CENTROS DE OPERACIONES DE CIBERSEGURIDAD (SOC) y RED NACIONAL DE SOC (RNS)

Red Nacional de SOC

Liderado por CCN-CERT

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

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

01

SOBRE EL 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 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS).

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 cumplimiento del RD 12/2018, de seguridad de las redes y sistemas de información, en el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC. Pero 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 todos los CSIRT nacionales.

02

OBJETIVO DE ESTE DOCUMENTO

Fruto de la experiencia de estos años de funcionamiento, se ha podido constatar que, si bien se dispone de un marco regulatorio extenso y maduro, cuya referencia fundamental es el Esquema Nacional de Seguridad (ENS, recientemente actualizado, RD 311/2022), el grado de cumplimiento por parte de las distintas administraciones es muy heterogéneo debido a múltiples factores: al progresivo proceso de transformación digital de las distintas administraciones que requiere de continuas inversiones económicas, se añade unos recursos humanos especializados que no están disponibles en la mayor parte de las administraciones, o en muchos casos , están desfasados.

Cada organismo de la Administración Pública que se incorpora al proceso de digitalización, ofreciendo sus servicios a través de plataformas digitales, debe hacerlo adoptando las medidas de ciberseguridad (exigidas en el ENS), para no poner en riesgo el funcionamiento de la administración y los datos sensibles de los ciudadanos que manejan. Una parte importante de estas medidas de seguridad se puede atender con el despliegue de un **Centro de Operaciones de Ciberseguridad** (SOC, por sus iniciales en inglés)

Por último, y además del apoyo que ya presta el CCN-CERT en la respuesta a incidentes de ciberseguridad a nivel nacional, se considera necesario formalizar una nueva línea de trabajo que se va a llamar **Red Nacional de SOC**, (RNS), que pretende dar un nuevo impulso a la mejora de la ciberseguridad de la Administración Pública, creando un nuevo entorno de colaboración con todos los SOC que se vayan creando.

El objeto de este documento es explicar en detalle qué entiende el CCN-CERT por SOC, así como dejar claro en qué consiste la RNS.

03 ESTRATEGIAS Y PLAN NACIONAL DE CIBERSEGURIDAD

La Estrategia de Seguridad Nacional 2021, aprobada en Consejo de Ministros mediante Real Decreto 1150/2021, de 28 de diciembre, identifica la vulnerabilidad del ciberespacio como un riesgo para la seguridad nacional, siendo este un espacio común global en el que se distinguen dos tipologías generales de amenazas, por un lado las acciones disruptivas cuyos ejemplos más representativos, entre otros, son los ataques tipo “ransomware” o la “denegación de servicios” y por otro, su posible utilización para llevar a cabo actividades ilícitas como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización”.

Dada la importancia de contar con un ciberespacio más seguro para hacer frente a las amenazas que afectan a la Seguridad Nacional, el Consejo de Seguridad Nacional, aprobó la Estrategia Nacional de Ciberseguridad, desarrollada por el Consejo Nacional de Ciberseguridad, entre cuyas funciones se encuentran el proponer las directrices en materia de planificación y coordinación de la política de Seguridad Nacional relacionadas con la ciberseguridad.

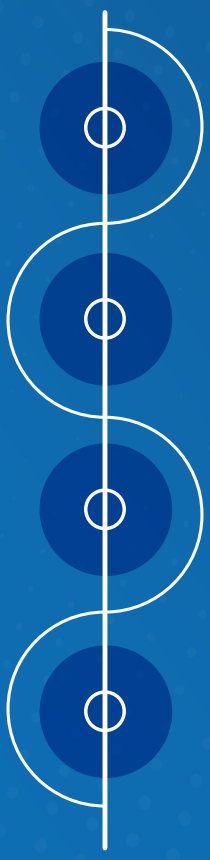
La Estrategia establece la hoja de ruta de España en el marco de la ciberseguridad. Por este motivo se elabora el Plan Nacional de Ciberseguridad al objeto de concretar, a través de actuaciones y proyectos específicos, las medidas recogidas en la Estrategia mediante la participación activa de los principales órganos y organismos nacionales con competencias en ciberseguridad, con el objetivo de identificar aquellas medidas en las que se deben priorizar esfuerzos y recursos.

Los Objetivos del Plan Nacional de Ciberseguridad se derivan de la Estrategia Nacional de Ciberseguridad con el compromiso de que "España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socioeconómico."

El Plan Nacional de Ciberseguridad recoge en concreto como medida urgente potenciar las capacidades de los CSIRT de referencia, así como constituir los siguientes SOC:

Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos.

Infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y en sus organismos vinculados o dependientes.



Centro de Operaciones de Ciberseguridad (COCS) del Ministerio de Defensa, en coordinación con el CCN, para reforzar las estructuras de seguridad y la capacidad de vigilancia de los sistemas de información clasificada.

Centro de Operaciones de Ciberseguridad para las Infraestructuras Científicas y Técnicas Singulares (ICTS) que permita proporcionar servicios de ciberseguridad horizontales a estas instalaciones.

04 SOC. VISION DEL CCN-CERT.

Para garantizar un nivel de seguridad adecuado en los sistemas, es necesario actuar antes de que se produzca un incidente o, por lo menos, ser capaz de detectarlo en un primer momento para reducir su impacto y alcance.

La implantación del SOC no es una tarea fácil, y requiere de **un proceso de mejora continua**, es decir, requiere de recursos económicos y humanos que no siempre estarán disponibles, por lo que, en distintas fases, y en función de los recursos disponibles en cada momento, se deberá ir mejorando su implantación. Esta **aproximación por iteraciones**, debe ir atendiendo las vulnerabilidades más importantes en un orden priorizado, aumentando el nivel de madurez de la ciberseguridad del organismo progresivamente.

