC en esto últimos municipios es algo imposible para todos ellos. No obstante, y según la normativa vigente, las Comunidades Autónomas uniprovinciales tienen la obligación de proporcionar los servicios TIC a los Ayuntamientos o Entidades Locales con una población inferior a los 20.000 habitantes. En el caso de las autonomías pluriprovinciales, esta responsabilidad recae en las Diputaciones, Consejos Insulares y Cabildos[16].

El CCN-CERT está impulsando la constitución de SOC Virtuales en Entidades Locales en donde una Diputación/ Consejo Insular/Cabido ofrezca estos servicios a todos los municipios de su demarcación.

Por todo ello, el CCN-CERT está impulsando también la constitución de SOC Virtuales en Entidades Locales en donde una Diputación/Consejo Insular/Cabido ofrezca estos servicios a todos los municipios de su demarcación. Para facilitar este impulso, el CCN-CERT ofrecerá las diferentes herramientas ya mencionadas y con ellas mejorar las capacidades de detección, notificación de incidentes y seguimiento de auditorías.

El CCN-CERT ofrece distintas herramientas, entre otras:

MicroCLAUDIA, para la protección frente al ransomware o frenar ataques de una forma más rápida y en coordinación directa con el CCN-CERT.

16. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192

En la actualidad existen proyectos iniciales con servicios de detección en Córdoba, Cádiz, Zaragoza y Valencia, mientras que en Murcia, Asturias, Navarra y Cabildo de Tenerife, se está acompañando a los organismos en el cumplimiento del ENS, y en servicios de vigilancia, detección y respuesta.

Estos servicios horizontales en ciberseguridad se pueden proporcionar en coordinación con los CSIRT/CERT/SOC autonómicos para buscar la máxima eficiencia del gasto en ciberseguridad.

4.5 SOC Sectoriales

Los SOC sectoriales tienen la misma filosofía que los centros descritos anteriormente, pero en este caso están dirigidos a sectores identificables con los **servicios esenciales** establecidos en la Directiva NIS: Salud, Distribución Alimentaria, Aguas, Autoridades Portuarias, Confederaciones Hidrográficas, etc.

En este epígrafe se englobarían entidades públicas que ofrecen servicios sin ser Ministerios o Entidades Locales.

Sus servicios son esenciales lo que propicia que sean objetivos principales de ciberataques y necesiten un SOC para mejorar sus capacidades de detección y repuesta.

Un ejemplo de ello son los servicios **andaluz, extremeño y madrileño** de **Salud** que se han presentado a fondos *Conection Europe Facility* (CEF) con los que dar servicio de detección tanto a la red corporativa como a la red de control industrial (quirófanos, aparatos de electromedicina y otros dispositivos).

Además, se ha iniciado un proyecto con **Red IRIS** para proporcionar servicios similares para Infraestructuras Científicas y Técnicas Singulares (ICTS), derivada de la reciente amenaza contra estos centros de investigación (algunos intervienen en desarrollo de vacunas y otros tratamientos).

En los SOC sectoriales se englobarían entidades públicas que ofrecen servicios sin ser Ministerios o Entidades Locales. Sus servicios son esenciales lo que propicia que sean objetivos principales de ciberataques y necesiten un SOC para mejorar sus capacidades de detección y repuesta.

Este proyecto también contempla el cumplimiento y adecuación al Esquema Nacional de Seguridad como ejemplo catalizador de la implementación y gestión centralizada de la seguridad.

4.6 SOC Privados

El alcance de un SOC, con la infraestructura y perfiles profesionales que requiere, es muy difícil cubrirlo íntegramente con personal propio. De ahí, que se contemple la interacción con Centros de Operaciones de Seguridad privados que den servicio a las distintas Administraciones Públicas.

Estos SOC colaborarán con el CCN-CERT a través de distintas herramientas como:

LUCIA, en la comunicación de incidentes (véase Anexo I).

REYES, para el intercambio de información, gracias al cual, colaborarán en la Red Nacional de SOC y se beneficiarán de los mecanismos de detección del sector público (véase Anexo I).

