Debate OSPI

Centros de Operaciones de Ciberseguridad en las Administraciones Públicas

Mayo 2022

OSPI.
Observatorio del sector público
inetum.

Introducción

El **Observatorio del Sector Público de Inetum** -OSPI- ha celebrado un nuevo debate con expertos del sector público sobre los Centros de Operaciones de Ciberseguridad en las Administraciones Públicas, -SOC-, por sus siglas en inglés.

Ha contado con la participación de:

- **Carlos Córdoba**. Jefe del Área de Centros de Operaciones de Ciberseguridad (CCN-CERT)
- **Esther Muñoz**. Subdirectora General de Ciberseguridad, Protección de datos y Privacidad (Madrid Digital)
- **Carmen Serrano**. Subdirectora General de Ciberseguridad (Generalitat Valenciana)
- **José Morales**. Gerente de Eprinsa (Empresa Provincial de Informática de la Diputación de Córdoba)
- **Clemente Barreto**. Jefe del Servicio Técnico de Planificación y Estrategias TIC (Cabildo de Tenerife)
- **Manuel Calderón**. Director de Ciberseguridad e Identidad Digital (Inetum)

Modera **Víctor M. Izquierdo,** Presidente del OSPI.

Tras analizar la situación actual en la que se encuentran sus respectivos organismos a la hora de implementar un Centro de Operaciones de Ciberseguridad, las intervenciones se han vertebrado en torno a los siguientes bloques:

- **Problemática específica** a la que se enfrentan CC.AA. y EE.LL. a la hora de prestar los servicios propios de un SOC y **definición de una hoja de ruta**
- **Interconexión y colaboración** entre SOC.
- **Tecnología y soluciones**
- **Visión de futuro**. Problemática de la sostenibilidad más allá de la fecha fin del PRTR -Plan de Recuperación, Transformación y Resiliencia-

Resumen Ejecutivo

Nos encontramos en un momento de explosión de las cuestiones que afectan a la ciberseguridad en las administraciones públicas. Un reto al que la Administración debe dar respuesta y garantizar la protección ante ciberataques a todas las entidades que conforman el sector público.

En este momento, que algunos de los panelistas califican como "de saturación" -por el mayor impacto mediático y la llegada de los fondos europeos-, los expertos invitados en esta jornada ponen en valor la importancia de estos foros no solo para difundir, también para compartir experiencias en los distintos organismos de la administración pública en nuestro país. Creen que es importante coordinar las diferentes actuaciones e identificar y planificar cada uno de los pasos a seguir.

Por ello, el debate sobre Centros de Operaciones de Ciberseguridad en las Administraciones Públicas arranca con una puesta en común del momento actual en que se encuentran cada uno de los organismos públicos que componen el panel, para abordar a continuación qué dificultades encuentran y qué actuaciones planean acometer en un futuro próximo.

El papel del **CCN-CERT** en la construcción del ecosistema de ciberseguridad para las AA.PP. se centra en tres ámbitos:

- **Apoyo al SOC la AGE**. Se encuentra en pleno proceso de articulación y desarrollo de acuerdos de colaboración con motivo de la reciente creación del SOC de la AGE, cuya aprobación tuvo lugar en el Consejo de ministros celebrados el 24 de mayo de 2021. La responsabilidad del SOC-AGE es de la Secretaría General de Administración Digital (SGAD), mientras que la operación del servicio corresponde al CCN-CERT del Centro Criptológico Nacional. El objetivo de este centro es "proteger a la AGE y sus entidades de las amenazas de ciberseguridad, así como reforzar la capacidad de vigilancia, prevención, protección, detección, respuesta ante incidentes de ciberseguridad, asesoramiento y apoyo a la gestión de la ciberseguridad".
- **Creación de la Red Nacional de SOC**. Iniciativa puesta en marcha por el Centro Criptológico Nacional con el fin de mejorar las capacidades de protección y defensa del ciberespacio español. Esta iniciativa viene avalada por la UE, que apuesta por la creación de una red de centros de operaciones de seguridad en toda la Unión.
- **Establecimiento de convenios de colaboración** para la implantación de nuevos SOC, que podrían recibir financiación procedente de los fondos Next Generation UE.