Un SOC le proporciona a la organización las capacidades de **prevención** (ampliando el conocimiento respecto de sus vulnerabilidades, tanto técnicas como humanas, para reducir la superficie de exposición), **protección** (aplicando medidas de bloqueo, en diferentes puntos de la infraestructura, para impedir o limitar los ciberataques), **detección** (observando todo lo que ocurre en la organización, para buscar las amenazas existentes y casos de uso) y **respuesta** (actuando ante los ciberincidentes, para minimizar el impacto sobre la Organización). Así como la capacidad de **gestión de la seguridad**, estableciendo el rumbo del resto de capacidades, para desempeñar una correcta Gobernanza.

Los SOC deben destacar por su **proactividad**, ser capaces de detectar multitud de tipos de ataques, evitar su expansión, responder de forma rápida ante el incidente detectado y generar normas de actuación que eviten futuros incidentes. El almacenamiento de un número cada vez mayor de **eventos** proporcionará una panorámica completa y veraz de la situación de los sistemas de la Administración Pública española, que posibilitará una acción preventiva frente a las amenazas que sobre ellas se ciernen. Deben aplicar **casos de uso** para establecer qué registros son necesarios almacenar y ser tratados. Dichos registros deben ayudar y estar en consonancia para levantar alertas de seguridad y así ser eficientes. Y lo más importante, deben **intercambiar la información** sobre las amenazas y **notificar sus incidentes**, de manera que la inteligencia colectiva ayude a proteger a la sociedad en su conjunto.

En el ANEXO 1 se detallan las capacidades anteriormente mencionadas y los ámbitos de conocimiento de un SOC, así como las competencias que se han de desempeñar para cubrir dichas capacidades.

4.1 Puesta en marcha de un SOC

No todos los SOC tienen que disponer de los mismos servicios, cubriendo todas las capacidades y ámbitos, ni tener todas las competencias. Múltiples factores, a los que hay que añadir la madurez y los recursos disponibles obligarán a tomar una decisión en uno u otro sentido. La regla de entidad pequeña, SOC pequeño (o incluso no SOC, al estar cubierto por una entidad superior), entidad grande, SOC grande, debería ser la norma a seguir.

Los pasos a dar para poner en marcha un SOC con el apoyo del CCN-CERT serían los siguientes:

- **Evaluar los sistemas a proteger y estado de la seguridad**, para determinar la superficie de exposición del organismo. Para ello lo ideal es hacer una auditoría de los sistemas. Cuanto más completa sea la auditoría más información se tendrá de las vulnerabilidades y necesidades del organismo. En casos excepcionales, la auditoría podrá ser sustituida por entrevistas que proporcionen la información necesaria para la evaluación inicial. Los resultados de la auditoría se reasentarán en la herramienta ANA para favorecer el seguimiento de las vulnerabilidades detectadas y su corrección, además de obtener un inventario de sistemas para agilizar la notificación ante la aparición de nuevas vulnerabilidades. En otra faceta, la información obtenida sobre el estado de la seguridad del organismo se registrará en la herramienta INES para contribuir a la visión general del estado de la ciberseguridad a nivel nacional. Fruto de este trabajo inicial se podrá proporcionar al organismo una primera visión del estado de la seguridad del organismo, una primera aproximación de análisis de riesgos y un primer esbozo de plan de adecuación al ENS.
- **Definir objetivos de vigilancia.** En función del resultado de las auditorías y entrevistas se determinará qué se debe monitorizar y con qué tipo de herramientas.
- **Definir qué caso de uso aplica a la entidad** y que alertas pueden generar de valor.
- **Disponer de métricas de la superficie de exposición del organismo**. Para ello se deberán desplegar herramientas específicas. Esta información es muy importante para saber qué vulnerabilidades tiene el organismo, pudiendo determinar y priorizar los servicios y equipos que requieren de atención.
- **Apoyar el establecimiento de un EDR en todos los equipos de la organización** para tener una base defensa común y fuente de telemetría para el resto de servicios del SOC.
- **Dar formación** sobre la operación de un SOC.
- **Apoyar en la redacción de pliegos** para la contratación de servicios de ciberseguridad.

Las solicitudes de colaboración con el CCN para el despliegue de un SOC por parte de un organismo público se pueden realizar por correo electrónico, a la cuenta **socccn@ccn-cert.cni.es**. Si fuese necesario para el organismo solicitante, se podría llegar a firmar un convenio de colaboración. No obstante, teniendo en cuenta la multitud de organismos públicos existentes, esta opción quedará restringida a casos excepcionales.

4.2 Herramientas para SOC

Se recogen a continuación las herramientas más comúnmente usadas en ciberseguridad y qué tipo de SOC debería disponer de ellas.

Herramientas de Monitorización:

Son herramientas de distinto nivel de complejidad que sirven para que personal especializado pueda identificar eventos y alertas que requieren de atención.

- **Herramientas de administración de equipos de seguridad.**
  Entran en este grupo las herramientas de administración centralizada de cortafuegos (firewall), proxys, pasarelas, antispam, etc. Pueden estar a cualquier nivel de SOC, deseable al más bajo posible.

- **Antivirus (EPP) o Endpoint Detection and Response (EDR):**
  Es la primera línea de defensa y se instala en todos los dispositivos del organismo (ordenadores, servidores, teléfonos móviles, etc.). Debe ser atendida por el SOC de más bajo nivel. Además, es muy recomendable la instalación de la herramienta anti-ransomware del CCN-CERT, microCLAUDIA.

- **Sistema de detección de intrusiones (Intrusion Detection system-IDS) y Sistemas de Prevención de Intrusiones (Intrusion Prevention System-IPS).**
  Son sistemas que se usan para detectar o prevenir intrusiones. Normalmente van asociados a un sistema SIEM. Por su coste y complejidad solo está justificado su despliegue en accesos a internet de un elevado número de usuarios y sistemas, por lo que se deberá desplegar en SOC de nivel medio-Alto. Ejemplo: Sonda SAT-INET.

