MEMORIA FINAL DE PROYECTO

PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA

ORDEN TER/1204/2021 SUBVENCIONES DESTINADAS A LA TRANSFORMACIÓN DIGITAL Y MODERNIZACIÓN DE LAS ADMINISTRACIONES DE LAS ENTIDADES LOCALES, (COMPONENTE 11. INVERSIÓN 3).

Ayuntamiento de Rivas-Vaciamadrid

Centro de Operaciones de Ciberseguridad

Contenido

1. INFORMACIÓN GENERAL

DATOS GENERALES	
Nombre de la entidad	AYUNTAMIENTO DE RIVAS VACIAMADRID
Título del Proyecto	CENTRO DE OPERACIONES DE CIBERSEGURIDAD
Línea estratégica	LÍNEA 5 CIBERSEGURIDAD
Nº de expediente	362-512217_LÍNEA 5
Periodo de ejecución del proyecto	junio 2022 - febrero 2023
DENOMINACIÓN DEL PROYECTO Y LÍNEA ESTRATÉGICA DE LAS ACTUACIONES	
Denominación del proyecto	Proyecto de mejora de los sistemas de Ciberseguridad del Ayuntamiento de Rivas
Línea estratégica de las actuaciones	Línea 5. CIBERSEGURIDAD. Componente 11.I3

2. RESUMEN DEL PROYECTO

El Centro de Operaciones de Ciberseguridad (SOC) suministrado al Ayuntamiento de Rivas Vaciamadrid cumple con el objetivo de realizar un análisis y un seguimiento en redes, servidores, bases de datos, aplicaciones, sitios web y otros sistemas de información municipales, buscando actividades anómalas que puedan ser indicativas de amenazas de ciberseguridad, de modo que dicha información es recogida para aplicar medidas correctivas y poder informar a la red nacional de SOC (RNS).

Para ello, en base a los requerimientos red y sistemas de información del Ayuntamiento, se ha implementado como solución esencial la plataforma MonICA Next Generation SIEM como sistema automatizado de gestión de información y eventos de seguridad, incluyendo 16 licencias para monitorizar las diversas fuentes (sistemas y servidores de aplicaciones) requeridas.

Adicionalmente, se ha complementado con la instalación de dos sondas BoxICA para el análisis de tráfico de red y detección de intrusiones o anomalías del mismo en tiempo real, integradas ambas sondas con el SIEM, al que redirigen la información crítica.

Por último, se configuran las herramientas micro-Claudia de protección contra código dañino, SAT-iNET como sistema de alerta temprana de internet, y Lucía para la notificación de incidentes, todas ellas requeridas por el Centro Criptológico Nacional (CCN-CERT) para poder solicitar la inclusión del SOC en la Red Nacional de SOC (RNS).

3. MEMORIA DE LA ACTUACIÓN

Teniendo en cuenta las características de su memoria técnica y siguiendo las pautas del correspondiente resumen ejecutivo, con fecha de publicación del Pliego de Prescripciones Técnicas (PPT) 05/09/2022, el Ayuntamiento de Rivas Vaciamadrid, inició un proceso de licitación del suministro de toda la actuación del SOC según el lote 2 del PPT, con el expediente de contratación nº 21790/2022:

PLATAFORMA DE ADMINISTRACIÓN ELECTRÓNICA CON ASISTENTE VIRTUAL INTELIGENTE DE ATENCIÓN AL CIUDADANO Y CENTRO DE OPERACIONES DE CIBERSEGURIDAD

Dicho lote 2, fue adjudicado a la empresa ICA SISTEMAS DE SEGURIDAD, S.L. con fecha 03/11/2022 por un importe de 88.454,73€ IVA No incluido, y la recepción del suministro del SOC fue realizada con fecha 16/12/2022. El pago fue realizado el 23/02/2023.

