Red Nacional de SOC

Condiciones de adhesión y permanencia

Red Nacional de SOC

Índice

Abreviaturas

AGE	Administración General del Estado
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
IP	Internet Protocol
MISP	Malware Information Sharing Platform
PSSG	Proveedor de Servicios de Seguridad Gestionada
RNS	Red Nacional de SOC
SOC	Security Operations Center (Centro de Operaciones de Seguridad)
TTP	Tácticas, Técnicas y Procedimientos
URL	Uniform Resource Locator

Introducción

La Red Nacional de SOC (RNS), tal y como se describe en el documento específico "***¿Qué es la Red Nacional de SOC?***", es una red que integra los SOC de todos los organismos públicos de la Administración. Estos SOC podrán estar operados por personal propio de la Administración o por proveedores externos de servicios de seguridad gestionada (PSSG).

La Red Nacional de SOC (RNS) es una red que integra los SOC de todos los organismos públicos de la Administración.

Objetivo del documento

El objetivo del presente documento es describir el procedimiento de adhesión a la Red Nacional de SOC, sus requisitos de permanencia, condiciones de exclusión y proceso de valoración de la información.

Si bien este documento es de especial interés para aquellos PSSG que operen en la actualidad un SOC de un organismo público, es relevante también para todo el personal público responsable de cada SOC por parte de la Administración.

Relación entre entidades y categoría de los usuarios

Relación entre entidades

Para entender adecuadamente el proceso de adhesión a la RNS, se hace necesario identificar las distintas entidades y sus responsabilidades en el contexto de la RNS:

Organismo>

Entidad pública dentro de la Administración General del Estado.

PSSG>

Entidad privada que presta servicios de seguridad gestionada a un organismo público a través de un SOC.

SOC>

Centro de operaciones de ciberseguridad que da servicios de ciberseguridad al organismo público.

Responsable del SOC desde el punto de vista del organismo>

Persona responsable de la operación del SOC por parte del organismo público.

Responsable del SOC desde el punto de vista del PSSG>

Personal responsable de la operación del SOC por parte del PSSG, en caso de que los servicios del SOC sean prestados por un PSSG y no por personal del organismo público.

Categoría de los usuarios

Los usuarios dentro de la RNS se categorizan en:

Entidades públicas>

Cualquier responsable de SOC de la parte del organismo. Tendrá acceso a toda la información del MISP.

Usuarios con categoría “Gold" >

Responsables de SOC de la parte del PSSG. Tendrán acceso a toda la información del MISP.

Usuarios con categoría “Informado”>

Responsables de SOC de la parte del PSSG. Tendrán acceso a información limitada del MISP.

Beneficios de la categoría “Gold” frente a “Informado”

Información en tiempo real

La información que sea reportada será inmediatamente insertada en el MISP y compartida con todos los usuarios con categoría “Gold”. Es decir, todos estos usuarios tendrán acceso de manera inmediata a posibles amenazas detectadas por otros participantes de la RNS, lo que les permitirá adoptar medidas de prevención o contención con tiempo de antelación.

Una vez esta información sea valorada por el CCN y aprobada para su distribución, será compartida con el resto de participantes con categoría “Informado” de la RNS, lo que implicará que estos usuarios tendrán menos tiempo de reacción desde la publicación de la información hasta la adopción de medidas.

Diferenciación en contratos públicos

Dado que se pretende utilizar la RNS como una herramienta que mejore la seguridad de la información de las Administraciones Públicas nacionales, desde estas mismas Administraciones se impulsará progresivamente la adopción de esta categorización de “Gold” e “Informado” como valores diferenciadores a la hora de evaluar propuestas comerciales de PSSG que opten a contratos con las Administraciones Públicas.

Gold

Informado

Proceso de adhesión a la RNS

El proceso de adhesión de un SOC a la RNS contempla los siguientes pasos:

Adhesión del SOC a la RNS

- ✓ El responsable del SOC desde el punto de vista del organismo público solicita al CCN su adhesión a la RNS. Para ello, el SOC debe cumplir los requisitos descritos en el apartado "Requisitos de adhesión a la RNS".
- ✓ El CCN dará de alta el SOC en la RNS, teniendo el responsable del SOC desde el punto de vista del organismo, acceso a toda la información del MISP.