- **Sistema de gestión de eventos e información de seguridad (SIEM-Security Information Event Management).**
  Son sistemas complejos de instalar, gestionar y operar, que requieren de personal técnico muy especializado y cualificado. Por optimización de recursos se debe tender a usar en SOC de nivel alto-medio centralizando los eventos de SOC de nivel bajo, donde no sea viable por economía de recursos su despliegue. No tiene sentido escalar los eventos a varios SIEM ya que se duplicaría el trabajo. EL SIEM puede dar servicio a diversos organismos si así se agrupan en un SOC común. Finalmente, muy importante tener en cuenta que se corre el peligro de desbordamiento de logs de ese SIEM por lo que es muy importante el almacenamiento en base a casos de uso. Ejemplos: cualquier SIEM incluido en el catálogo CPSTIC 105.

- **Sistemas para la detección de amenazas persistentes avanzadas (APT-Advanced Persistent Threat):**
  Son herramientas muy sofisticadas que requieren de personal especializado y que se deben instalar en sistemas con información sensible. Solo son recomendables en entidades muy grandes, susceptibles de sufrir ataques esponsorizados por estados. Ejemplo CARMEN.

Herramientas de Auditoría:

Sirven para analizar las vulnerabilidades de los equipos y sistemas y ser consciente de la superficie de exposición. Ante cualquier nueva amenaza se puede saber qué sistemas y servicios se pueden ver afectados. Todos los organismos deberían realizar auditorías en el periodo previo a la implantación del SOC. Ejemplo: **ANA** como repositorio de resultados de auditorías.

Herramienta propia de gestión del SOC:

Herramienta de ticketing para las incidencias de los sistemas de seguridad del día a día.

Herramientas específicas de participación en la RNS:

- **Herramientas que permiten intercambiar información sobre amenazas y vulnerabilidades.** (MISP-Malware information Sharing Platform) Se plantean dos niveles distintos de información. Uno de nivel medio-bajo que debe estar en los SOC de nivel medio-bajo (MISP genérico), conteniendo indicadores de actividad anómala (IoA) e indicadores de compromiso (IoC). Y otra que solo estará a nivel alto-medio, REYES, por contener información más sensible, más centrada en indicadores de compromiso (IoC) e inteligencia sobre amenazas, para SOC de nivel Alto-Medio. Ambas herramientas se realimentarán entre ellas en la parte que se considere de interés.

- **Herramientas para la comunicación de Incidentes de Seguridad.** LUCIA para la comunicación y escalado de incidentes de ciberseguridad. Se empleará a todos los niveles. En última instancia el CCN-CERT podrá intervenir en la resolución del incidente.

4.3 Promover e Incentivar la implantación del ENS en los organismos públicos

El **Esquema Nacional de Seguridad** (RD 311/2022) es la norma base de obligado cumplimiento sobre la que se debe construir la ciberseguridad de cualquier organismo público. Cumpliendo con el ENS cada organismo, de forma aislada, podrá alcanzar un nivel adecuado de protección de la información y los servicios que presta a los ciudadanos.

El CCN ha desarrollado varias líneas de trabajo para facilitar la implantación del ENS, entre las que cabe destacar:

- Elaboración de 90 guías STIC (serie 800) para facilitar la implantación del ENS.
- Desarrollo de Herramientas para facilitar la implantación del ENS:
  - INES como asistente del plan de adecuación.
  - AMPARO como asistente de implantación y Gestión de la conformidad.
- Adaptación del ENS a determinados perfiles de cumplimiento, como las Entidades Locales. µCeENS.

La adecuación al ENS, que permite obtener la declaración/certificación de conformidad es un proceso ordenado que incluye las siguientes fases:

FASE 1	FASE 2	FASE 3
Plan de adecuación del sistema.	Implantación del plan de adecuación.	Conformidad.

Conseguir llegar hasta el final del proceso y conseguir la Conformidad es una obligación exigida por el RD 311/2022 del ENS para todos los organismos de la Administración Pública.

La puesta en marcha de un SOC debe servir también como un primer paso en la dirección de la aplicación del ENS. En este sentido, con la información y el trabajo inicial necesario para el despliegue del SOC se apoyará en lo posible al organismo para ponerlo en condiciones de poder llegar a cubrir la fase 1 de la implantación del ENS.

Dentro de la implantación del SOC se tendrá como objetivo secundario, en los organismos que aún no hayan superado la Fase 1 de implantación del ENS:

- **Dar de alta al organismo apoyado en INES, para colaborar con la visión general del estado de la seguridad en la Administración Pública.**
- **Facilitar un primer análisis de riesgos.**
- **Apoyar al organismo en la consecución de un plan de adecuación (Fase 1).**

4.4 Sinergias entre SOC (Modelo Federado)

Debido a la organización administrativa territorial en España, nos encontramos con una casuística muy variada que se verá afectada directamente por la madurez y por las capacidades de los servicios de ciberseguridad proporcionados por las entidades locales (EELL), Diputaciones/Cabildos/Consejos insulares (DIP) y Comunidades Autónomas (CCAA).

Se debe tener en cuenta el reparto de responsabilidades del modelo organizativo territorial y sus dependencias, ya que los recursos humanos y económicos van por distintas vías.

