Red Nacional de SOC

RED NACIONAL DE SOC

150 ENTIDADES PÚBLICAS Y PRIVADAS

30 ALERTAS DIARIAS SOBRE CIBERAMENAZAS

Liderada y coordinada por el Centro Criptológico Nacional, a través de esta iniciativa pionera a nivel nacional e internacional, sus más de 150 miembros disponen de acceso en tiempo real a información sobre ciberamenazas que permite la detección de posibles incidentes de ciberseguridad.

SHARE BEFORE HACKED

Hace ahora dos años, en octubre de 2021, el **Centro Criptológico Nacional** puso en marcha la **Red Nacional de Centros de Operaciones de Ciberseguridad (RNS)**. Nacía como respuesta a la necesidad de coordinar los diferentes SOC desplegados en las distintas administraciones públicas, muchos de ellos en colaboración con el propio CCN (en ministerios, diputaciones, comunidades autónomas, cabildos o entidades locales) y, sobre todo, ante la constatación del cambio de paradigma que han supuesto los acelerados procesos de transformación digital.

Desde el CCN se constató que la respuesta y protección individual dejaron de ser suficientes en un escenario en el que la superficie de exposición y las ciberamenazas crecían de forma exponencial. Era, por tanto, preciso sustituir el modelo reactivo por uno de defensa activa para conseguir una mejor protección del sector público español. Y para ello, era indispensable avanzar de la notificación individual del incidente al intercambio de esta información, compartiendo entre las distintas entidades los detalles necesarios para lograr ventajas competitivas frente al atacante.

Este objetivo coincidía además con las prioridades de la Comisión Europea que, en diciembre de 2020, daba a conocer la **Estrategia de Ciberseguridad de la Unión Europea** para la Década Digital. En ella se apostaba abiertamente por la creación de "una red de centros de operaciones de seguridad en toda la UE y la mejora de los centros existentes y el establecimiento de otros nuevos".

En este sentido, conviene señalar que España, junto con Italia, Luxemburgo, Portugal y Rumanía, han formado un consorcio para el desarrollo de una red europea de SOC que permita promover el intercambio de información entre estos cinco países.

En esta situación, el CCN-CERT decidió liderar la puesta en marcha de la **Red Nacional de SOC** para dar respuesta a este nuevo ecosistema de la ciberseguridad en el que es determinante promover la notificación colectiva de ciberamenazas para prevenir su materialización y evitar que se repliquen determinados ciberataques. Así lo asegura Carlos Córdoba, jefe del Área de Centros de Operaciones de Ciberseguridad del Centro Criptológico Nacional, quien además señala que *"si entre todos los SOC que dan protección al sector público compartimos información sobre las tácticas, técnicas y procedimientos de nuevas amenazas, se mejorarán las capacidades de detección y respuesta a posibles ciberincidentes"*.

En octubre de 2021, el Centro Criptológico Nacional puso en marcha la Red Nacional de Centros de Operaciones de Ciberseguridad (RNS). Nacía como respuesta a la necesidad de coordinar los diferentes SOC desplegados en las distintas administraciones públicas.

Estado actual de la RNS

Tras la prueba piloto iniciada en 2021, durante el año 2022 la Red Nacional de SOC evolucionó hasta alcanzar las **150 entidades adheridas en la actualidad**, entre SOC públicos y los pertenecientes a las empresas que les prestan servicios. Ministerios, diputaciones, cabildos, entidades locales, y operadores de servicios esenciales forman parte de esta plataforma de intercambio de información sobre ciberamenazas, mediante la que se comparten **de media diaria alertas de más de 30 incidentes de ciberseguridad**.

El principal activo de la Red Nacional de SOC es la información que se comparte sobre indicadores de ataque **(IOA)** y de compromiso **(IOC)** no identificados dentro de la comunidad para alertar y promover las acciones preventivas necesarias. Actualmente, los miembros de la RNS comparten información de distinto tipo:

Direcciones IP de atacantes

Firmas o **Hashes** de ficheros con contenido dañino

Direcciones de correo propagadoras de contenido dañino

Dominios de sitios comprometidos

URL específicas con contenido dañino

Reglas de detección de amenazas IoC

Es importante destacar que a través de la Red Nacional de SOC no se comparte información que pueda contener datos de víctimas de posibles ataques. Tampoco se intercambian informes o investigaciones genéricas sobre amenazas en el ciberespacio si éstas no se están materializando o no han sido detectadas por los miembros de la RNS.

¿Quién forma parte de la RNS?

Desde que entró en funcionamiento, la Red Nacional de SOC ha sido reconocida por su excelente labor. En la comunidad, ya es considerado el principal **instrumento para coordinar la colaboración y el intercambio de información** entre los Centros de Operaciones de Ciberseguridad del sector público español.

