



PROMOCIÓN DE CENTROS DE OPERACIONES DE CIBERSEGURIDAD EN ENTIDADES LOCALES



Contacto: ccn@cni.es



ÍNDICE

Resumen ejecutivo	P.3
Escenario actual de ciberamenazas	P.4
Centros de Operaciones de Ciberseguridad	P.6
SOC Entidades Locales	P.7
Proceso de despliegue de un SOC	P.8
Aportación del CCN al SOC	P.9
Red Nacional de SOC	P.10
Anexo: Casos de éxito destacados	P.11

RESUMEN EJECUTIVO

Centros de Operaciones de Ciberseguridad



CCN-cert
centro criptológico nacional

Ningún organismo escapa hoy de la amenaza de un ciberataque

En cuestión de minutos una organización puede ser víctima del robo y destrucción de la información de toda su entidad.

Las pérdidas y la repercusión que para una organización tendría ser víctima de un ciberincidente podrían ser irreversibles.

Los desafíos y amenazas en ciberseguridad son cada vez más numerosos y complejos, técnicamente más avanzados y con mayor capacidad de impacto.

Cualquier organización debe estar preparada para prevenir, detectar y responder a un posible ciberataque.

SOC: ciberseguridad integral y horizontal

Los Centros de Operaciones de Ciberseguridad (SOC) son la respuesta a este paradigma. Proporcionan servicios horizontales de prevención, detección, cibervigilancia, protección y respuesta a todas las áreas de una organización y ante cualquier tipo de amenaza.

La implementación de los SOC ha de ser una prioridad estratégica para cualquier organismo de la Administración Pública como medida urgente para reforzar sus políticas y estrategia de seguridad.

SOC Entidades Locales

La arquitectura y dimensión de los Centros de Operaciones de Ciberseguridad (SOC) es flexible y atiende al tipo de organización en la que se integra: pequeñas entidades o vSOC (virtual).

El objetivo de los SOC Locales es dar seguridad de forma centralizada a conjuntos de organismos o ayuntamientos pequeños.

Red Nacional de SOC

Todos los Centros de Operaciones de Ciberseguridad que se desplieguen en este ámbito formarán parte de la Red Nacional de Centros de Operaciones de Ciberseguridad, en la que el CCN ya está trabajando, y que integrará a una amplia tipología de SOCs.

La coordinación de todos los SOCs integrados en esta red nacional se llevará a cabo a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

SUPUESTO DE INSTALACIÓN Y DESPLIEGUE DE UN SOC ENTIDADES LOCALES



Centraliza y ofrece servicios de ciberseguridad horizontal a un máximo de **20 organismos***



Cubre la ciberseguridad de los puestos de trabajo de **5.000 usuarios**

Servicios iniciales

- Auditoría inicial
- Revisión
- Formación de equipo de seguridad
- Instalación de soluciones y SW de defensa
- Instalación de solución específica de protección contra el ransomware
- Apoyo para la adecuación al ENS
- Equipo de búsqueda de incidentes de seguridad

Servicios avanzados

- Servicios del SOC Inicial +
- Implementación de listas blancas
 - Instalación de herramienta avanzada de detección de anomalías en equipos de usuario
 - Auditorías recursivas y de código
 - Servicio de monitorización de los sistemas
 - Vigilancia digital
 - Apoyo a la implementación del ENS



Tipo de **servicios**



Coste aproximado y orientativo de instalación

600.000 €

1.000.000 €



Coste servicio anual

150.000 €

250.000 €

* El coste asociado a cada SOC no varía en función del número de organismos al que dé servicio. Es decir, dar servicios de ciberseguridad a 20 organismos tendría un coste similar que ofrecerlo solo a dos.