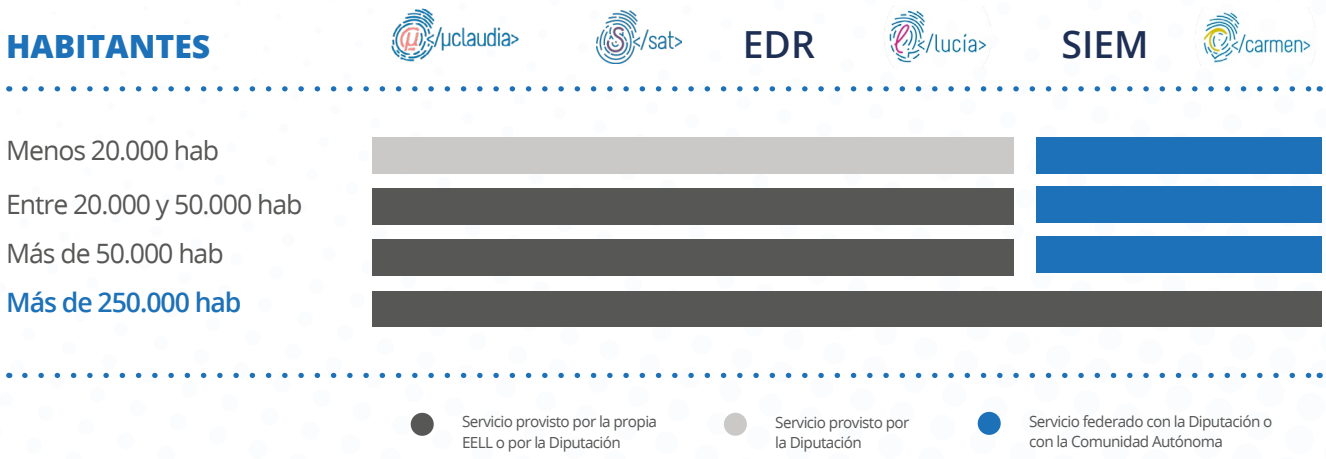
La transformación digital es un proceso largo y costoso que se va a extender durante muchos años. La ciberseguridad es algo novedoso que surge como consecuencia de la digitalización y para lo que las administraciones no estaban preparadas. Conseguir un adecuado nivel de ciberseguridad va a ser un reto constante en el tiempo que va a requerir grandes esfuerzos en recursos humanos y económicos. Por lo tanto, **es necesario pensar en un modelo que debe poder evolucionar a lo largo del tiempo en función de las necesidades y los recursos disponibles.**

Dado que la realidad nacional ya contempla un modelo de relación entre entidades y organismos basada en la federación (entidades locales, Diputaciones/Cabildos/Consejos insulares, Comunidades Autónomas y estado central), donde determinados servicios son provistos por entidades superiores en función de su tamaño y capacidad, **para la gestión de la ciberseguridad se propone seguir el mismo modelo de federación, de manera que los servicios de ciberseguridad se provisionen atendiendo al tamaño, capacidad y posición de la entidad.**

De esta manera, se pretende que no todas las entidades tengan que invertir la misma cantidad de dinero dedicado a la ciberseguridad, generando duplicidades en el gasto e infraestructura, sino que se hará atendiendo a los criterios anteriormente mencionados (tamaño, capacidad y posición de la entidad) siendo, en la mayoría de los casos y según las particularidades de la Administración, las Comunidades Autónomas las que harán la mayor inversión en ciberseguridad, posteriormente las Diputaciones/Cabildos/Consejos insulares, para finalizar por las entidades locales. Se consigue de esta forma mejorar la eficiencia de las inversiones.

Además de lo anterior, cuando se trata de invertir en un SOC se tiende a pensar en infraestructura tecnológica que cubra el parque tecnológico del organismo. Sin embargo, **el principal componente de un SOC son las personas encargadas de proporcionar la vigilancia constante de estos sistemas**, en la que se exige un nivel de conocimiento técnico muy específico. Así pues, los organismos públicos, además de las herramientas de seguridad que pueden adquirir con los fondos europeos, DEBEN contratar servicios de seguridad gestionada que deben ser asumidos por sus presupuestos ordinarios.

Teniendo en cuenta lo que se ha establecido en el punto anterior, los SOC de nivel medio y bajo deberían contar con los servicios que se recogen en la siguiente tabla en función del tipo de municipio:



En definitiva, mediante el modelo federado se pretende que el "escalón superior" asuma aquellos servicios que requieren más personal para atenderlo, al disponer de más presupuesto para su contratación.

05 RNS. VISIÓN DEL CCN-CERT.

El CCN-CERT tradicionalmente ha colaborado y colabora **en varios SOC de diferente magnitud**, ya sea a nivel de Ministerios, Diputaciones/Cabildos, o Entidades Locales, a los que se han venido a añadir últimamente Operadores de Servicios Esenciales. En esta dinámica **surgió la necesidad de crear una herramienta** que interconectara los SOC para que de manera fulminante se pudiera **cortar cualquier intento sospechoso de ciberataque**, incluso antes de determinar si consistía realmente en tal o no.

Posteriormente, a finales de 2020, la Comisión Europea lanzó su Estrategia de Ciberseguridad para la Década Digital, en la que adquiere un papel relevante una red europea de SOC, basada en herramientas de Inteligencia Artificial. La justificación de la Comisión viene de que **Europa había sufrido una pandemia de ransomware y la red de CSIRT existente a nivel europeo no había sido capaz de pararla**. Por tanto, se quería focalizar ahora la detección en los SOC.

Todo ello lleva al CCN-CERT a crear la **Red Nacional de SOC, plataforma que integra los SOC de todos los organismos públicos de la Administración**, junto con las entidades proveedoras que prestan dichos servicios de SOC y las entidades públicas que se benefician de los mismos.

Su objetivo principal es **impulsar la capacidad de protección** de sus miembros mediante el bloqueo casi inmediato de cualquier indicio de actividad anómala que se esté detectando en cualquier punto de la Administración.

5.1 Entidades participantes

A la Red Nacional de SOC podrán adherirse entidades de las siguientes categorías:

Entidades públicas: Organismos de la Administración Pública. Generalmente sus servicios de seguridad son prestados por proveedores contratados.