Adhesión del PSSG de servicios de ciberseguridad a la RNS

- ✓ El responsable del SOC desde el punto de vista del PSSG solicitará el registro de su entidad a la RNS.
- ✓ El CCN confirmará el registro del usuario y su adhesión a la RNS con categoría de Informado. El PSSG podrá alcanzar la categoría de Gold en función de la información que comparta.

Requisitos de adhesión a la RNS

Requisitos de adhesión del SOC de la entidad pública a la RNS

Son requisitos de adhesión a la RNS los siguientes:

Ser institución pública con sede española.

Presentación de los servicios SOC.

- ✓ Motivación por pertenecer a la RNS.

Cumplimentar formulario de ingreso, Anexo 2 de este documento.

- ✓ Razones de participación, valor añadido, representante, etc.

Tener instalado LUCÍA y utilizarlo para compartir la información relativa a incidentes ya materializados.

Aceptación del código ético y de conducta profesional de la RNS.

Requisitos de adhesión del PSSG a la RNS

Son requisitos de adhesión a la RNS los siguientes:

Ser empresa (pública o privada) que preste servicios de ciberseguridad a la Administración Pública.

Presentación del PSSG:

- ✓ Motivación por pertenecer a la RNS.
- ✓ Beneficios de la participación del nominado para la RNS.

Cumplimentar formulario de ingreso, Anexo 2 de este documento.

- ✓ Razones de participación, valor añadido, representante, etc.

Autorización de los clientes implicados para compartir información no confidencial, Anexo 3 de este documento.

Compromiso de compartir información en los términos definidos en el Anexo 4.

Tener instalado LUCÍA y utilizarlo para compartir la información relativa a incidentes ya materializados.

Aceptación del código ético y de conducta profesional de la RNS.

Valoración positiva por parte del CCN.

Condiciones de permanencia del PSSG de servicios en la RNS

Las condiciones de permanencia del PSSG en la RNS, descritas a continuación, se revisarán cada 3 meses, proponiéndose su exclusión, mantenimiento en categoría o evolución de las mismas:

- Dar soporte al resto de miembros en caso de que algún otro miembro de la RNS requiera ayuda.
- Aportación en trabajos en común (por ejemplo, la colaboración en la creación de herramientas y procedimientos).
- Aportar información valiosa para la RNS:
  - ✓ La información se valora en función de los parámetros expuestos en el Anexo 1 de este documento.
  - ✓ La información que debe compartirse en la RNS se detalla en el Anexo 4.
- Compartir toda la información relativa a incidentes ya materializados a través de LUCÍA.
- Participar en las decisiones de la RNS.
- Asistir a todas las reuniones de la RNS.
- Mantener una calificación mínima “Informado” derivada de la calidad y cantidad de información compartida.
- Cálculo cuantitativo mediante fórmula explicada a continuación.
- En cada periodo se actualizan los pesos de los SOC.
- Cumplir con el principio de legalidad.

Condiciones de exclusión de la RNS

Las condiciones de exclusión del PSSG de servicios de ciberseguridad de la RNS son las siguientes:

- Incumplimiento de las condiciones de permanencia durante 3 periodos.
- Incumplimiento del código de conducta.
- A propuesta de cualquiera de los miembros, refrendada por dos tercios de los miembros.
- El CCN se reserva el derecho de expulsión.

Anexo 1: Método de valoración

Valoración de la tipología de la información en función de su relevancia

La información reportada será valorará por el CCN en función de su categoría, según la siguiente tabla:

Categoría	Valoración
IPs sospechosas	1 punto
Grupos de IPs, URL, dominio, hash, etc.	2 puntos
Reglas Yara, snort, sigma básicas, etc.	3 puntos
TTP, etc.	5 puntos

