El Centro de Operaciones de Ciberseguridad de la AGE

El Centro de Operaciones de Ciberseguridad (conocido abreviadamente como SOC o 'SOC de la AGE') viene a materializar el Servicio Compartido de Seguridad Gestionada y a 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.

Miguel Ángel Amutio / Pablo López

El Centro de Operaciones de Ciberseguridad persigue incrementar la protección de la seguridad perimetral de la Administración General del Estado y sus Organismos Públicos frente a amenazas externas, mediante la prestación de servicios horizontales de ciberseguridad. Se trata de una iniciativa conjunta del Centro Criptológico Nacional y de la Secretaría General de Administración Digital.

En un ecosistema de la ciberseguridad donde las redes aisladas ya no garantizan que no se introduzca o extraiga información de las mismas, se hacen públicas capacidades de ataque significativas, se generaliza la actividad de empresas comercializadoras de "*hacking*" y los ataques a la cadena de suministro se están convirtiendo en una tendencia preocupante, resulta ineludible, no solo aceptar un riesgo residual, sino también potenciar las capacidades de monitorización y vigilancia, junto a una respuesta eficaz.

Se trata de un escenario complejo en el que se combinan, por un lado, el hecho de que la transformación digital hace de las TIC el fundamento de los servicios prestados por las administraciones públicas, y, por otro lado, el hecho de que son crecientes los riesgos y ciberamenazas, de forma que, según el CCN-CERT, el año 2017 ha concluido con del orden de 26.500 ciberincidentes de diversos tipos en las entidades del sector público y empresas de interés estratégico.

Finalidad y ámbito de aplicación

La finalidad del Centro de Operaciones de Ciberseguridad o SOC es la prestación de 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, así como la mejora de su capacidad de respuesta ante cualquier ataque.

Por su naturaleza centralizada, el SOC ha de facilitar tanto la implantación de las herramientas y tecnologías más adecuadas en cada momento, como la adopción de medidas oportunas para una defensa eficiente. Este enfoque supone la evolución hacia un

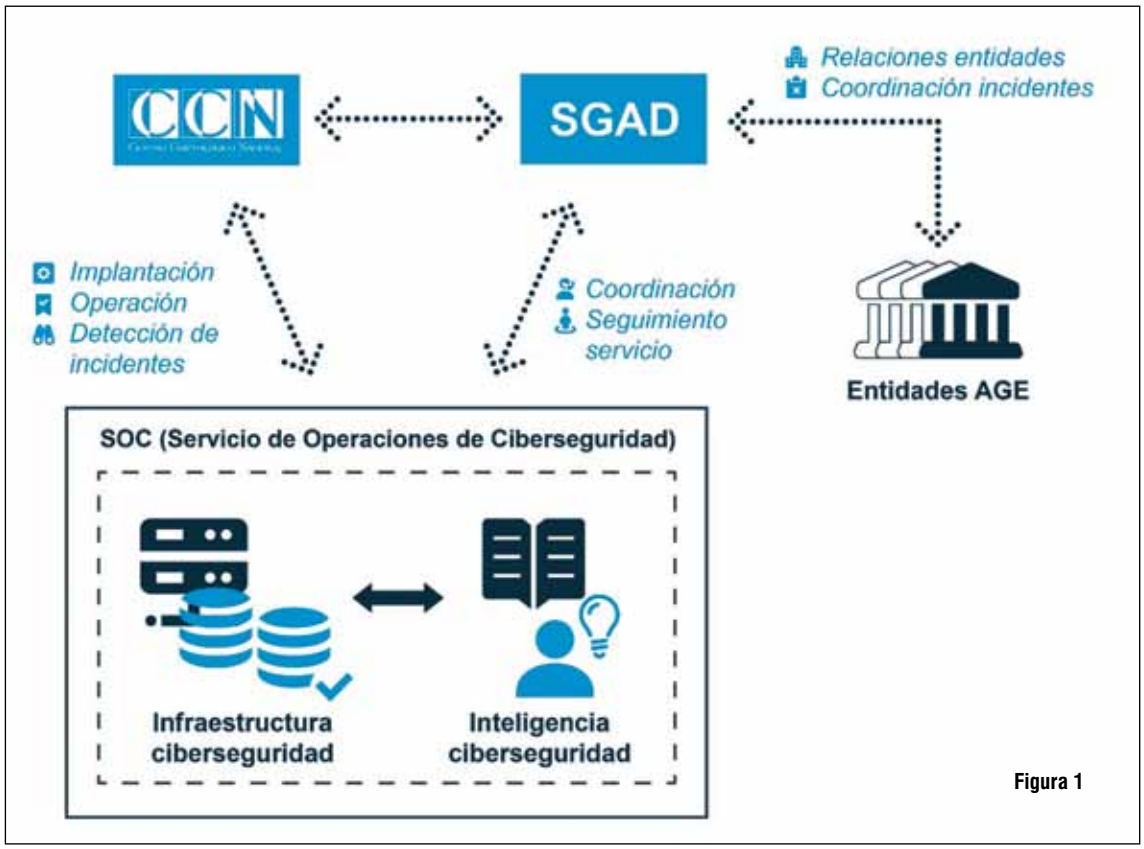

Figura 1

La responsabilidad del SOC 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.

modelo integral que favorezca la coordinación interdepartamental, a la vez que permite a cada entidad establecer sus propias políticas de seguridad y facilita el intercambio de información, todo ello con economías de escala, al favorecerse la eliminación de duplicidades y la especialización.