ESCENARIO ACTUAL DE CIBERAMENAZAS

NINGÚN ORGANISMO ESCAPA HOY DE LA AMENAZA DE UN CIBERATAQUE

Desde el inicio de la pandemia de la COVID-19, estamos siendo testigos de un indudable aumento cuantitativo y cualitativo de los incidentes de seguridad; incidentes que están afectando de forma progresiva a un mayor número de organismos y entidades del sector público.

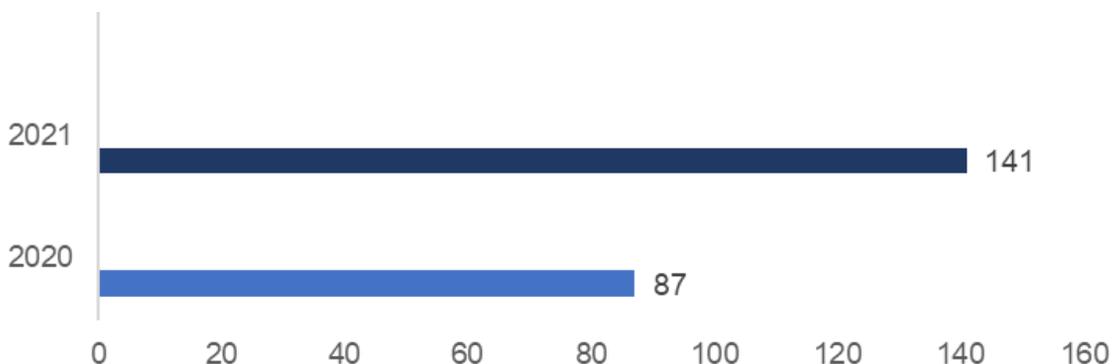
La situación excepcional de teletrabajo, que obligó a multitud de organismos a implementar de forma urgente y precipitada redes, conexiones y sistemas que permitiesen a su personal dar continuidad a su actividad de forma remota, ha afectado y continúa afectando a la seguridad de sus infraestructuras y redes.

Los riesgos a los que una organización se enfrenta son cada vez mayores, no solo por el aumento de su superficie de exposición, sino también por las cada vez más sofisticadas capacidades operativas y técnicas de los ciberatacantes: **en cuestión de minutos una organización puede ser víctima del robo y destrucción de la información de toda su entidad**. Un escenario que se está agudizando ante la creciente hiperconectividad y dependencia tecnológica.

Los conocidos **ciberataques por ransomware han evolucionado a una velocidad incontestable**. Su ejecución por parte del ciberatacante es hoy casi automática; sin embargo, **las pérdidas y la repercusión que para una organización tendría ser víctima de un incidente de este tipo podrían ser irreversibles**



En cuestión de minutos una organización puede ser víctima del robo y destrucción de la información de toda su entidad.



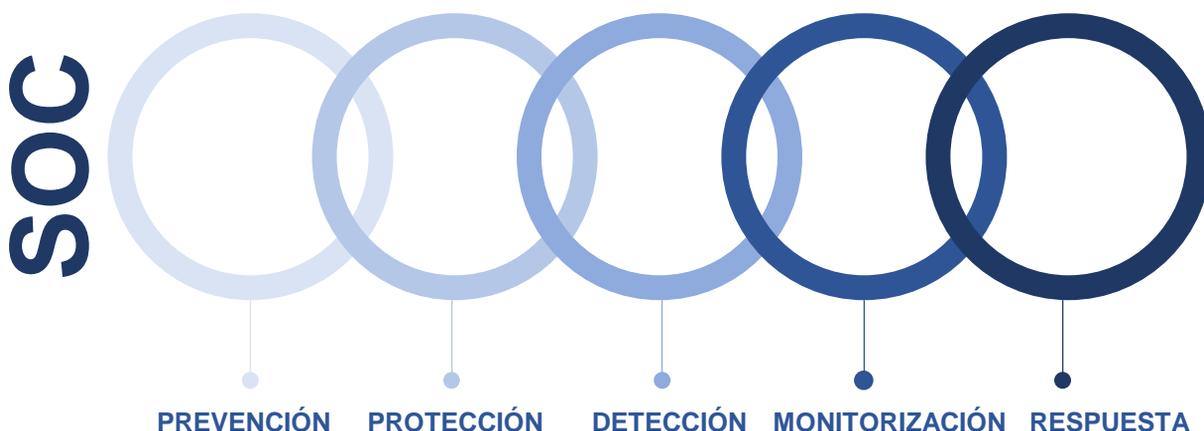
Pero el ransomware no es la única amenaza a la que está expuesta una organización, también lo está a la **explotación de vulnerabilidades de seguridad de dispositivos o productos de software, a otras variantes de código dañino, a la explotación de servidores mal configurados o a campañas de amenazas persistentes avanzadas (APT)**. Y además del robo o secuestro de la información de una entidad, una organización también puede ser víctima de una **interrupción de servicios, fraude, de brechas de datos, de ciberespionaje o de la paralización de sistemas y procesos productivos**.