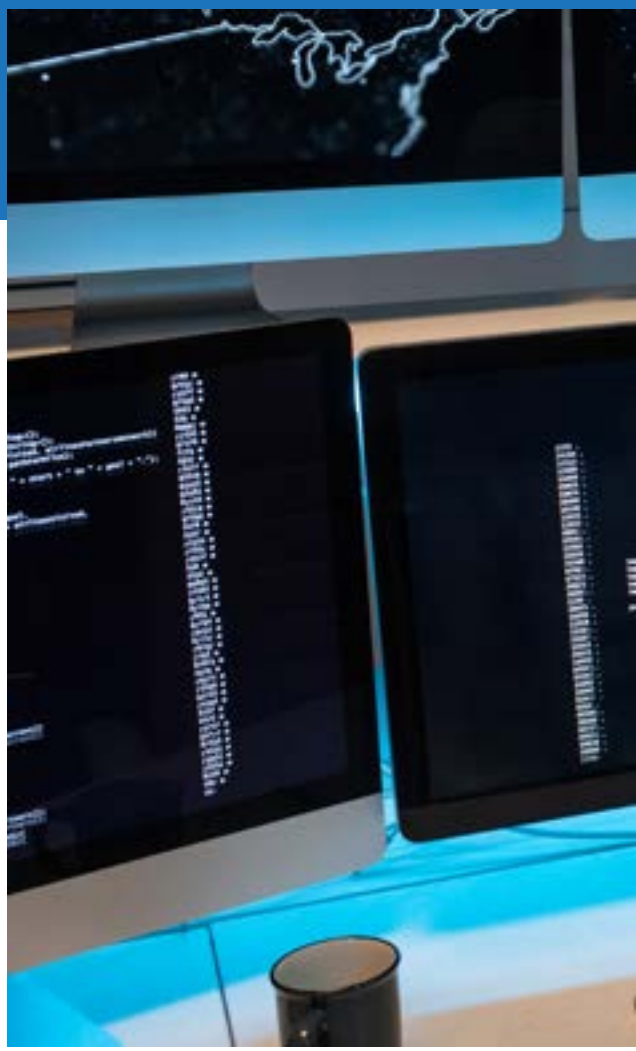
Participación del resto de SOC: valoración del aporte

Una vez la información ha sido publicada en la RNS con su valoración inicial, cada SOC valora la información aportada por cada participante en función de la calidad y utilidad de la misma. Esta valoración estará expresada como “muy útil” o “poco útil” por parte de la Red, y podrán darse los siguientes escenarios:

En caso de que la información aportada sea valorada como “muy útil” por, como mínimo, dos componentes de la RNS más que como “poco útil”, se incrementará la valoración de la información en +2 puntos.

En caso de que la información aportada sea valorada como “poco útil” por, como mínimo, dos componentes de la RNS más que como “muy útil”, se decrementará la valoración de la información en -2 puntos.

En cualquier otro escenario, la información mantendrá la valoración inicial según su categoría.



