El Centro de Operaciones de Ciberseguridad de la AGE y sus OO.PP.

Prestación de servicios horizontales de ciberseguridad

El Centro de Operaciones de Ciberseguridad (conocido abreviadamente como SOC o 'SOC de la AGE') viene a prestar servicios horizontales de ciberseguridad que aumenten la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones de la Administración General del Estado y sus Organismos Públicos, así como a mejorar su capacidad de respuesta ante cualquier ataque. En concreto, persigue incrementar la protección de la seguridad perimetral frente a amenazas externas, mediante la prestación de servicios horizontales de ciberseguridad.

Así, el Centro de Operaciones de Ciberseguridad viene a materializar el Servicio Compartido de Seguridad Gestionada para dotar a la Administración General del Estado y a sus Organismos Públicos de una infraestructura global y única que incluya el equipamiento necesario, así como su configuración, puesta en marcha, mantenimiento, operación, monitorización y gestión de incidentes de manera centralizada, como se había previsto en la primera Declaración de servicios compartidos, a la luz de la Estrategia de Ciberseguridad Nacional y de su Plan Nacional de Ciberseguridad. Es una

iniciativa conjunta del Centro Criptológico Nacional y de la Secretaría General de Administración Digital.

Contribuye a medidas previstas en el Esquema Nacional de Seguridad como las relativas a la protección de las comunicaciones, a la protección de los servicios (navegación por Internet, correo seguro, acceso remoto, etc.), la detección de intrusiones, la gestión de incidentes de seguridad, entre otras.

Por su naturaleza centralizada, el Centro de Operaciones de Ciberseguridad facilitará tanto la implantación de las herramientas y tecnologías más adecuadas en cada momento, como la adopción de medidas oportunas para una defensa eficiente, con economías de escala, por razón de la eliminación de duplicidades y la especialización.

Ámbito de aplicación y responsabilidades

El ámbito de servicio del Centro de Operaciones de Ciberseguridad será la Administración General del Estado y sus organismos públicos. Para poder participar de sus servicios se requiere que la entidad usuaria esté adscrita a la salida centralizada a internet de la Administración General del Estado, es decir, al lote 3 del contrato de Servicios consolidados de telecomunicaciones de la Administración General del Estado Fase 1.

La responsabilidad del Centro de Operaciones de Ciberseguridad recaerá en la Secretaría General de Administración Digital (SGAD) adscrita a la Secretaría de Estado de Función Pública, del Ministerio de Hacienda y Función Pública,

mientras que la operación del servicio corresponderá al CCN-CERT del Centro Criptológico Nacional, en su calidad de CERT Gubernamental Nacional.

Por un lado, la dirección técnica y estratégica incluirá actividades tales como el seguimiento y gestión del servicio, abarcando la coordinación con los Responsables de Seguridad de las entidades y otros actores involucrados, la gestión de la incorporación de nuevas entidades al servicio, la coordinación de la respuesta ante incidentes de seguridad, así como la difusión y promoción del servicio.

Por otro lado, la operación del servicio incluirá, fundamentalmente, la implantación de la infraestructura técnica y servicios de seguridad, los procedimientos de ciberseguridad, la operación de ciberseguridad y cuestiones asociadas como la detección de incidentes de seguridad, entre otras.

La dirección técnica y estratégica junto con la operación del servicio seguirá el esquema descrito en la Figura 1.