Madrid Digital –agencia de la Comunidad de Madrid que da servicio a 150.000 empleados públicos; más de 5.500 sedes de la Comunidad y cuenta con más de 1.500 aplicaciones-, puso en marcha en 2019 un Centro de Operaciones de Ciberseguridad, mediante licitación pública, que ofrece un servicio de análisis de vulnerabilidades, detección, vigilancia digital y capacidades de respuesta.

La **Generalitat Valenciana** acumula una larga trayectoria en la gestión de ciberseguridad. Desde 2007, con el CSIRT-CV, adscrito a la Dirección General de Tecnologías de Información, órgano encargado de prestar servicios TIC a la Generalitat. Presta servicios de prevención, detección y respuesta a incidentes a la administración valenciana y sus organismos públicos, así como a ciudadanos y empresas y a todas las administraciones territoriales propias de la Comunidad. Cuentan con un Pplan intensivo de integración de las entidades locales en su propio SOC, en el que han integrado 584 municipios, con servicios de vigilancia y detección para entidades locales. A las entidades locales de mayor tamaño les facilitan tener un SOC propio y estar integrados en la Red Nacional, pudiendo recibir ayudas de los fondos.

La **Diputación de Córdoba** presta servicio a todo el sector público de la Diputación: organismos de recaudación, empresas de agua, de recogida de residuos y a todos los ayuntamientos de la provincia de Córdoba, no solamente a los de menos de 20.000 habitantes, excepto a la capital. Y, desde 2019, prestan un servicio de SOC de atención junto con el CCN-CERT de Andalucía .

En 2018 el **Cabildo de Tenerife** -isla de casi 1 millón de habitantes y 31 municipios-, comenzó diversas actuaciones de centralización de infraestructuras y servicios TIC, especialmente en el ámbito de las comunicaciones, con diversas actuaciones de despliegue de fibra. En 2020 comienzan a plantearse una mejora de la ciberseguridad, con el apoyo del Centro Criptológico Nacional, mediante un convenio de colaboración para desplegar un SOC de entidades locales. Su alcance inicial incluye el Cabildo insular de Tenerife, el sector público insular (40 entidades) y un total de 17 municipios, aquellos con menos de 20.000 habitantes. La valoración, en el segundo año de implantación, es positiva. Se han incorporado más organismos de los inicialmente previstos y ya están trabajando conjuntamente con el Cabildo de El Hierro.

Inetum cuenta con un SOC desde el que ofrecen servicios a algunos de los organismos que participan en el debate, para que presten a su vez servicios de seguridad gestionada a terceros. En su intervención, **Manuel Calderón**, director de Ciberseguridad e Identidad Digital de la compañía, destaca la heterogeneidad y los diferentes grados de madurez en la evolución del catálogo de servicios de las diferentes comunidades autónomas y entidades locales. Desde servicios centrados en operación de seguridad y monitorización de eventos de seguridad, pasando por una evolución más orientada hacia la prevención y la detección basada en alerta temprana o respuesta a incidentes. “Vemos un reto en la evolución hacia la inteligencia de amenazas, analítica de eventos y adaptación a los contextos de cada una de las entidades, con diferentes situaciones”.

Dificultades y hoja de ruta

Aborda este primer bloque la problemática específica a la que se enfrentan las comunidades autónomas y las entidades locales a la hora de prestar los servicios propios de un SOC y cuál es la hoja de ruta y la situación hacia la que avanza cada uno de los organismos. Destacan, entre las **dificultades**, las siguientes:

- Recursos muy escasos, tanto en la propia administración como en las empresas contratadas para prestar servicios de seguridad gestionada. Consideran los expertos reunidos en esta jornada que, ante esta situación de escasez de recursos las operaciones de seguridad tienen que ser contratadas a terceros, pero la gobernanza debe recaer en todo caso en el ámbito interno, algo difícil en un contexto de escasez de personal. Por otro lado, el alto índice de rotación en las empresas en ocasiones plantea problemas de continuidad del servicio contratado. Exponen, además, en este punto, el fenómeno de fuga de talento hacia otros países que se está produciendo, propiciada por la extensión del teletrabajo. "Tenemos técnicos que han sido contratados en otro país. Contra eso no podemos competir", expone uno de los panelistas.
- Mayor exposición a posibles ataques, como consecuencia del aumento de la prestación de servicios digitales por parte de las administraciones y del teletrabajo. Ambas circunstancias contribuyen a un aumento de los riesgos.
- Profesionalización del ciberdelincuente.
- Aumento del panorama internacional de ciber amenazas.
- Vulnerabilidades del hardware y software adquiridos a terceros.
- Dificultad de integración de las entidades locales.
- Y, por último, un problema inicial no resuelto en muchos casos: la falta de centralización de las comunicaciones.