Sin duda, los vectores de ataque y de amenaza a una organización con deficiencias en su política de ciberseguridad pueden llegar a ser inagotables si no se toman las decisiones y medidas necesarias. **La ciberseguridad** requiere del mismo nivel de exigencia que se aplica de forma análoga a otras áreas de protección de una organización, como puede ser su seguridad física. Se trata, por tanto, de implementar en los activos digitales de una organización los mismos mecanismos de defensa que a los bienes materiales.

ES NECESARIO TOMAR DECISIONES Y MEDIDAS EN MATERIA CIBER

Los servicios de seguridad de prevención, protección, monitorización, detección y respuesta, en el ciberespacio se integran y ofrecen desde los **Centros de Operaciones de Ciberseguridad (SOC)**

Estos servicios de seguridad de **prevención, protección, monitorización, detección y respuesta**, en el ciberespacio se integran y ofrecen desde los **Centros de Operaciones de Ciberseguridad (SOC)**, que permiten a una organización aumentar su **capacidad de vigilancia y detección de amenazas** en el empleo diario de los sistemas de información y comunicaciones y mejorar su capacidad de respuesta ante cualquier ataque.

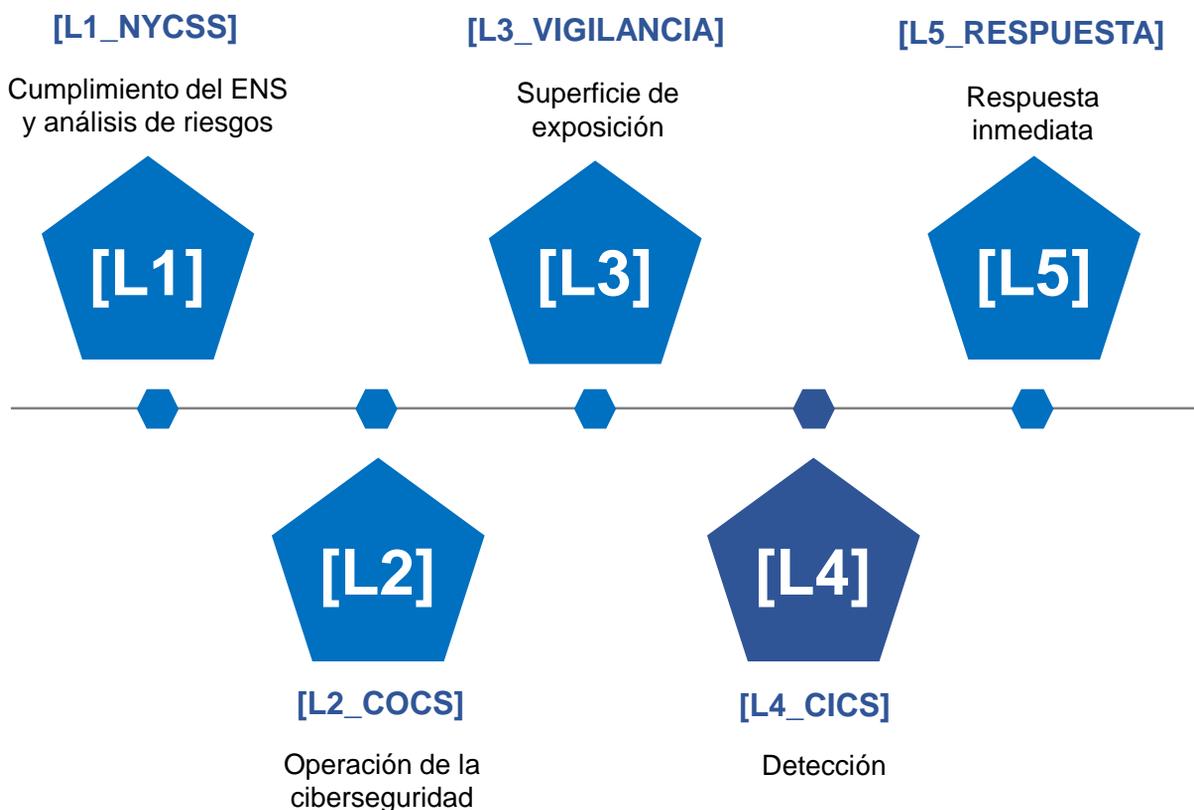


CENTROS DE OPERACIONES DE CIBERSEGURIDAD

Los desafíos y amenazas en ciberseguridad son cada vez más numerosos y complejos, técnicamente más avanzados y con mayor capacidad de impacto. Cualquier organización debe estar preparada para **prevenir, detectar y responder a un posible ciberataque**. Y, sin duda alguna, los **Centros de Operaciones de Ciberseguridad** constituyen la respuesta a este paradigma.

Los SOC se integran dentro de la estructura de una organización para ofrecer seguridad integral a todos sus departamentos, áreas y servicios. **Su misión, por tanto, es centralizar la ciberseguridad de la organización y proporcionar servicios horizontales de prevención, detección, cibervigilancia, protección y respuesta a todas sus divisiones ante cualquier tipo de amenaza.**