Valoración del PSSG de servicios de ciberseguridad

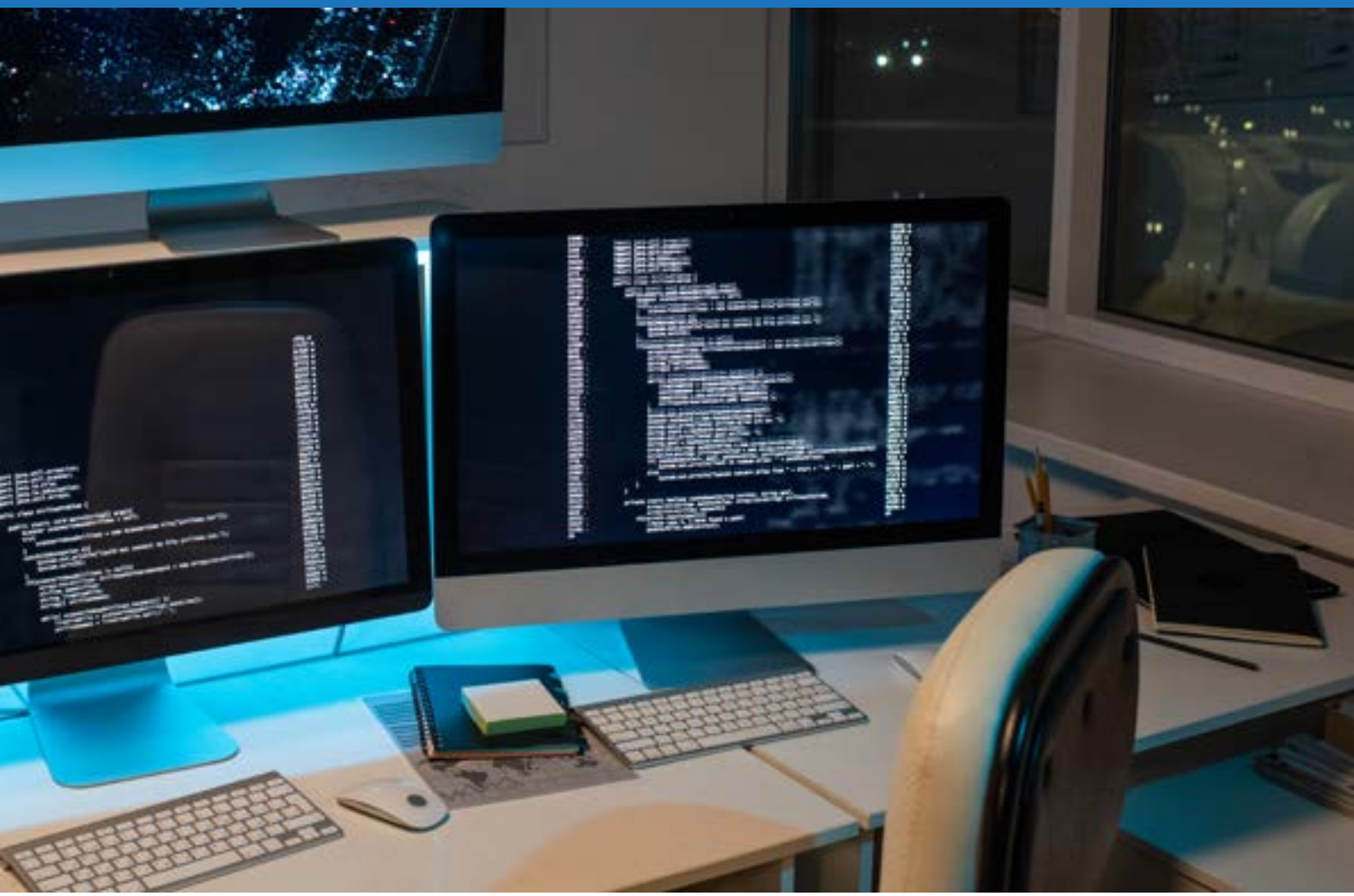
Cada PSSG será dado de alta, por defecto, en la categoría de "Informado". Cada PSSG alcanzará la categoría máxima "Gold" una vez logre acumular 15 puntos. Una vez alcanzada la categoría "Gold", se mantendrá en ella acumulando, al menos, 5 puntos al mes. Si no lo alcanzase, rebajará su categoría a "Informado" y comenzará el proceso de nuevo.

En caso de que el PSSG no acumule ningún punto durante el periodo de revisión (3 meses), el CCN valorará la expulsión del PSSG de la RNS.

Periodos de revisión de categoría del PSSG de servicios de ciberseguridad

Se establece un periodo de 3 meses para la revisión de la categoría de cada uno de los PSSG dados de alta en la RNS, pudiéndose dar los siguientes escenarios:

El PSSG se encontraba en la categoría de "Informado" y durante el periodo de 3 meses previo ha logrado acumular, al menos, 15 puntos: el PSSG pasará a la categoría "Gold".



- El PSSG se encontraba en la categoría de “Informado” y durante el periodo de 3 meses previo ha acumulado más de 0 puntos, pero menos de 15 puntos: el PSSG mantendrá la categoría “Informado”.

- El PSSG se encontraba en la categoría de “Informado” y durante el periodo de 3 meses previo no ha acumulado ningún punto: el CCN estudiará la exclusión del PSSG de la RNS.

- El PSSG se encontraba en la categoría de “Gold” y durante el periodo de 3 meses previo ha acumulado, al menos, 7 puntos: el PSSG mantendrá la categoría “Gold”.

- El PSSG se encontraba en la categoría de “Gold” y durante el periodo de 3 meses previo ha acumulado menos de 7 puntos: el PSSG pasará a la categoría “Informado”.