5. ¿CÓMO IMPLEMENTAR UN SOC CON EL CCN-CERT?

Todo aquel organismo del sector público que desee implementar un SOC puede contar con la asistencia del CCN-CERT.

Para ello, tal y como ya se ha hecho con otros organismos, se firma un convenio de colaboración entre todas las partes implicadas (organismo, CCN y empresa) y se detallen las responsabilidades de cada una, al tiempo que se analizan las acciones previas al despliegue del SOC:

- **Estudio preliminar:** información para evaluar los sistemas a proteger y estado de la seguridad.
- **Definición de los objetivos de vigilancia** para el Organismo y casos de uso.
- **Métricas iniciales de superficie de exposición**, estado interno de la seguridad y medición del desempeño del SOC.
- **Apoyo de consultoría** sobre la formación y operación del SOC.
- **Apoyo al Organismo** en la redacción del pliego de prescripciones técnicas.

Como ya se ha comentado con anterioridad, este tipo de proyectos contarán con financiación europea y deberán ajustarse a las características de cada entidad. En función de los requerimientos de cada una, el CCN-CERT aportará unos u otros servicios, aunque existen algunos que se consideran indispensables:

Integración en LUCIA
(herramienta de notificación de incidentes)
Ver Anexo I

Integración en REYES
(herramienta para compartir información de amenazas)

La valoración del cumplimiento del organismo con el **ENS**, la adhesión al **Sistema de Alerta Temprana** (Internet, SARA o ICS), las licencias o instalación de algunas de sus herramientas como **microCLAUDIA** (vacuna frente al ransomware) o **ANA** (auditoría continua) y el apoyo en la investigación de **incidentes**, particularmente los críticos, son algunas de las aportaciones del CCN-CERT a todos los organismos públicos.

Pasos para implementar un SOC

CCN-CERT / Organismo público / Empresa

1. Acuerdo CCN-CERT/AAPP/Empresa

2. Evaluación de sistemas a proteger y estado la seguridad

3. Definición de objetivos de vigilancia

4. Métricas de superficie de exposición

5. Consultoría formación y operación SOC

6. Ayuda en redacción de pliego de prescripciones técnicas

Financiación europea

Integración con herramientas CCN-CERT

/lucía> /reyes>

Adicionalmente

/sat> /claudia> /μclaudia> /ana> /carmen>

6. RED NACIONAL DE SOC

La magnitud de incidentes como el WannaCry o los derivados de la pandemia han demostrado la necesidad de intercambiar información entre todos los actores cíber.

Si con el primero se reactivó el **Foro CSIRT.es**, en el que se reúnen todos los CSIRT con representación en España, en estos momentos se pretende dar un paso más y crear la **Red Nacional de SOC** con la que mejorar las capacidades de protección y defensa del ciberespacio español.

Este giro de tuerca viene avalado, como ya se ha mencionado, por la **Unión Europea** y su propuesta de crear una red de centros de operaciones de seguridad en toda la UE, coordinados adecuadamente con la red de CERT/CSIRT.

Esta Red Nacional debe buscar una mayor coordinación y un intercambio de información más detallado entre todos sus miembros. Para ello se necesitará el apoyo del sector privado que facilite la implantación de nuevos Centros de Operaciones de Seguridad en el sector público y la experiencia del Foro CSIRT.es.

A pesar de la creación de esta Red, hay que tener en cuenta que la compartición de información en el ámbito de la ciberdefensa no es una tarea sencilla.