En base a la experiencia del CCN-CERT, cualquier iniciativa en la creación de este tipo de estructuras debe ir acompañada de un proceso de adecuación al **Esquema Nacional de Seguridad (ENS)** como marco de referencia en medidas de seguridad. El ENS se convierte de esta manera en la guía que marcará al organismo hacia dónde debe **encaminar sus medidas de seguridad**.



SOC ENTIDADES LOCALES

La arquitectura y dimensión de los Centros de Operaciones de Ciberseguridad (SOC) es flexible y atiende al tipo de organización en la que se integra. Es decir, su estructura y los recursos necesarios para su despliegue y operación varían en función del tamaño de la organización y su escenario de actuación, pudiendo llegar a ser virtuales, (vSOC). La capacidad de adaptación de estos centros a la casuística de cualquier organismo de la Administración, independientemente de su tamaño y funcionamiento, hacen de los SOC una **iniciativa viable para todo aquel organismo comprometido con la ciberseguridad**.

El objetivo de estos SOC es dar seguridad de forma centralizada a conjuntos de organismos o ayuntamientos pequeños. Esta gestión centralizada permite aunar fuerzas y esfuerzos para **ofrecer a las pequeñas entidades mejores servicios con una dedicación de personal que de forma individual no tendrían**.

La gestión centralizada que permite llevar a cabo un SOC, unido a su capacidad de **vigilancia y monitorización de amenazas en tiempo real**, permite a cada Diputación **conocer de forma global el estado y nivel de seguridad de los ayuntamientos y entidades locales de su provincia**, reforzando sus capacidades de defensa frente a las ciberamenazas. Al mismo tiempo, **facilitará la adecuación al ENS de los organismos a los que da servicio**.