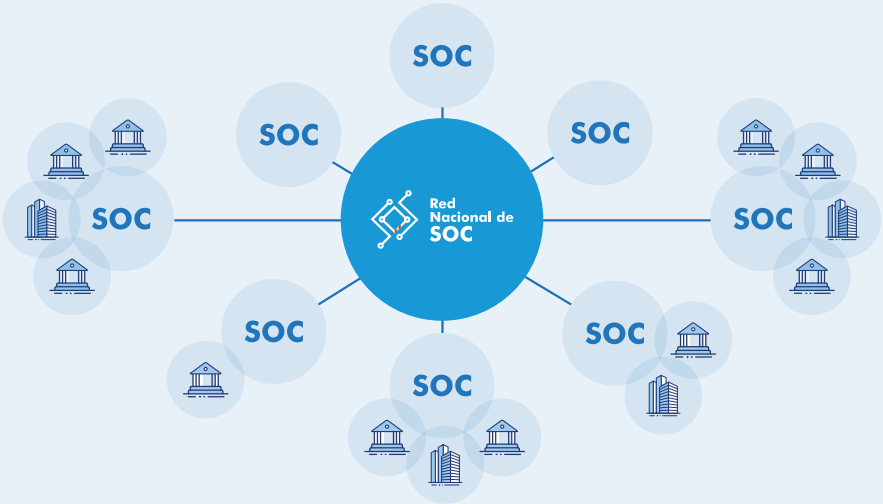
Entidades proveedoras (o simplemente "Proveedores"): Empresas que, con personal propio, prestan sus servicios de ciberseguridad o de SOC (Implementación, Operación, Mantenimiento...) a alguna entidad de la Administración Pública.

Entidades invitadas: Entidades que no cumplen los requisitos de las 2 anteriores categorías, pero a las que se quiere permitir el acceso a la información intercambiada en la RNS.

Las entidades públicas y los proveedores se relacionan entre sí por medio de los SOC, pudiéndose dar los siguientes escenarios:

SOC privado, perteneciente a un Proveedor, que presta servicio a una o varias AAPP. Su responsable será, por tanto, una persona de la empresa. Y el nombre estará relacionado con dicha empresa. Ej. SOC EmpresaA

SOC público, prestado por uno o varios Proveedores (o incluso con personal propio) y que cubre a una o varias AAPP. Su responsable será un empleado público. Y el nombre estará relacionado con la AAPP. Ej SOC MinisterioB



Además, actualmente las entidades proveedoras pueden tener los siguientes niveles (en base a su participación):

"Gold": Proveedores con un nivel alto de participación. Tendrán acceso inmediato a toda la información compartida y consolidada en la RNS.

"Informado": Proveedores con un nivel de participación normal. Tendrán acceso a la información compartida y consolidada en la RNS, pero con cierto retraso.

La participación se medirá a través de la información técnica compartida, que **será valorada y puntuada** en función de la naturaleza de la misma y su relevancia. Dado que se pretende utilizar la RNS como una herramienta que mejore la seguridad de la información de las Administraciones Públicas, desde estas mismas Administraciones se podrá impulsar progresivamente la adopción de esta categorización de "Gold" e "Informado" como valores diferenciadores a la hora de evaluar propuestas comerciales de proveedores que opten a contratos públicos

El listado actualizado de participantes se puede consultar en la página web de la RNS:

https://rns.ccn-cert.cni.es

5.2 Infraestructura tecnológica

La integración de la red se materializa mediante el uso de herramientas colaborativas, como la **mensajería** establecida en la red, tanto por parte de las entidades públicas que se benefician de los servicios del SOC como por parte de las empresas que prestan sus servicios en el mismo. Dicha solución se utiliza tanto para propagar alertas sobre incidentes en curso (o indicios de posibles incidentes), como para compartir otro tipo de información de interés: informes de ciberseguridad, procedimientos operativos de los SOC, procedimientos administrativos o de contratación de servicios....

Otra herramienta colaborativa es la de intercambio de información sobre amenazas **(MISP)** donde se podrán registrar tanto **Indicadores de Ataques (IOA)** como los **Indicadores de Compromiso (IOC)**. En modo lectura, para aquellas entidades públicas menos maduras que únicamente necesiten acceder en determinadas situaciones a los datos técnicos de una amenaza (por ejemplo, ante una alerta notificada a través de la solución de mensajería). O en modo integración, conectando directamente las propias herramientas de los SOC más maduros, de tal manera que se facilite la distribución de los indicadores a bloquear al resto de entidades. Esta herramienta alimentará de forma coordinada a REYES, que se usará al más alto nivel.

A corto plazo se integrará en la RNS el despliegue federado existente de la herramienta de notificación de **ciberincidentes LUCIA**, de modo que se pueda utilizar como un indicador más tanto del compromiso del SOC con el resto de miembros como de la evolución de los ciberincidentes en el territorio nacional.

Y a medio plazo se irán integrando en la RNS otras soluciones: **IRIS** para la visualización en tiempo real del **estado de la ciberseguridad** en la RNS; **ANA** para poder generar desde la RNS un sistema de aviso ante la publicación de **vulnerabilidades**; los **SIEM**, para recopilar aquellas alertas críticas generadas por los SOC y que puedan servir de fuente de datos para correlar incidentes desde una perspectiva global.

Todo ello centralizado en la **página web** de la Red Nacional de SOC, en donde desde su **área privada** se tendrá acceso a la información de pertenencia de la propia entidad. Y desde allí las entidades también podrán compartir entre sí información interesante como: casos de uso, ejemplos de pliegos, indicadores de servicio para SOC, procedimientos...

https://rns.ccn-cert.cni.es

5.3 Beneficios de participar

Para los proveedores con nivel "Gold", el principal beneficio es el **acceso a todos los IOC/IOA** compartidos en la RNS desde un inicio. De modo que pueda trasladar la protección ante dichas amenazas a sus clientes de manera **casi inmediata**. E, indirectamente, un mejor **posicionamiento** frente a los **procesos de contratación** en los que se haya especificado como requisito pertenecer a la Red Nacional de SOC con dicho nivel.