El ámbito de servicio del SOC será la Administración General del Estado y sus organismos públicos. Para poder participar de los servicios del SOC se requiere que la entidad 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.

Quién es responsable de qué

La responsabilidad del SOC 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 ha de incluir 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**.

Las entidades integradas en el Centro de Operaciones de Ciberseguridad mantienen, 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.

Funciones del Centro de Operaciones de Ciberseguridad

El SOC ofrecerá servicios como los que se indican a continuación:

- 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 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 (ACM) que determine su constitución. En el segundo semestre de 2017 ya se habían 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.

De esta manera, 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.

Valor añadido

El Centro de Operaciones de Ciberseguridad no viene a sustituir o reemplazar funciones o responsabilidades existentes. 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**:

- 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.

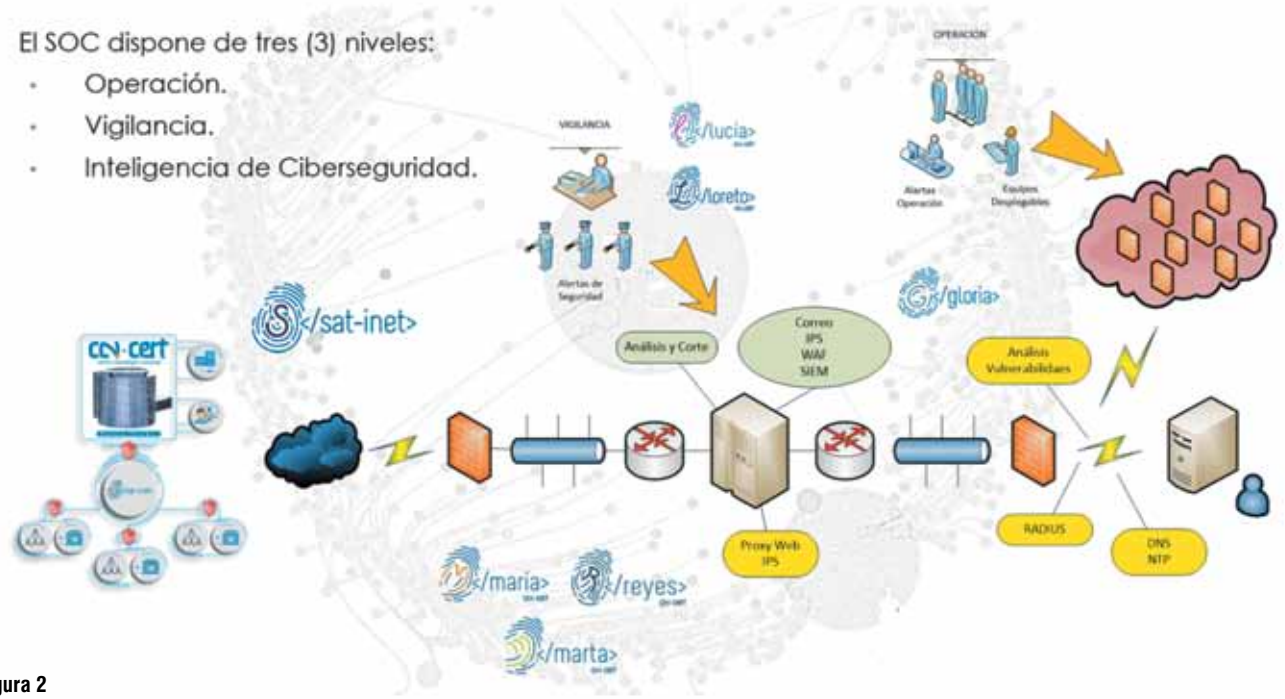

Figura 2

• 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

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 (ACM) que determine su constitución. En el segundo semestre de 2017 ya se habían 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. También, más allá de 2019, se realizarán actuaciones de mantenimiento y mejora del servicio.

mejorar las capacidades para parametrizar la amenaza, identificar a los atacantes, determinación de objetivos y difusión de Inteligencia al respecto.

El reto es grande, pero también la oportunidad de poder llevar a cabo un salto cualitativo en el ecosistema de ciberseguridad de la Administración General del Estado prestando un servicio no solo necesario, sino que aporte el valor añadido que haga del sector público junto con la colaboración público-privada un referente en este ámbito. ■

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. También, más allá de 2019, se realizarán actuaciones de mantenimiento y mejora del servicio.

Conclusiones

El incesante incremento de los ciberataques ha hecho que nuestro país, como el resto de los que componen su entorno, venga sufriendo, cada vez con mayor virulencia, intensidad y volumen, ataques de esta naturaleza, siendo también las entidades que componen su Sector Público víctimas de los mismos con los riesgos que ello puede suponer para nuestra posición estratégica, económica y social.

Por tanto, es prioritario reforzar la capacidad de prevención, monitorización, vigilancia y respuesta en el sector público a través de un Centro de Operaciones de Ciberseguridad, además de incrementar y

Miguel Ángel Amutio
Subdirector Adjunto en la S.G.
de Coordinación de Unidades TIC de
la Secretaría General de Administración Digital
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

Pablo López
Segundo Jefe del Departamento
de Ciberseguridad
CENTRO CRIPTOLÓGICO NACIONAL