Servicios de los SOC Entidades Locales



Adecuación al ENS



Capacitación y sensibilización de profesionales



Seguridad en Ayuntamientos y Diputaciones



Mayor capacidad de correlación de ataques



Mayor visibilidad sobre incidentes



Vigilancia digital de ataques y amenazas



Mejor capacidad de respuesta

PROCESO DE DESPLIEGUE DE UN SOC

Como paso previo al despliegue del SOC, es muy importante que las Diputaciones que lideren el proyecto de despliegue **consoliden y centralicen los Centros de Proceso de Datos (CPDs)** de todas las entidades adheridas, así como la **salida integrada a internet a nivel provincial**.

Como se ha mencionado, **la arquitectura y dimensión es flexible y atiende al tipo de organización en la que se integra**. En este sentido, es importante destacar que la unión de esfuerzos y **la centralización de servicios abarata los costes asociados a su despliegue**, y que este además puede realizarse acorde a las necesidades y partidas presupuestarias del organismo.

Atendiendo a esta idea de mejora continua, se estiman a continuación los costes aproximados de instalación y despliegue de un SOC para Entidades Locales, que centralice y ofrezca servicios de ciberseguridad horizontal a 20 organismos y a un total de 5.000 usuarios.



Centraliza y ofrece servicios de ciberseguridad horizontal a un máximo de **20 organismos***



Cubre la ciberseguridad de los puestos de trabajo de **5.000 usuarios**

Servicios iniciales

Servicios avanzados



Tipo de servicios

- Auditoria inicial
- Revisión
- Formación de equipo de seguridad
- Instalación de soluciones y SW de defensa
- Apoyo para la adecuación al ENS
- Equipo de búsqueda de incidentes de seguridad
- Instalación de solución específica de protección contra el ransomware

Servicios del SOC Inicial

+

- Implementación de listas blancas
- Auditorías recursivas y de código
- Instalación de herramienta avanzada de detección anomalías en equipos de usuario
- Servicio de monitorización de los sistemas
 - Vigilancia digital
- Apoyo a la implementación del ENS

€

Coste aproximado y orientativo de instalación

600.000 €

1.000.000 €

€

Coste servicio anual

150.000 €

250.000 €

* El coste asociado a cada SOC no varía en función del número de organismos al que dé servicio. Es decir, dar servicios de ciberseguridad a 20 organismos tendría un coste similar que ofrecerlo solo a dos.

APORTACIÓN DEL CCN A LOS SOC

El CCN, en el desarrollo de sus funciones de capacitación del sector público en materias de ciberseguridad, pone a disposición de los SOC de entidades locales además de sus conocimientos y asesoramiento, todas sus **soluciones de ciberseguridad**. En concreto, las principalmente utilizadas en el proyecto son las siguientes:



Herramienta de inteligencia y análisis de información sobre ciberameanzas.



Herramienta de gestión y notificación de ciberincidentes, desarrollada por el CCN para automatizar la notificación, comunicación e intercambio de información sobre incidentes.



Herramienta que proporciona protección frente a amenazas de tipo ransomware. Mediante el despliegue de vacunas, con microCLAUDIA se impide la infección de los equipos.



Servicio desarrollado e implantado por el CCN-CERT para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico que fluye entre la red interna del Organismo adscrito e Internet.