Para el resto de proveedores, los beneficios son los mismos aunque demorados ligeramente en el tiempo.

Y **para las entidades públicas**, no sólo el acceso a los indicadores anteriormente mencionados, sino a un **foro de compartición** en donde pondrán intercambiar recomendaciones respecto a la **gestión y dirección de los SOC**. Como pudieran ser modelos de contratación, recomendaciones sobre proveedores, definición de indicadores para la medición de los servicios...

5.4 Adhesión y permanencia

Los requisitos para que un organismo pueda adherirse a la Red Nacional de SOC como **entidad pública** son:

Pertenecer al Sector Público.
Disponer de servicios de ciberseguridad o de SOC.
Aceptar el código ético y de conducta profesional de la RNS.
Tener instalado y utilizar LUCIA (o estar en proceso de instalación).

Por su parte, **los requisitos** que han de cumplir las empresas para adherirse como **Proveedores** son:

Ser empresa (pública o privada).
Prestar servicios de ciberseguridad o de SOC al Sector Público.
Aceptar el código ético y de conducta profesional de la RNS.
Utilizar LUCIA para notificar incidentes al CCN-CERT en alguno de sus clientes (o estar en proceso de implantación).

Si se cumplen l**os requisitos** enumerados anteriormente, el proceso de adhesión consiste en:

- Solicitud por parte de la entidad: Rellenando el formulario de adhesión que se encuentra en la página web de la RNS, indicando si se es entidad pública o proveedor.
- Aprovisionamiento, por parte de la RNS, en las herramientas disponibles. Y notificación a la entidad de las credenciales correspondientes.
- Confirmación de la adhesión y publicación de la membresía en la web.

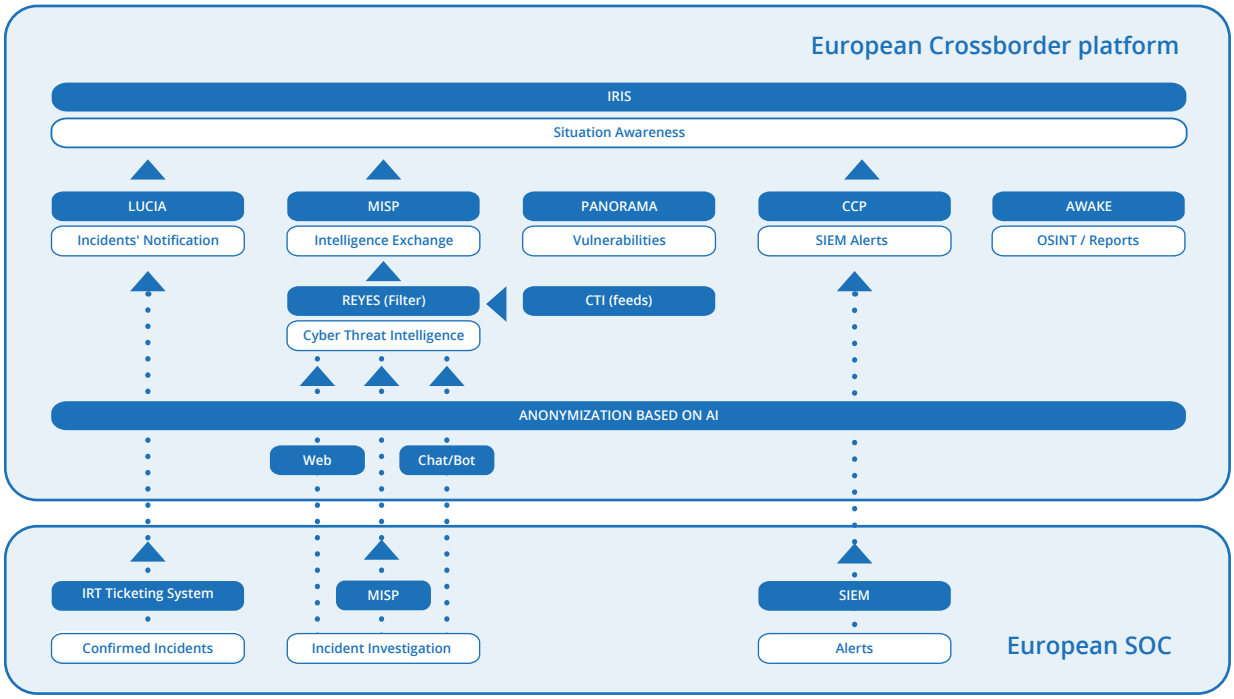
Una vez adheridas a la Red Nacional de SOC, las entidades han de cumplir las siguientes **condiciones de permanencia**, que serán revisadas de manera trimestral:

- **Seguir cumpliendo los requisitos de adhesión.**
- **Utilizar las herramientas a disposición de la RNS: acceder de manera continua a la solución de mensajería y estar al corriente de la información intercambiada; acceder puntualmente a la solución de intercambio para tener la capacidad de descargar la información técnica intercambiada; ...**
- **Adicionalmente, para las entidades proveedoras, compartir información técnica que sea novedosa y relevante. Por medio de las herramientas a disposición de la RNS, para que dicha información pueda ser valorada y puntuada correctamente.**

5.5 Desarrollo de la red de SOC europea. ENSOC

Para el desarrollo de un escudo europeo para el ciberespacio común de los países de la UE, la RNS trabajará y apoyará el desarrollo de proyectos conjuntos con otros países de forma que se amplíe la colaboración y el intercambio de información.