Anexo 2: Formulario de adhesión

El siguiente formulario debe ser rellenado por el responsable del SOC por parte del PSSG de servicios:

Formulario de Ingreso

Informe de la organización

Nombre de la organización:

Servicios del SOC:

SOC del sector público al que da servicio:

Sede de la organización:

Razones de participación

Valor añadido

Datos del representante

Nombre y apellidos:

Cargo/puesto en la organización:

Email de contacto:

Ciudad:

Firma

Nombre y apellidos:

Firma:

Fecha:

Red Nacional de SOC

Anexo 3: Documento de entrega al organismo apoyado por el SOC

Plantilla de correo electrónico para el cliente.

Buenos días,

Por la presente deseamos informarle sobre la iniciativa de la **Red Nacional de SOC (RNS)**, coordinada por el CCN-CERT, que tiene como misión promover la cooperación entre los SOC de distintos organismos públicos y privados, con el fin de incrementar la capacidad de detección y la protección de los miembros de la red.

Para ello, el **CCN-CERT** ha establecido mecanismos internos de compartición de información relevante sobre ataques activos. Dicha compartición se llevará a cabo garantizando, en todo momento, que estos datos genéricos no identificarán el organismo en el que se han encontrado. Esta colaboración repercutirá positivamente en todos los participantes, ya que los integrantes de la red y sus clientes se beneficiarán de la información compartida para tomar medidas proactivas frente a las amenazas activas en el ciberespacio nacional.

Con la intención de mejorar siempre el servicio que le ofrecemos, queremos comunicarle la participación de nuestra empresa en esta actividad y esperamos contar con su aprobación para integrar en la RNS los indicadores de ataque (convenientemente anonimizados) que localicemos en su organización y que puedan ser de interés para la acción común.

Por favor, devuelva firmado y completado el formulario de autorización adjunto a este correo.

Atentamente,

[Representante del SOC]

Formulario de autorización para cliente

Al cliente / organismo apoyado por el SOC se le adjunta el formulario de autorización presente en la siguiente página, que debe devolver firmado y completado.

D/Dª:

_____

en representación de la organización:

_____

por su cargo en dicha organización como:

_____

autoriza al SOC _____, como miembro de la Red Nacional de SOC (RNS) coordinada por el CCN-CERT, a integrar en la RNS los indicadores de ataque (totalmente anonimizados) localizados en su organización y que puedan ser de interés para la acción común.

El fin de esta iniciativa será poder tomar medidas proactivas frente a las amenazas activas en el ciberespacio nacional, de manera que todos los organismos apoyados por los SOC miembros de la RNS se vean beneficiados por el incremento de su capacidad de detección y protección que esto supone.

En _____, a ____ de _____ del año _____

Anexo 4: Qué se debe compartir en la RNS

Se definen 4 líneas de compartición diferentes:

1

Una primera línea

En la cual, si hay algún incidente activo cuya víctima sea un organismo público, se introducirá automáticamente en el MISP evitando identificar el nombre de la víctima.

2

Segunda línea de comunicación

Basada en la certeza que tiene la empresa que reporta el evento de la IP sospechosa. En los casos en los que se tenga una certeza alta de que la IP es maliciosa y está vinculada a un evento de ransomware o intrusión (mecanismo de detección, comportamiento, etc.), se incluirá la alerta en el MISP con una etiqueta que identifique la certeza con un valor de alerta según el criterio de la empresa que lo reporta.

3

Tercera línea de comunicación

A través de Element se creará un "BOT" encargado de validar IPs potencialmente maliciosas. Las IPs introducidas en este canal se revisarán y se contrastarán con repositorios existentes de direcciones IP previamente identificadas como maliciosas. En caso que la dirección IP reportada no se encuentre en ninguno de estos repositorios, se creará una lista de IPs potencialmente peligrosas en las que se incluirá esta dirección IP. Esta lista tendrá una validez de 2 semanas. Además, este canal y su contenido será susceptible de debate para cuestionar la veracidad de lo ahí reportado.

4

Cuarta línea de comunicación

Se ocupará de todo lo referente a las alertas "ZERO Days", con objetivo de registrar todo lo referente a un ZERO Day concreto. El "BOT" creado por el CCN será el encargado de crear una lista en la que registrará toda la información relevante por cada caso de ZERO Day relevante (por ejemplo, Log4j). Esta lista tendrá una caducidad de 2 semanas (se eliminará una vez pasado ese tiempo).

Condiciones de adhesión y permanencia

Red Nacional de SOC