3.1 Descripción del proceso de implementación de las actividades:

Para la puesta en marcha del SOC de una forma segura y ordenada, se planificaron las actividades o tareas siguiendo un programa que cumplía las siguientes fases:

- Estudio de la implantación
- Implantación de las herramientas
- Transición y puesta en marcha
- Prestación del servicio

Durante la fase de Estudio de implantación, se identificaron los procesos y procedimientos que en función de la arquitectura de los sistemas del Ayuntamiento, produjeron un diseño de implementación en el que se ordenaron en el tiempo las herramientas fundamentales a implementar:

1º Plataforma SIEM MonICA
2º Sondas NDR BoxICA
3º Herramientas CCN-CERT

En la fase de implantación se determinó la instalación de la plataforma SIEM MonICA y una configuración inicial de las dos sondas virtualizadas BoxICA contratadas que permitieron el arranque de la ingesta de datos y el arranque del vSOC. En paralelo se iniciaron los trámites de solicitud de las herramientas al CCN-CERT.

Toda vez que la instalación de la plataforma y de las sondas fue acabada se inició la fase de transición y puesta en marcha en la que se reubicaron las sondas en modo On-premises en determinados segmentos de red para una primera optimización de su rendimiento y se instalaron de forma progresiva, micro-Claudia, SAT-iNET y Lucia.

Finalmente, la fase de prestación de servicio contratada contempla una garantía que incluye el servicio de soporte con la Operación del CiberSOC en horario 7 horas x 5 días, hasta diciembre de 2023 para la mejora continua del servicio en el marco del contrato.

3.2 Estado final de cada una de las actividades, resultados obtenidos:

Estudio de implantación: se determinan las fuentes a integrar en el SIEM, la modalidad de configuración de las dos sondas NDR y la planificación de la integración posterior del SOC en la red nacional de SOC. Queda definido el orden de implementación de las herramientas.

Implantación de las herramientas: se instala la plataforma MonICA SIEM, las sondas NDR y las herramientas del CCN-CERT. Como resultado se obtiene un informe ejecutivo mensual con la relación de incidentes desde el mes diciembre de 2022.

Transición y puesta en marcha: se reubican las sondas para su mejor rendimiento, se instalan y configuran micro-Claudia, SAT-iNET y Lucia.

Prestación del servicio: se dispone de la herramienta iTop como sistema con acceso vía web de gestión de peticiones e incidencias.

3.3 Hitos y objetivos alcanzados:

En relación con los objetivos concretos del proyecto el SOC contribuye a que el Ayuntamiento de Rivas Vaciamadrid pueda:

- Garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales que presta el Ayuntamiento y mejorar su capacidad de prevención, detección y respuesta ante ataques o incidentes de seguridad.
- Contar con un sistema de seguimiento que permite la monitorización de los sistemas.
- Integrar todas las herramientas para poder compartir con otras administraciones públicas integradas en la RNS toda la información relativa a incidentes de seguridad que pueda ayudar a prevenir y evitar ataques.
- Mejorar la protección de la información tratada y almacenada en el conjunto de sistemas de información del Ayuntamiento.
- Proteger la continuidad de los servicios digitales que se prestan a la ciudadanía desde el ayuntamiento.
- Proteger y garantizar la normal actividad municipal.
- Capacitar a los técnicos informáticos en materia de ciberseguridad, en particular para corregir fallos de configuración, prevenir y/o subsanar incidentes.

Según la línea de actuación 5 Ciberseguridad , el SOC contribuye a los siguientes hitos y objetivos críticos del Componente 11, medida de Inversión 03, Proyecto 01, y Subproyecto 46 del PRTR:

Hitos:
C11.I03.P01.S46.HTC01 - 167 Digitalización de las Entidades Regionales y Locales.
C11.I03.P01.S46.HTC02 - 169 Finalización de todos los proyectos de apoyo a la transformación digital del Ministerio de Política Territorial y Función Pública y de las Administraciones de las Comunidades Autónomas y de los Entes Locales.
Objetivos:
C11.I03.P01.S46.OBC01 -168 Adjudicación de proyectos de apoyo a la transformación digital del Ministerio de Política Territorial y Función Pública y de las Administraciones de las Comunidades Autónomas y de los Entes Locales.