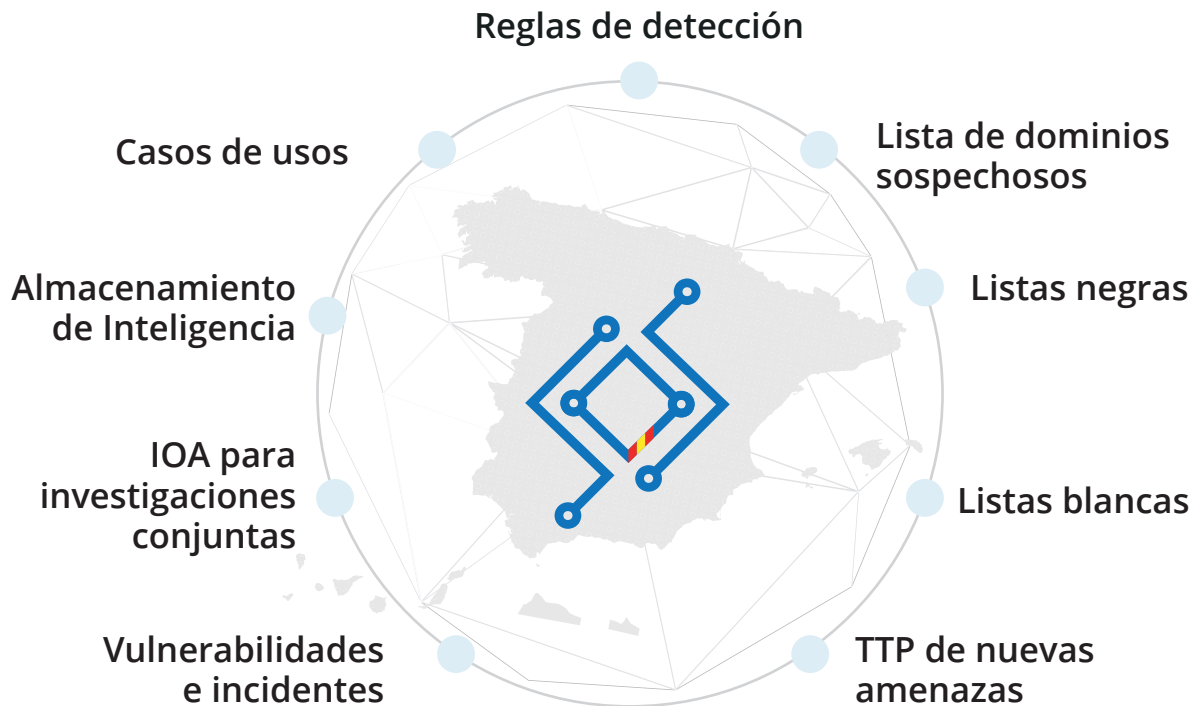
Tiene los límites del negocio de los que participan de él y no se puede olvidar que cada CSIRT o SOC tiene detrás una empresa que está haciendo negocio y puede (debe) compartir información hasta cierto punto en aras a mantenerse en el mismo.

El CCN-CERT pondrá sus herramientas a disposición de la Red Nacional de SOC. En concreto, LUCIA, para centralizar la gestión de todos los incidentes del sector público, y REYES, como base de la ciberinteligencia a compartir.

Todos los SOC se integran con el CCN-CERT mediante las herramientas **LUCIA** y **REYES** que constituirán la base la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes[17]. El funcionamiento de dicha Plataforma se describe más adelante.

Una vez establecido el SOC, se trataría de establecer un **modelo colaborativo** en el que en base a unos incentivos se facilite el intercambio de información. Los datos más susceptibles de intercambiar serían entre otros:

Información a compartir en la Red Nacional



17. CCN-CERT, INCIBE-CERT y Mando Conjunto del Ciberespacio, tal y como recoge el Real Decreto-Ley 12/2018, de 7 de septiembre.