A día de hoy, son miembros de la RNS los SOC de los organismos de la Administración Pública española, las entidades proveedoras y privadas que con personal propio prestan sus servicios de ciberseguridad a entidades públicas (en este caso con distintos niveles de participación); y entidades invitadas a las que, sin cumplir alguno de los dos requisitos anteriores, se les da acceso a la información intercambiada en la propia Red; pero como explicaremos más adelante, esta composición evolucionará próximamente.

Para que un organismo pueda ser admitido en la Red Nacional de SOC como entidad pública, debe cumplir cuatro requisitos:

1. **Pertenecer al sector público español.**
2. **Disponer de servicios de ciberseguridad o de SOC.**
3. **Aceptar el código ético y de conducta profesional de la RNS.**
4. **Tener instalada y utilizar la herramienta LUCIA (o en proceso de instalación).**

Por su parte, las empresas que desean adherirse como Proveedores deben hacerlo en calidad de "empresa" (pública o privada), y para formar parte de la RNS han de cumplir con las siguientes premisas:

1. **Prestar servicios de ciberseguridad o de SOC al sector público.**
2. **Aceptar el código ético y de conducta profesional.**
3. **Utilizar LUCIA para notificar incidentes al CCN-CERT en nombre de alguno de sus clientes (o estar en proceso de implantación).**

Para garantizar su calidad, la información técnica compartida por los miembros de la RNS está sometida a un **proceso de valoración continuo** en el que se evalúa la naturaleza y relevancia de las aportaciones realizadas por cada miembro puesto que el nivel de implicación de los miembros de la RNS es determinante a la hora de permanecer en la Red. Por otra parte, el **parámetro de calidad** también interviene en la evaluación de la información intercambiada. Desde su puesta en marcha, la RNS ha recibido **más de 5.000 eventos de ciberseguridad**; sin embargo, alrededor de un 20% fueron descartados por no cumplir las condiciones para ser compartidos por el resto de los miembros.

Además, con el objetivo de fomentar la **participación y el intercambio**, la RNS dispone de un mecanismo, dirigido exclusivamente a las entidades proveedoras, que puntúa la colaboración y posiciona a los miembros en dos niveles en función de su actividad dentro de la Red ("**Gold**" e "**Informado**").

*Desde su puesta en marcha, la RNS ha recibido más de **5.000 eventos** de ciberseguridad.*

Próximas mejoras de la RNS

Si bien el objetivo de la Red Nacional de SOC continuará siendo la ampliación de las capacidades de protección frente a ciberamenazas a través del intercambio de información, el Centro Criptológico Nacional tiene trazadas las líneas principales para mejorar la efectividad de la información compartida a través de esta red de nodos de centros de operaciones de ciberseguridad.

Como punto de partida, está previsto integrar en esta Red Nacional no solo a los SOC de los organismos de la Administración Pública española, sino a **todos aquellos que operan en España**. La participación en la Red se hará extensiva **también** a **otras comunidades y foros** de intercambio de información **nacionales**, como CSIRT.es, **o internacionales**, como la Red Europea de SOC (ENSOC).

En paralelo a esta expansión, desde el CCN se están definiendo **pautas concretas para enriquecer la información compartida** con el objetivo de lograr un intercambio de datos más eficaz. Por ello, está previsto incluir en el intercambio información de contexto (fuentes externas) y mejorar los criterios de caducidad de la información compartida, descartando falsos positivos y haciendo uso de los protocolos de compartición PAP/TLP. También está previsto ampliar de manera procedimentada la tipología de la información a compartir e incluir casos de uso para detección, métricas de SOC, o buenas prácticas de gestión.

Asimismo, se está trabajando en el establecimiento de **nuevos criterios de puntuación**, que midan y evalúen la naturaleza del incidente compartido y **que penalicen los falsos positivos**. En este sentido, y como novedad, la clasificación por niveles se hará extensible a todas las entidades privadas, en base a la puntuación recibida por su información compartida, y se añadirá un nivel "Inhabilitado" cuando no exista registro de actividad. Se cambiará también el nombre de los actuales niveles a "Oro" (en lugar de "Gold") y "Plata" (en lugar de "Informado").

A corto plazo, la RNS medirá la eficacia de la información cuando se produzcan los bloqueos de los indicadores compartidos y se proporcionarán **nuevas capacidades** a los miembros a partir de la información global recibida:

Prevención: mediante notificación de vulnerabilidades.

Detección: mediante correlación de alertas.

Gestión: mediante cuadros de mando centralizados.

Entre todos los SOC integrados en esta Red y a través del intercambio y la participación colectiva de sus miembros, se logrará una mejora sustancial de las capacidades nacionales de prevención, detección y respuesta a ciberamenazas.

Mejoras de la RNS

Integrantes

Información compartida

Capacidades

RED NACIONAL DE SOC

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

centro criptológico nacional

centro criptológico nacional