La **hoja de ruta** pasa por:

- Una mayor automatización.
- Mutualización de servicios para entidades locales.
- Creación de SOC siguiendo un modelo híbrido y adaptados al contexto de cada organización.
- Certificación en el Esquema Nacional de Seguridad (ENS).
- Concienciación y capacitación al personal de las administraciones.
- Enfoque cooperativo.
- Unificación de salidas a Internet y redes datos.

En cuanto a la hoja de ruta, en el caso de Madrid Digital, aumentarán los servicios que prestan de forma automatizada con el apoyo de fabricantes, proveedores y empresas. "Gestionamos más de 80.000 eventos por segundo; unos datos que debemos contextualizar y extraer información para construir casos de uso que faciliten la detección de amenazas e impedir o contener aquellaos que se produzcan", afirma **Esther Muñoz**, Subdirectora General de Ciberseguridad, Protección de datos y Privacidad de Madrid Digital.

Por otro lado, aunque este organismo TIC no incluye la prestación de servicios a entidades locales, la Comunidad de Madrid sí tiene previsto crear una **Agencia de Ciberseguridad** encargada de desplegar una cartera de servicios incrementales hacia las entidades locales y de apoyo a la *pyme* y la ciudadanía.

Corrobora **Manuel Calderón**, de Inetum, las dificultades para la atracción y retención de talento en las empresas, una situación que relaciona con otros dos aspectos: cree necesario elevar la función del personal de los centros de operaciones de seguridad, evolucionando hacia una actuación más analítica aprovechando las nuevas tecnologías. Y apuesta por un formato de SOC hibrido y adaptado al contexto del negocio, ya sea una entidad pública o privada. Aunque, en el ámbito público, explica, "nos regimos por la Ley de Contratos, por lo que es difícil comparar con el sector privado. Aportamos valor agregado con el entendimiento de contexto, lo que es un reto y un punto de dificultad".

La Generalitat Valenciana ha duplicado su personal interno dedicado a ciberseguridad. Aunque con dificultades, entre otras, la necesidad de dar un itinerario formativo previo a los profesionales que se incorporan. Apuesta por contener la creación de SOC. "Nos robamos personal unos a otros. Nos pone en riesgo a los que tenemos gente especializada y formada", afirma **Carmen Serrano**, Subdirectora General de Ciberseguridad, y señala la dificultad de integración en el SOC de las entidades locales. "La heterogeneidad y diversidad de tecnologías y arquitecturas requiere un esfuerzo importante por parte del SOC en cada caso para el despliegue de herramientas. Con un total de 584 municipios, 438 tienen menos de 5.000 habitantes. En estos casos recurrimos a las diputaciones, que aportan personal de última milla, gracias a su mayor cercanía al municipio".

En cuanto a sus planes de futuro, se encuentran redefiniendo el catálogo de servicios, teniendo en cuenta las nuevas entidades a las que prestarán apoyo: también aumentarán los servicios que ofrecen a entidades locales y, por último, aspiran a automatizar tareas repetitivas, de modo que los técnicos se centren en tareas de más valor, como son las funciones de alto nivel de seguridad frente a aquellos trabajos más próximos a la operación de sistemas y redes.

Considera **José Morales**, Gerente de Eprinsa (Diputación de Córdoba), que antes de abordar la creación de un SOC, es necesario centralizar las comunicaciones y las compras en las distintas administraciones. Apuesta por la creación de SOC regionales y nacionales, híbridos, en colaboración con las empresas, "ya que, para una entidad pública es inviable contar con un SOC que dé servicio 24x7"; y por la certificación por parte de entidades acreditadas, para cumplir unos requisitos mínimos de seguridad. "Tenemos la nueva versión del ENS recién publicada, y aún estamos pendientes de cumplir la anterior. Es una cuestión previa al SOC, es una necesidad imperiosa que debemos resolver de forma inmediata".