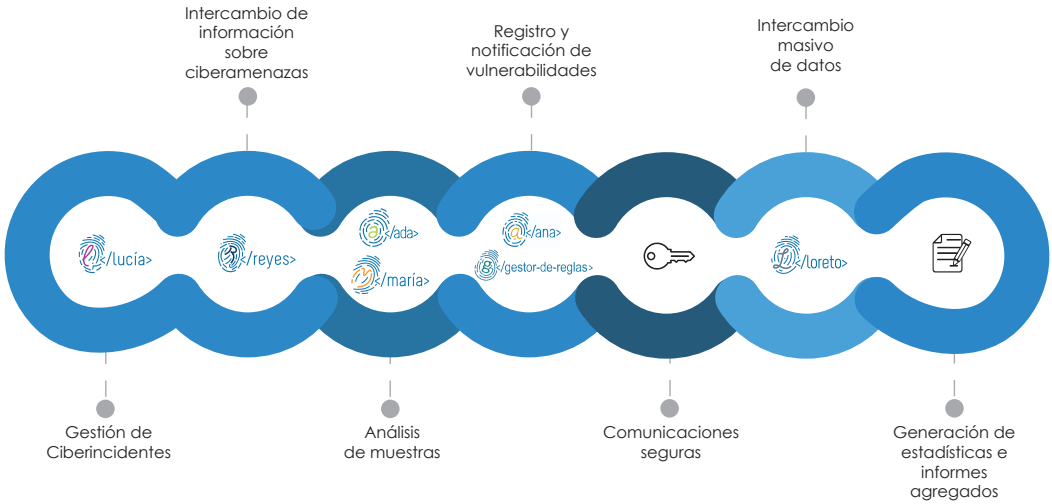
7. PLATAFORMA NACIONAL DE NOTIFICACIÓN DE CIBERINCIDENTES

Para coordinar esta Red Nacional de SOC, el RD 43/2021, de 26 de enero, que desarrolla la directiva de seguridad en redes de la UE establece en su artículo 11 la creación de una ***Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes****.*

Esta plataforma debe ser el instrumento de los tres CERT de referencia (el CCN-CERT en el caso del sector público -*véase Anexo II*-) para coordinar e intercambiar información de forma ágil con sus organismos atendidos que, a su vez, deben estar protegidos por un SOC público o privado.

Esta Red Nacional de SOC dispondrá de un portal web donde estarán los diferentes repositorios de compartición de información, foros para la resolución de problemas comunes y discusión de las ciberamenazas más actuales.

Capacidades de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes



ANEXO I. Herramientas de intercambio

El CCN-CERT pone a disposición del sector público sus herramientas de intercambio de ciberincidentes (LUCÍA) y de ciberamenazas (REYES).

7.1 LUCÍA. Intercambio de ciberincidentes

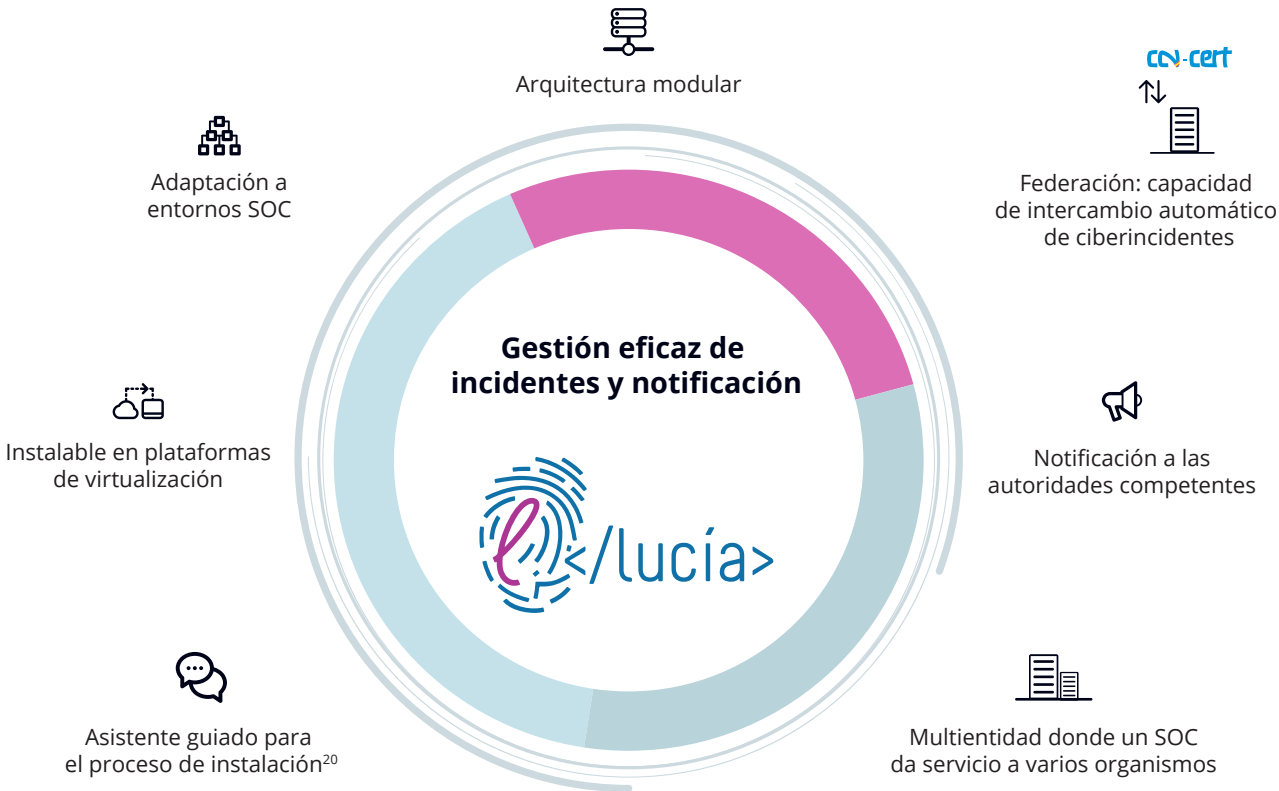
Saber qué y en qué momento notificar un incidente es uno de los aspectos clave para cualquier organización. Para la primera cuestión, España cuenta con dos guías muy importantes que definen claramente la taxonomía y criticidad de los incidentes[19]. Documentos que han sido consolidados y establecidos como obligatorios en el citado RD 43/2021, y que da respuesta a la segunda cuestión.