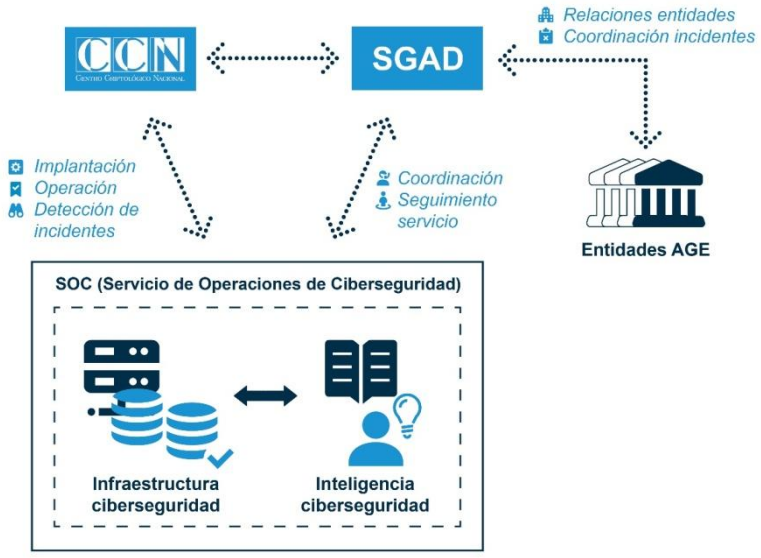

Figura 1. Esquema de prestación del servicio

El Centro de Operaciones de Ciberseguridad no viene a sustituir o reemplazar funciones o responsabilidades existentes. El enfoque de la arquitectura es *multitenant*, por lo que podrán implementarse configuraciones diferentes ante necesidades específicas de una Entidad. Cada entidad integrada en el Centro de Operaciones de Ciberseguridad mantendrá, a través de su responsable de seguridad, su responsabilidad en cuanto a la protección de la información y los servicios a su cargo. No obstante, la SGAD coordinará la respuesta ante incidentes de seguridad entre los diferentes agentes afectados.

Servicios del Centro de Operaciones de Ciberseguridad

El SOC ofrecerá servicios tales como:

- Operación, monitorización y actualización de dispositivos de defensa perimetrales.
- Detección, respuesta coordinada, investigación de ciberataques y ciberamenazas y resolución de incidentes de seguridad.
- Servicio de Alerta Temprana (SAT) de alertas de seguridad en las conexiones a Internet, a redes interadministrativas comunes y, bajo petición, a redes corporativas de las entidades.
- Análisis de vulnerabilidades de aplicaciones y servicios.
- Servicios anti-abuso de identidad digital.

Se contempla reforzar los servicios de carácter más nuclear de un SOC con otros servicios complementarios que proporcionan un valor añadido. Además, según la demanda de las entidades y la evolución del escenario de ciberamenazas en el tiempo, se realizará una evolución progresiva del servicio con el objetivo de obtener una mejora continua del nivel de seguridad ofrecido. Su objetivo final es apoyar, dar soporte y aumentar las capacidades existentes de vigilancia y respuesta donde se detecten carencias y los organismos demanden su ayuda, siendo prioritario lo siguiente:

- Monitorizar y evaluar de manera continua las medidas de seguridad en uso verificando su implementación.
- Actuar de manera proactiva incrementando y ampliando las capacidades de detección, vigilancia, protección y reacción ante incidentes.

- Parametrizar la amenaza mediante inteligencia de ciberseguridad que permita integrar la información siendo fundamental mejorar la notificación de incidentes e incrementar el intercambio de información.

La concepción habitual de un SOC hace referencia a una operación de la seguridad perimetral e integración con una gestión automática y centralizada de eventos a través de un SIEM (*Security Information and Event Management*). En este caso, el valor añadido del SOC será directamente proporcional a las capacidades de análisis y tratamiento de tráfico en la zona de corte delimitada por la "nube" central de la Figura 2:

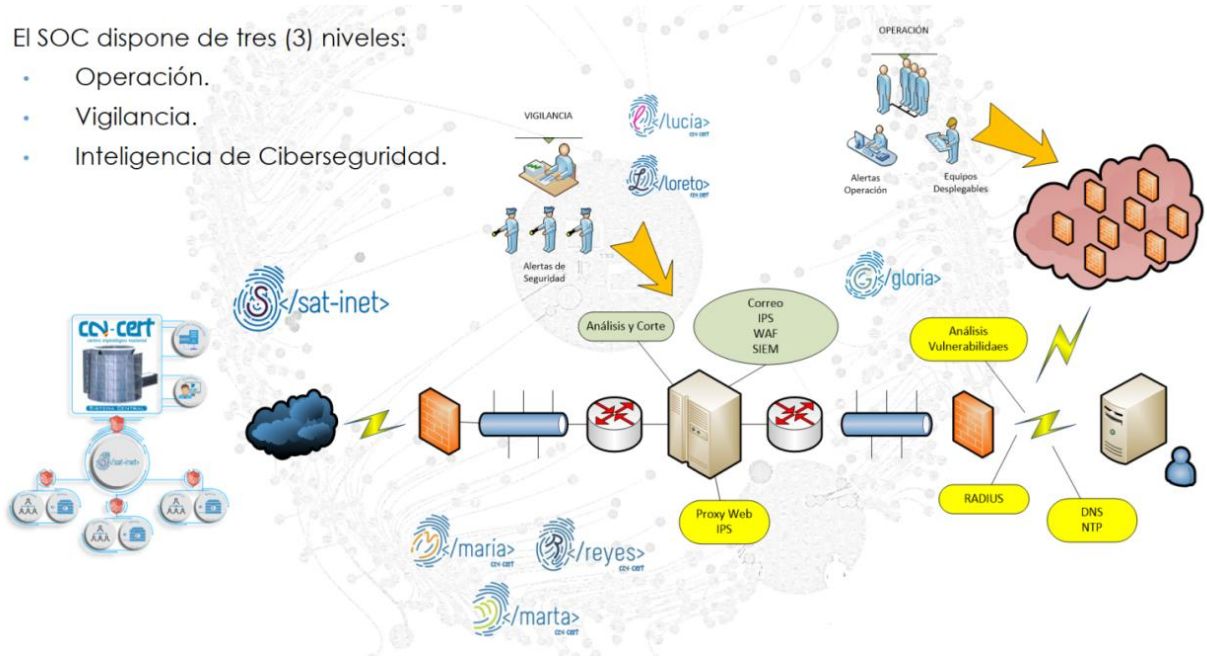

Figura 2. Esquema del Centro de Operaciones de Ciberseguridad de la AGE y sus OO.PP.

- Despliegue de infraestructura que permita descifrar las conexiones de cara a protección de servicios y aplicaciones.
- Analizar eventos de seguridad, emitir informes y recomendaciones.
- Filtrar y monitorizar, según la política de seguridad, el correo electrónico.
- Garantizar la seguridad de la navegación a Internet de los usuarios.
- Acceso VPN para conexiones desde el exterior.
- Análisis de vulnerabilidades y DNS pasivo.

Como complemento a dichos servicios, se dispondrá de un equipo de expertos para dar soporte en la investigación de incidentes de seguridad, en análisis forense, análisis de código, realizando análisis manuales e ingeniería inversa de binarios, asistencia in-situ para la contención y resolución de incidentes críticos y cibervigilancia en redes sociales e Internet.

Fases de despliegue del SOC

Se ha previsto que la constitución del Centro de Operaciones de Ciberseguridad se realice en un plazo de veinticuatro meses a la publicación del Acuerdo de Consejo de Ministros que determine su constitución. No obstante, en el segundo semestre de 2017 ya se han realizado tareas de diseño conceptual de las comunicaciones y del propio SOC.

Para el año 2018 se ha previsto una fase piloto en la cual se aborden tareas tales como la definición de los parámetros y niveles de servicio, la adquisición e instalación de la infraestructura técnica, la implantación de servicios básicos de ciberseguridad y la incorporación de primeras entidades.

En 2019 y años posteriores, se contempla una fase de consolidación con la extensión del servicio a todo el ámbito de aplicación del citado Acuerdo de Consejo de Ministros y la inclusión de nuevos servicios avanzados de ciberseguridad. Más allá de 2019 se realizarán actuaciones de mantenimiento y mejora del servicio.

Conclusiones

El incesante incremento de los ciberataques que también sufren las entidades del Sector Público, en particular, la Administración General del Estado y sus Organismos Públicos, hace que sea prioritario reforzar la capacidad de prevención, monitorización, vigilancia y respuesta a través de un Centro de Operaciones de Ciberseguridad, además de incrementar y mejorar las capacidades para parametrizar la amenaza, identificar a los atacantes, así como para la determinación de objetivos y difusión de Inteligencia al respecto.

Autores:

Secretaría General de Administración Digital

Centro Criptológico Nacional – CCN