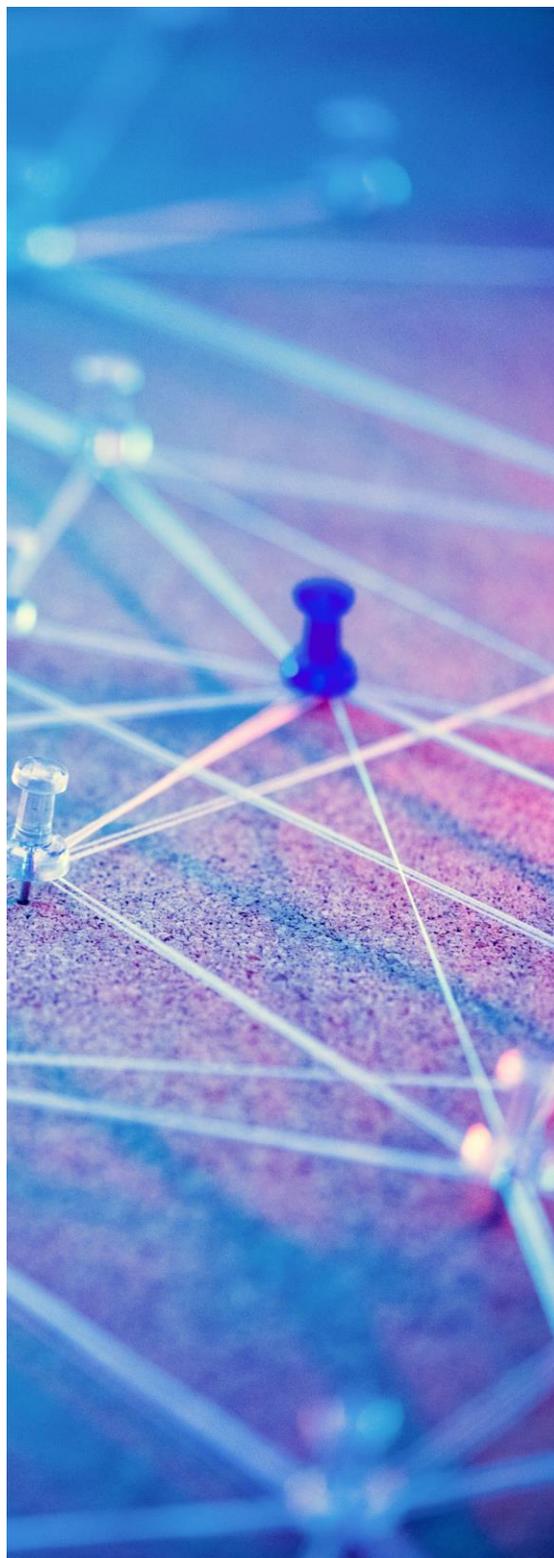
RED NACIONAL DE SOCs

Ante el actual escenario ciberamenazas, y dado el alcance y el nivel de protección que un SOC otorga a la ciberseguridad de una organización, el Centro Criptológico Nacional está impulsando la implantación de estos Centros en el sector público español. **Todos los Centros de Operaciones de Ciberseguridad que se desplieguen en este ámbito formarán parte de la Red Nacional de Centros de Operaciones de Ciberseguridad**, en la que el Centro Criptológico Nacional ya está trabajando, que **integrará a una amplia tipología de SOCs**, como son el de la AGE y los SOC Entidades Locales, autonómicos, sectoriales, ministeriales, autonómicos y privados del ámbito nacional.

La coordinación de todos los SOCs integrados en esta red nacional se llevará a cabo a través de la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes**, que mejorará la gestión de ciberincidentes, el intercambio de información sobre ciberamenazas, las capacidades de análisis de muestras y la notificación de vulnerabilidades, así como las capacidades de intercambio masivo de datos, favoreciendo la gestión continua de la ciberseguridad.



Los SOC de entidades públicas, para su integración en la Red Nacional de SOC, es condición ineludible que reporten los incidentes a través de la herramienta **LUCIA**.



ANEXO: CASOS DE ÉXITO DESTACADOS

COMUNIDAD VALENCIANA – DIPUTACIÓN DE VALENCIA



El Centro Criptológico Nacional ha coordinado la **implementación y operación de diversos Centros de Operaciones de Ciberseguridad en el sector público**, entre los que cabe destacar el **SOC virtual del Cabildo de Tenerife y el de la Diputación de Valencia**.