Carlos Córdoba, Jefe del Área de Centros de Operaciones de Ciberseguridad (CCN-CERT), coincide en la necesidad de certificarse. "En la actualidad hay más organismos privados que públicos certificados en el ENS. Es el Himalaya al que se enfrentan las administraciones públicas: se ponen delante de él y mueren en el intento. Debemos pensar en cómo facilitar esa certificación". Apunta, no obstante, que a los nuevos SOC que proponen se les exige contar con una oficina ENS que asesore en las medidas de seguridad, lo que, en su opinión, contribuirá a que aumenten las certificaciones. Aunque, matiza, muchos organismos desestiman esa certificación porque carecen de los recursos necesarios.

Menciona, además, el objetivo del CCN-CERT de involucrar a los responsables públicos en la Red Nacional de SOC, representados en una parte pública destinada a intercambiar información. "Queremos atraer a los responsables públicos que van a dirigir estos centros de seguridad. Tenemos que asesorarlos y organizarlos". Explica cómo los casos del Cabildo y la Diputación de Córdoba son dos ejemplos a seguir en relación con su estrategia de creación de SOC. "En el caso de Córdoba, tienen la salida integrada a Internet de toda la provincia. Es el paso 0".

Como conclusión a este primer bloque de debate, **Clemente Barreto**, Jefe del Servicio Técnico de Planificación y Estrategias TIC del Cabildo de Tenerife, menciona los retos principales a considerar:

- Concienciación a la Dirección, algo que se ve beneficiado por el impacto mediático de los problemas de ciberseguridad.
- Necesidad de concienciación y capacitación al personal interno de las organizaciones.
- El enfoque de SOC no debe incluir solo aspectos de ciberseguridad. También gobernanza y concienciación. El Esquema Nacional de Seguridad actúa como hoja de ruta.
- Enfoque híbrido del SOC, con participación del sector privado, que compense las carencias de la administración pública.
- Enfoque cooperativo. Las diputaciones, cabildos y comunidades autónomas afrontan el reto de definir SOC regionales, por ello es necesaria la coordinación entre los organismos. Con proyectos de centralización de infraestructuras y comunicaciones para ser más eficientes a la hora de cumplir el ENS.

Interconexión y colaboración

Las intervenciones en el segundo eje del debate se centran en la **Red Nacional de SOC**[1]. Cómo organizar los SOC en red, más allá del ámbito propio de actuación de cada administración.

Destacan, como aspectos principales, los siguientes:

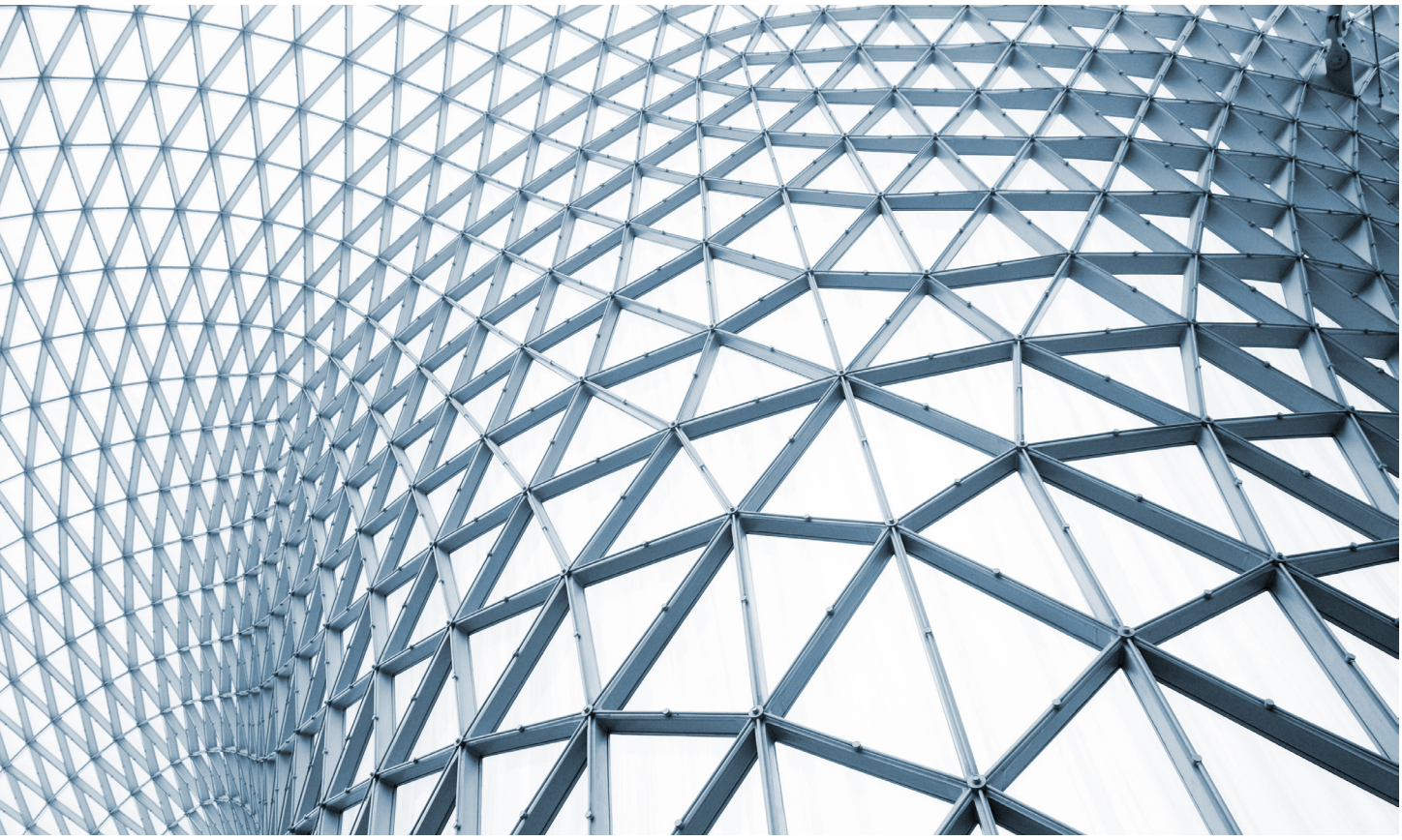
- Intercambio de datos técnicos entre entidades.
- Modelo federado, jerárquico y centralizado a través de los distintos modelos de administración, con una definición clara de competencias entre administración general, regional y local, con una gobernanza única y supervisión por parte del CCN-CERT.
- Colaboración con empresas que estén dentro de la Red Nacional de SOC, certificadas en el ENS.
- Elaboración de pliegos tipo y contratación de servicios completos.
- Uso inflacionista del término SOC. Exceso de convenios de colaboración.
- Cooperar-colaborar entre muchas partes.

En relación a cómo mejorar las dificultades expuestas en el punto anterior, desde la Red Nacional de SOC tienen varios objetivos. En primer lugar, concienciar a los empleados públicos de la necesidad de compartir los datos de sus organismos. Explica **Carlos Córdoba**, de CCN-CERT, cómo en el proyecto de creación de la Red Nacional de SOC ya han intercambiado datos técnicos entre seis empresas. "El modelo federado propuesto asesora a los SOC sobre las soluciones que deben tener en los distintos niveles de administración: a nivel local, o de comunidad autónoma. Asimismo, la UE aspira a la creación de una red europea de SOC, y en España es el país somos de los más avanzados en la puesta en marcha de esta red".

Para **Carmen Serrano,** de la Generalitat Valenciana, la colaboración entre los organismos públicos y la implicación del sector privado es el modelo adecuado. Defiende un modelo jerárquico con integración a través de los distintos niveles de administración, frente a la dispersión de muchos SOC.

Señala **José Morales**, de la Diputación de Córdoba, la necesaria definición de competencias de las administraciones general, regional y local y del CCN-CERT "y dotarlas de recursos presupuestarios, como se hizo con la administración electrónica". Añade, además, consideraciones en relación con los pliegos. "Las diputaciones provinciales demandan pliegos tipo para contratar todos lo mismo; servicios completos, ya que no estamos preparados para elaborar pliegos muy específicos".