La RNS compartirá experiencias y propondrá el uso de las herramientas disponibles para colaborar con la defensa del ciberespacio común europeo, apoyando al sector español de ciberseguridad.



06 PLATAFORMA NACIONAL

Fruto de la trasposición de la Directiva NIS (Directiva de Seguridad de los Sistemas de Información) a la legislación nacional, en donde se obligaba a los Estados Miembros a que aplicaran una serie de medidas de coordinación a nivel interno entre los actores en ciberseguridad, nace la creación de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

El CCN-CERT según dispone el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en colaboración con el INCIBE-CERT y el ESPDEF-CERT del Mando Conjunto del Ciberespacio pondrá a disposición de todos los actores involucrados la citada Plataforma Nacional.

La plataforma permitirá el intercambio de información y el seguimiento de incidentes entre los operadores de servicios esenciales o proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia de manera segura y confiable, sin perjuicio de los requisitos específicos que apliquen en materia de protección de datos de carácter personal. Además, como se ha mencionado anteriormente, esta plataforma será el espacio de coordinación de todos los SOC pertenecientes a la Red Nacional de SOC.

Esta plataforma deberá garantizar asimismo la disponibilidad, autenticidad, integridad y confidencialidad de la información, así como podrá emplearse también para dar cumplimiento a la exigencia de notificación derivada de regulaciones sectoriales, de acuerdo con el artículo 19.5 del Real Decreto-ley 12/2018, de 7 de septiembre.

Asimismo, la plataforma implementará el procedimiento de notificación y gestión de incidentes, que estará disponible durante todas las horas del día y todos los días del año, y dispondrá como mínimo de las siguientes capacidades:

- Capacidad de gestión de ciberincidentes, con incorporación de taxonomía, criticidad y notificaciones a terceros, según lo establecido en el anexo.
- Capacidad de intercambio de información sobre ciberamenazas.
- Capacidad de análisis de muestras.
- Capacidad de registro y notificación de vulnerabilidades.
- Capacidad de comunicaciones seguras entre los actores involucrados en diferentes formatos y plataformas.
- Capacidad de intercambio masivo de datos.
- Generación de estadísticas e informes agregados.

ANEXO I: CENTROS DE OPERACIONES DE CIBERSEGURIDAD (SOC).

1 Capacidades y ámbitos de conocimiento

El SOC proporciona al Organismo las capacidades de:

PREVENCIÓN, ampliando el conocimiento respecto de sus vulnerabilidades, tanto técnicas como humanas, para reducir la superficie de exposición.

PROTECCIÓN, aplicando medidas de bloqueo, en diferentes puntos de la infraestructura, para impedir o limitar los ciberataques.

DETECCIÓN, observando todo lo que ocurre en la organización, para buscar las amenazas existentes.

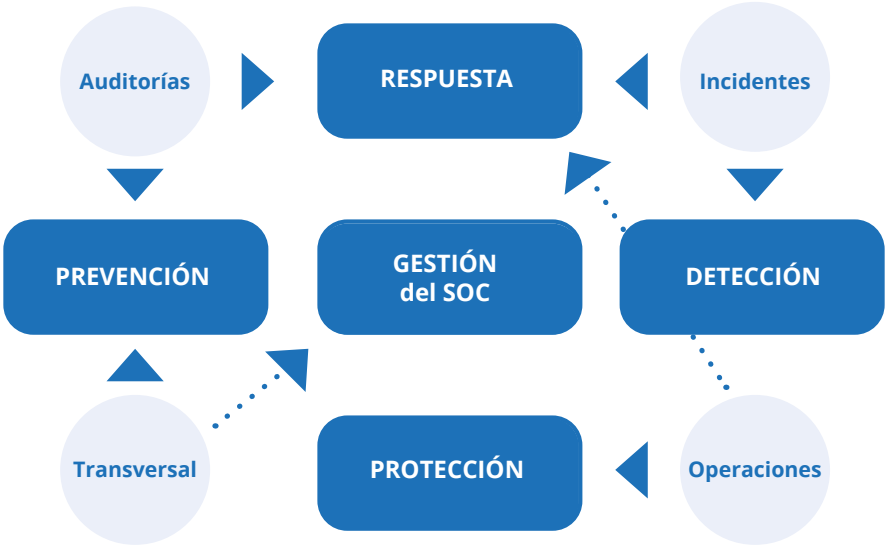
RESPUESTA, actuando ante los ciberincidentes, para minimizar el impacto sobre la Organización.

Así como la capacidad de **GESTIÓN DE LA SEGURIDAD,** estableciendo el rumbo del resto de capacidades, para desempeñar una correcta Gobernanza.

Desde el CCN se entiende que el alcance del SOC dependerá del Organismo al que presta servicio, pudiéndose encontrar casos en los cuáles el SOC sólo proporciona un subconjunto de estas capacidades.

Por otro lado, y en función del conocimiento o experiencia de las personas que forman parte del SOC, sus actuaciones se pueden clasificar en los siguientes ámbitos:

- Ámbito de las **OPERACIONES**: en donde se pone foco en las actuaciones que requieren conocimientos respecto de la tecnología de seguridad implantada en el Organismo, para su explotación.
- Ámbito de los **INCIDENTES**: en donde se pone foco en las actuaciones que requieren conocimientos respecto de los actores y amenazas existente; sus tácticas, técnicas y procedimientos (TTP); así como en el proceso completo de la gestión de un incidente.
- Ámbito de las **AUDITORÍAS**: en donde se pone foco en las actuaciones que requieren conocimientos respecto de las vulnerabilidades, para su análisis y posterior mitigación.
- Ámbito **TRANSVERSAL**: en donde se agrupan aquellas actuaciones que no requieren de un conocimiento propio en un ámbito en concreto.



Relación entre los ámbitos de conocimiento que participan en cada capacidad.