Sin embargo, es preciso dar un paso más en la notificación de incidentes. No solo hay que notificarlos. Es necesario intercambiar toda la información posible sobre ellos. De lo contrario, sin los datos técnicos y reales del incidente no se puede actuar sobre él ni impedir su propagación a otras organizaciones.

Para ello, el CCN-CERT lleva desde 2014 desarrollando la herramienta LUCÍA. Esta solución permite intercambiar de forma automática toda la información de un ciberincidente, posibilitando la ayuda y el soporte del CCN-CERT al organismo afectado, así como la inteligencia que el CERT Gubernamental posee.

19. Guía CCN-STIC 817 y la Guía Nacional de Notificación y Gestión de Ciberincidentes.

Capacidad de LUCIA 4.1



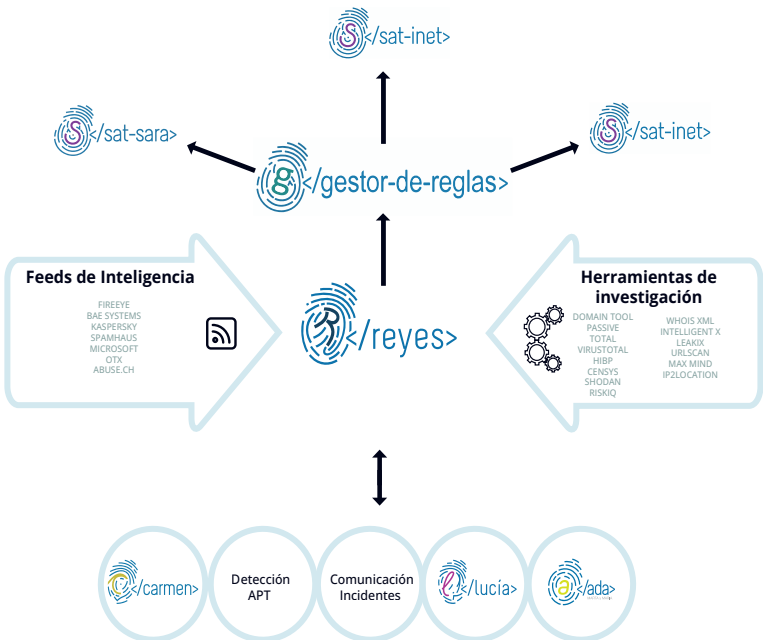
20. LUCIA Demo (http://ccn-cert.net/luciademo). Disponible para descarga con todos los servicios necesarios autocontenidos.