[1] *Rentero, A. (22 agosto 2022).* ***Inetum se convierte en miembro Gold de la Red Nacional de SOC del Centro Criptológico Nacional.*** *Silicon. https://www.silicon.es/inetum-se-convierte-en-miembro-gold-de-la-red-nacional-de-soc-del-centro-criptologico-nacional-2462730*



"El modelo de los SOC tiene que ser jerárquico y centralizado". En el caso de la Comunidad de Madrid, con un total de 105 municipios con menos de 5.000 habitantes "no tiene sentido que cada uno monte un SOC por su cuenta", afirma Esther Muñoz, de Madrid Digital. "A ello hay que unir una gobernanza y control únicos en el ámbito de la organización y contar con la supervisión del CCN-CERT. Además, las redes de datos y salidas a Internet deben estar unificadas para dar servicios de SOC de forma más eficiente". Concluye su intervención en este bloque con una reflexión sobre el alcance del término SOC. Un SOC debe ofrecer servicios de prevención y, sobre todo, de detección, pero en ocasiones se hace un uso inflacionista del término, confundiéndolo con la prestación de otros servicios, como gestión de accesos o servicios antispam… entre otros.

Clemente Barreto, del Cabildo de Tenerife, enfatiza en este bloque la colaboración para mejorar la detección. "Cuantas más entidades monitoricemos y compartamos información, más protegidos estaremos y más posibilidades de atención conjunta tendremos". Cree que esta colaboración ha de ir acompañada de una regulación mínima que todos los nodos de la red han de cumplir. "El reto es grande; el alcance es grande. Es un proyecto estructural, un servicio, un organismo, un grupo de personas que vienen para quedarse en la organización". Apuesta, por tanto, por definir y estandarizar qué es un SOC, de qué debe ir acompañado el proyecto de un SOC, y acompañarlo de la regulación necesaria para que la operación, la detección y la cooperación sean una realidad.

Tecnología y soluciones

Cuáles son las ventajas e inconvenientes de las diferentes alternativas y qué papel desempeña el CCN-CERT en la evaluación y homologación de productos de seguridad que faciliten un catálogo a las AAPP son las principales cuestiones debatidas en el este bloque.

Comienza el turno de intervenciones **Manuel Calderón**, de Inetum, empresa que colabora con la Comunidad de Madrid en la concentración en la salida a Internet, alabando la función del CCN-CERT en la evaluación y homologación de productos y servicios de seguridad que se recogen en un catálogo que se actualiza mensualmente y es de mucha utilidad para las AAPP. Aunque señala, como punto de mejora, que tendría que ser más dinámico, ya que, "la tecnología avanza rápido, con nuevos paradigmas, nuevas soluciones que nacen nativas en *cloud*… Es una misión clave y sirve de gran ayuda a las entidades públicas que un tercero vele por los requisitos básicos que una determinada solución de seguridad debe cumplir". Por otra parte, c continuar mejorando la metodología LINCE y que se adapte al contexto actual de la ciberseguridad.

Reconoce **Carlos Córdoba**, del CCN-CERT, que han de ganar agilidad en cuanto a certificación de las soluciones. "Es el muro donde se está estrellando la UE". Así, frente a procesos de certificación de seis meses que no tienen sentido porque los productos se actualizan, también existen riesgos en certificaciones realizadas con excesiva rapidez, expone.

En relación a las soluciones propias del CCN-CERT, "gratuitas y compartidas para las administraciones, porque los organismos públicos carecían de recursos, tuvieron su momento. Y lo siguen teniendo; nuestras soluciones son buenas y ahí están" afirma **Carlos Córdoba**. Y efectivamente, así es, tal como corroboran el resto de los panelistas, que apuestan por estas soluciones comunes y compartidas, que, además de resolver la problemática del coste, evitan la gestión de los contratos, contrataciones de soportes y mantenimientos y suponen una apuesta por la tecnología española y la soberanía digital. Aunque, por otro lado, demandan también la necesidad de que estas herramientas puedan escalar a entornos de mayores dimensiones, como ocurre con Madrid Digital, con la ingente cantidad de eventos gestionados. "Es nuestro futuro, optar por herramientas de CCN-CERT que pueden complementarse con soluciones de empresas privadas", expone **Esther Muñoz**.