Estos ámbitos pueden ayudar, sobre todo al principio, a estructurar los equipos de trabajo del SOC. De modo que se pueda empezar con tres equipos de trabajo diferenciados (Operaciones, Incidentes y Auditorías), aunque posteriormente y según vaya creciendo el SOC se vayan estructurando más por competencias.

2 Competencias

Para alcanzar las capacidades anteriormente identificadas, el SOC ha de desarrollar una serie de competencias que, posteriormente y en función del catálogo de servicios del Organismo, podrán formar parte un servicio específico o estar agrupadas bajo un servicio de nivel superior.

2.1 De prevención

- Inspecciones Técnicas de Seguridad: las cuales podrán llevarse a cabo sobre la infraestructura en producción, y/o de manera previa integrada en el ciclo de vida del desarrollo del software, y/o en la puesta en marcha de nuevas infraestructuras (adquisiciones de impresoras, proyectores, termostatos...); podrán ser de "caja negra", "caja blanca" o "caja gris"; podrán ser de código fuente (sin ejecutar) o de código en ejecución; ...
- Análisis de vulnerabilidades automatizados.
- Seguimiento a la publicación de vulnerabilidades tecnológicas que pudieran afectar al Organismo.
- Gestión de vulnerabilidades: que podrá ser llevado a cabo con herramientas específicas (e.g. ANA), y que incluiría tanto el registro y seguimiento de las vulnerabilidades identificadas como el apoyo a la remediación de dichas vulnerabilidades.
- Capacitación, del personal del Organismo, en técnicas de seguridad.
- Concienciación, del personal del Organismo, respecto de los riesgos existentes.
- Cibervigilancia o Vigilancia Digital, tanto en Internet como en la darkweb.

2.2 De protección

- Protección del tráfico, ya sea perimetral o interno, mediante la gestión de cortafuegos, de los sistemas de detección y/o prevención de intrusiones...
- Protección de la navegación, mediante la gestión de los "proxies", "sinkholes" (DNS),...
- Protección del correo, mediante la gestión de los sistemas "antispam".
- Protección de las aplicaciones web, mediante la gestión del WAF o la inspección TLS.
- Protección del acceso remoto, mediante la gestión de las VPN o del acceso a los escritorios virtuales (VDI).
- Protección de los puestos de trabajo y servidores ("endpoints"), mediante la gestión de las soluciones antivirus, EPP, EDR...
- Protección de la fuga de documentación, mediante la gestión de las soluciones DLP, IRM...

2.3 De detección

- Registro de eventos o “logs”, mediante servidores centralizados.
- Correlación de eventos, mediante sistemas SIEM. Con la posibilidad de generar reglas de detección de manera proactiva.
- Monitorización de alertas, procedentes de múltiples orígenes como el EDR, SAT, SIEM, AntiDDoS de CORA...
- Investigaciones avanzadas o “Threat hunting”, mediante soluciones como CARMEN, CLAUDIA, los EDR... y haciendo uso de informaciones compartidas como IoC o TTP (Mitre ATT&CK).

2.4 De respuesta

- Bloqueo centralizado de IoC.
- Gestión de incidentes, incluyendo la gestión de evidencias, el análisis forense, la contención, mitigación y recuperación.
- Análisis de código dañino o “malware”, también denominado “reversing”, con laboratorios o soluciones como ADA.
- Intercambio de información mediante MISP, REYES, RNS...
- Análisis y confirmación de vulnerabilidades bajo ataque.

2.5 De gestión

- Asesoramiento.
- Implantación del ENS.
- Desarrollo normativo.
- Análisis de Riesgos.
- Cumplimiento legal y normativo.
- Información del Estado de la Seguridad (Cuadros de mando).

2.6 Cuadro resumen

	Operaciones	Incidentes	Auditorías	Transversal
PREVENCIÓN			• ITS • Análisis automáticos • Seguimiento público • Gestión vuln. (ANA)	
	• Capacitación	• Concienciación	• Cibervigilancia	
DETECCIÓN		• Registro de logs • Correlación (SIEM) • Monit. alertas • Threat Hunting		
PROTECCIÓN	• De tráfico (FW, IDS) • De nav. (Proxy, DNS) • De correo • De apps web (WAF) • De acceso remoto • Del endpoint • De fugas (DLP, IRM)			
RESPUESTA	• Bloqueo de IOC	• Gestión de Inc. • Análisis de malware • Intercambio (MISP, REYES)	• Confirmación de vuln	
GESTIÓN	• Asesoramiento • Implantación ENS	• Desarrollo normativo • Análisis de Riesgos	• Cumplimiento legal • Cuadros de mando	

ANEXO II: BASE LEGAL EN LA CREACIÓN DE LA RNS

El primer problema que tuvo que afrontar la RNS fue la poca predisposición de muchos actores implicados, tanto organismos públicos como proveedores de ciberseguridad gestionada, a compartir información sobre posibles ciberataques. En cierto modo, preservando los ciberataques sufridos se preserva la identidad del organismo, así como las consecuencias que pudiera tener en cuanto a crédito, prestigio, consecuencias legales...

La legislación vigente avala perfectamente la creación de esta RNS por parte del CCN: según el RD 311/2022, de 4 de mayo de 2022, Artículo 34, Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público, el CCN-CERT prestará los siguientes servicios:

- **Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las entidades del ámbito de aplicación de este real decreto. Para su cumplimiento se podrán recabar informes, registros de auditoría y configuraciones de los sistemas afectados y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la normativa de protección de datos que resulte de aplicación, así como de la posible confidencialidad de datos de carácter institucional u organizativo.**

- **Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.**

Todo ello ha motivado y justificado la creación del este escudo unificado que es la Red Nacional de SOC para intercambio de información ágil y en tiempo oportuno.

Red Nacional de SOC

Liderado por CCN-CERT

socccn@ccn-cert.cni.es
https://rns.ccn-cert.cni.es