En el caso de la Diputación de Valencia, el CCN está colaborando en la puesta en marcha del proyecto SOC virtual para el cumplimiento del Esquema Nacional de Seguridad por las Entidades Locales de la provincia de Valencia, diseñado para ayudar a los ayuntamientos en el cumplimiento del ENS, en especial con aquellas medidas que implican vigilancia de seguridad de su infraestructura, así como la recolección, análisis y almacenamiento de registros y actividad de red, activos críticos, y gestión y notificación de incidentes.

El proyecto vSOC está diseñado para gestionar **desde un único centro de operaciones de ciberseguridad, gestionado por la infraestructuras de servicio de CSIRT-CV, la seguridad de los ayuntamientos**.

El despliegue de este SOC ha conestado de dos fases. La primera aplica a unos pocos ayuntamientos seleccionados en base a su tamaño y características técnicas de su infraestructura y, en bases a los resultados de esta fase, en una segunda fase se extiende el proyecto al resto ayuntamientos de la provincia que se acojan a este proyecto.

Este proyecto se basa en la colaboración entre el CCN-CERT que aporta las herramientas y el soporte; el CSIRT-CV, que integra las fuentes y opera el SOC y la Diputación de Valencia que coordina la integración de las entidades locales al proyecto.



ANEXO: CASOS DE ÉXITO DESTACADOS



CABILDO DE TENERIFE

En el Cabildo de Tenerife, el CCN ha formalizado un convenio de colaboración con este organismo con el objetivo de:

Actuaciones de **intercambio de información técnica** en materia de seguridad de los sistemas, servicios y redes en los siguientes campos.

Actuaciones de **promoción del desarrollo de herramientas** de seguridad y programas específicos.

Actuaciones de **implementación y funcionamiento de un Centro Virtual de Operaciones de Ciberseguridad (vSOC)** que aumente de forma significativa las capacidades actuales de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones de las entidades adheridas, así como la mejora de su capacidad de respuesta ante cualquier ataque.

Actuaciones para la **adecuación y certificación con el Esquema Nacional de Seguridad**.

El despliegue se realiza en dos fases, una primera fase con 5 Ayuntamientos y el Cabildo, que se extenderá en una segunda fase a 12 ayuntamientos.