Concluye este eje temático con los beneficios de los acuerdos marco en el ámbito TIC de la administración. "La centralización de contratación del Estado tiene acuerdos marco para la adquisición de productor informáticos, servidores…" afirma **Clemente Barreto**, del Cabildo de Tenerife. En cuanto a soluciones de ciberseguridad, coincide en que la primera opción es usar las soluciones del CCN-CERT. "Más allá, soluciones certificadas del catálogo de ciberseguridad y si tenemos que comprarlas, ir hacia escenarios de centralización y racionalización de la contratación".

Visión de futuro

A continuación, lanzan los ponentes una mirada al futuro, teniendo en cuenta el momento favorable presupuestario propiciado por los Fondos europeos de Recuperación y Resiliencia y la problemática de la sostenibilidad más allá de la fecha fin del Plan de Recuperación, Transformación y Resiliencia.

- Actuar con coherencia. Cuando los fondos europeos se agoten, habrá que pagar con fondos ordinarios al personal del SOC. La Red Nacional de SOC aportará orden y organización a la situación.
- Apostar por SOC centralizados y jerárquicos con carteras de servicios incrementales, siguiendo las recomendaciones del CCN-CERT.
- Racionalizar. Lo importante es contar con los servicios de un SOC, no tener un SOC. Hay que estar en la Red Nacional de SOC a través de un modelo racional, centralizado y jerárquico. Es la solución. No está justificado invertir en SOC que no podamos mantener. Lo costoso serán los recursos humanos, cada vez más demandados.
- Más que dedicar los fondos a la creación de SOC, el organismo -autonómico o local- debe disponer de presupuesto para dedicar a temas de ciberseguridad, que no debe depender de una subvención, sino debe ser considerado un gasto corriente que tiene que asumir todos los años. Algo que deben hacer todas las administraciones, no solo aquellas que consigan fondos. El presupuesto de entidades locales o autonómicas tiene que contemplar un presupuesto anual para SOC, considerándose así un gasto corriente más. Y, por otro lado, destinar los fondos de Recuperación y Resiliencia a la creación de empleo y formación de personal en ciberseguridad, tanto en el sector público como en la empresa privada, contribuyendo así a crear empresas más potentes.
- Pensar en la ciberseguridad como:
  - Un aspecto estructural, que forma parte del gasto corriente de las organizaciones;
  - Requiere colaboración y cooperación y no ha de plantearse como una guerra particular de cada entidad;
  - Comienza en los usuarios. No depende solo de implantar software, sino que debe ir acompañada de gobernanza, centralización de infraestructuras y de servicios. Debe formar parte de un plan más amplio, vinculado a la digitalización, y a muchas otras actuaciones de transformación de las AAPP.
- Apoyo de las entidades públicas en el sector privado para hacer sostenible la prestación del servicio, basado en un análisis coste-beneficio, con un caso de negocio que lo haga sostenible, y no sea algo puntual. La colaboración y la interconexión serán clave; poder trabajar y evolucionar en cierto grado de automatismo y capacidades predictivas, para reducir las necesidades de personal intensivo en tareas de menor valor. Destaca, en este ámbito, la incorporación de Inetum al **Clúster de Inteligencia Artificial de la Comunidad de Madrid** , con el objetivo de aplicar la inteligencia artificial para reducir personal en tareas que no aportan valor.

Sobre el Observatorio del Sector Público

Con el foco puesto en la transformación digital de las Administraciones Públicas, el Observatorio del Sector Público lleva a cabo tareas de identificación, ordenación, valoración y difusión de políticas públicas, planes de acción, proyectos y servicios exitosos para la transformación digital, provenientes principalmente del ámbito internacional, a partir de los cuales se pueden efectuar propuestas aplicables al sector público español, dando lugar a un verdadero centro de conocimiento de la Administración Digital.

OTRAS PUBLICACIONES:

www.ospi.es

OSPI.

Observatorio
del sector público

inetum