7.2 REYES. Intercambio de ciberamenazas

REYES es una herramienta para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas.

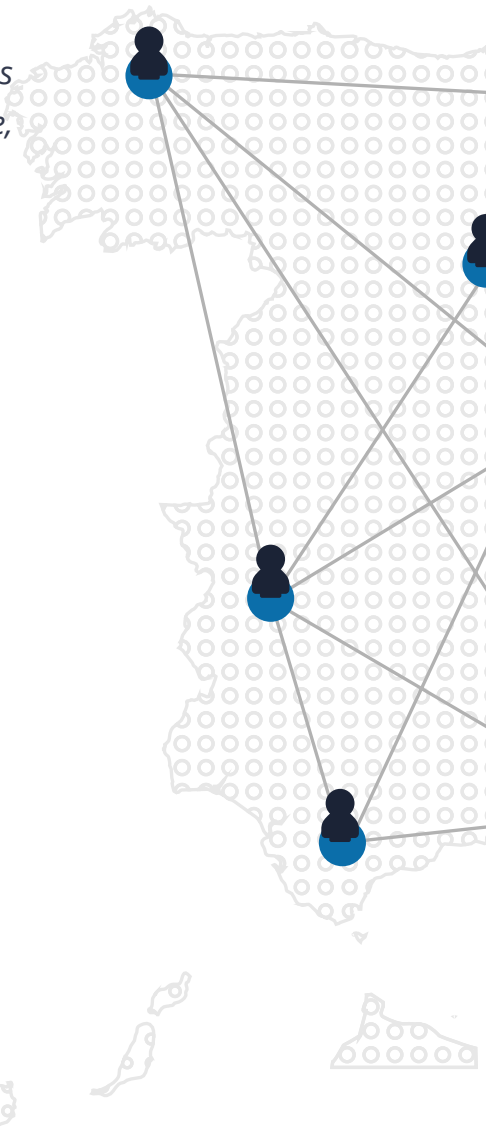
A través de este portal centralizado de información puede realizarse cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes. Una información contextualizada y correlada con las principales fuentes de información, tanto públicas como privadas. e integrada con un conjunto de herramientas de investigación para la parametrización completa del atacante.

Funcionalidades REYES



ANEXO I. Gobernanza de CERT y SOC en España

En España, los SOC que se desplieguen para dar apoyo en los centros del sector público se coordinarán a través de su CERT de referencia que, en este caso es el CCN-CERT.



A continuación, se recoge la legislación que establece este papel de coordinación del CCN-CERT:

RD 3/2010 que regula el **Esquema Nacional de Seguridad (ENS)**.

- **Artículo 36**: "*...notificación al Centro Criptológico Nacional de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados*". Desarrollado en la **Instrucción Técnica de Seguridad**: Notificación de incidentes de seguridad. (BOE nº 95 (19.04.2018).

- **Art.37.1. a)** "*El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las Administraciones públicas*".

- **Art. 37.2.** "*El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las Administraciones públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquél, será coordinador a nivel público estatal*".

RDL 12/2018 Artículo 11. Define las funciones de los equipos de respuesta a incidentes y la necesidad de su coordinación. En su apartado 2 establece que en los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, ***el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT***. Esta coordinación se concreta en el RD 43/2021 que desarrolla el anterior.

RDL 14/2019 por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. **Artículo 7**. Modificación del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Otorga al ***CCN-CERT la coordinación CSIRT públicos y el enlace con exterior***.

RD 43/2021 que desarrolla el RDL 12/2018 que traspone Directiva NIS. **Art 11**. Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes. ***Asigna al CCN-CERT la responsabilidad de su desarrollo y soporte***.

WWW.CCN-CERT.CNI.ES
WWW.CCN.CNI.ES
OC.CCN.CNI.ES

CCN-CERT
centro criptológico nacional