FASE 1

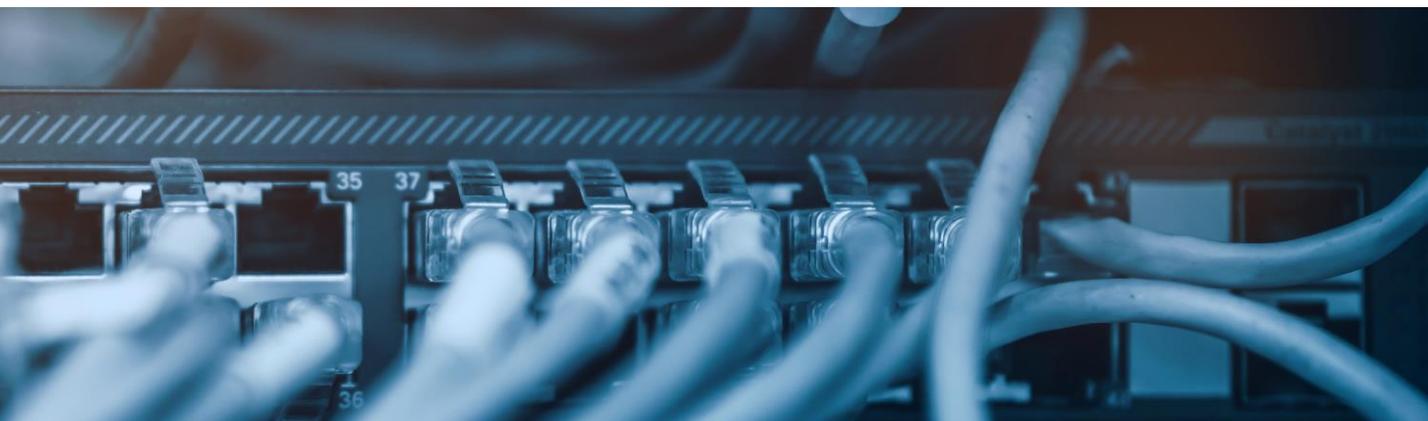
5 + CABILDO

Ayuntamientos

FASE 2

12

Ayuntamientos



ANEXO: CASOS DE ÉXITO DESTACADOS

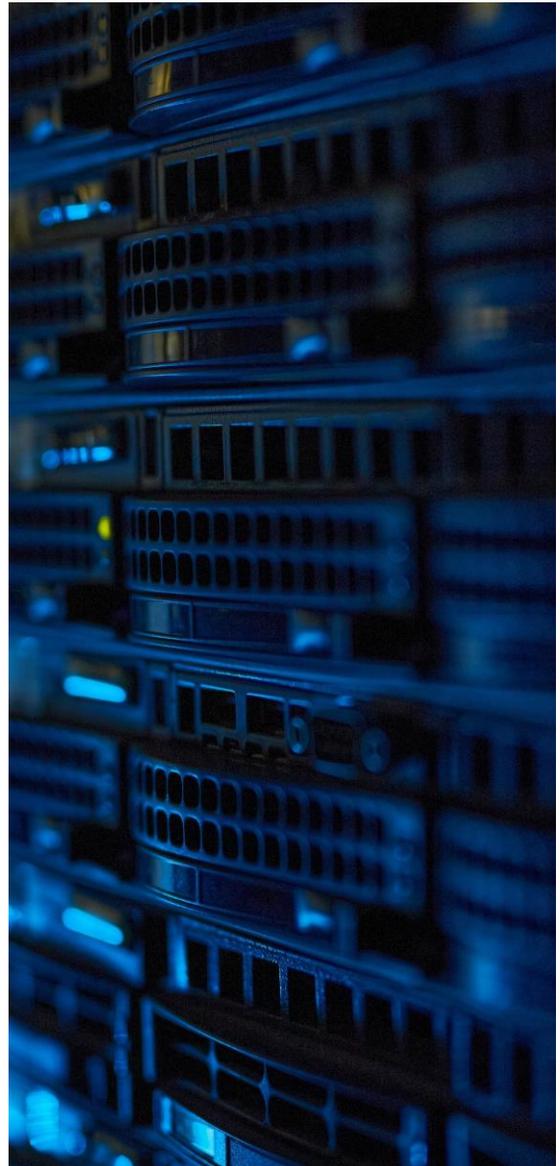


DIPUTACIÓN DE CÓRDOBA

La Diputación de Córdoba inició hace dos años una **consolidación de los Centros de Protección de Datos (CPDs)** de los ayuntamientos, ofreciendo una **salida agregada a internet para todas las entidades locales de la provincia**. Esta acción ha supuesto un **ahorro de costes** y una facilidad en la **implementación de medidas de ciberseguridad**.

Con esta arquitectura ofrecer servicios horizontales de ciberseguridad es mucho más sencillo. En el caso de los servicios del CCN-CERT, **el Sistema de Alerta Temprana (SAT) puede dar cobertura a todos los ayuntamientos de la provincia**.

EPRINSA, empresa provincial de informática que ofrece asistencia a las Administraciones Locales de la provincia de Córdoba, **ha contribuido de manera significativa a la ciberseguridad de todos sus ayuntamientos atendidos, mediante la prestación de servicios horizontales proporcionados desde el SOC**.





PROMOCIÓN DE CENTROS DE OPERACIONES DE CIBERSEGURIDAD EN ENTIDADES LOCALES



Contacto: ccn@cni.es