Digitalización de la Entidad Local (hito nº 167)

Para contribuir al cumplimiento del hito número 167 recogido en el Anexo de la Propuesta de Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del plan de recuperación y resiliencia de España, el Ayuntamiento de Rivas-Vaciamadrid perteneciente a la Comunidad Autónoma de Comunidad de Madrid ha completado el presente proyecto dentro de la línea estratégica 5. Ciberseguridad. En particular, el Centro de Operaciones de Ciberseguridad permite reforzar la ciberseguridad municipal y reducir los riesgos a los que nos enfrentamos en la actividad normal y prestación de servicios digitales al ciudadano. Además, el establecimiento de una red compartida de información a través de la Red Nacional de Centros de Operaciones de Ciberseguridad beneficiará al conjunto de Administraciones Públicas en su defensa contra ciberataques.

Adjudicación de proyectos de apoyo a la transformación digital de los Entes Locales (objetivo nº 168)

En línea con el objetivo número 168 relativo a la adjudicación de proyectos de apoyo a la transformación digital, era intención de este Ayuntamiento proceder a la licitación y consiguiente publicación en la Plataforma de Contratos del Sector Público de la adjudicación del contrato relativo al proyecto de ciberseguridad (vSOC) consistente en la implantación de un Centro de Operaciones de Ciberseguridad y su integración en la Red Nacional de Centros de Operaciones de Ciberseguridad, antes de finalizar el segundo trimestre de 2022, sin embargo la publicación de esta licitación se realizó durante el tercer trimestre de 2022, concretamente el 05/09/2022.

Finalización de todos los proyectos de apoyo a la transformación digital de los Entes Locales (hito nº 169)

En línea con el objetivo nº 168 se dispone de la plataforma de ciberseguridad objeto del proyecto implementada y operativa en el cuarto trimestre de 2022. Concretamente, desde el día 16 de diciembre de 2022.

3.4 Desviaciones de las actividades respecto a la previsión inicial y posibles modificaciones de las actividades aprobadas durante la ejecución del proyecto:

Para el cumplimiento del hito 168 se acomete una reducción del tiempo asignado a la tareas incluidas en las dos primeras fases de implementación inicialmente planificadas, cuya duración prevista hasta el suministro de SOC adquirido era de 40 días naturales.

Concretamente, fue posible reducir la duración de cada una de estas fases en un 25%. Por los que la recepción del suministro del SOC (plataforma SIEM y las dos sondas) contratado pudo ser realizada el 16/12/2022.

4. MEMORIA ECONÓMICA

4.1 Relación clasificada de los gastos e inversiones de la actividad:

Todos los gastos e inversiones de la actividad están incluidos en el proyecto del suministro del SOC, lote 2 del expediente de contratación 21790/2022, por un valor de 88.454,73€ IVA NO INCLUIDO.
El presupuesto total de la actuación El coste total elegible

Ver *anexo I Económico*

4.2 Desviaciones económicas respecto a la previsión inicial y a las posibles modificaciones económicas aprobadas durante la ejecución del proyecto:

Según el presupuesto contemplado en la memoria inicial, en la solicitud se realizó la financiación del 100% del coste del proyecto, incluido el IVA por no ser repercutible y estando todas las actuaciones e importes del mismo limitados a los aspectos subvencionables recogidos en la Orden TER/1204/2021 de 3 de noviembre, por lo que el coste subvencionable para el que se solicitó la financiación fué de 67.686,00€, coincidiendo este importe con el de valor de concesión, según la Resolución de concesión de ayudas Orden TER/1204/2021.

Al iniciar el proceso de licitación en el segundo trimestre de 2022, tras la publicación de la concesión de las ayudas se decidió aumentar la dotación económica del Ayuntamiento de Rivas Vaciamadrid al proyecto, por valor de importe de 18.593,47€ IVA no incluido, por lo que el importe de licitación se incrementó hasta los 109.214,52€ IVA incluido.

Resultó finalmente un importe de adjudicación de 107.030,22€ IVA Incluido, de los que 67.686,00€ constituyen los Costes elegibles de la actuación, 20.768,73€ son los Costes no elegibles de la actuación y los 18,575,49€ restantes son el IVA correspondiente.

5. REPORTAJE FOTOGRÁFICO

Panel de control de la herramienta MonICA NGSIEM virtual

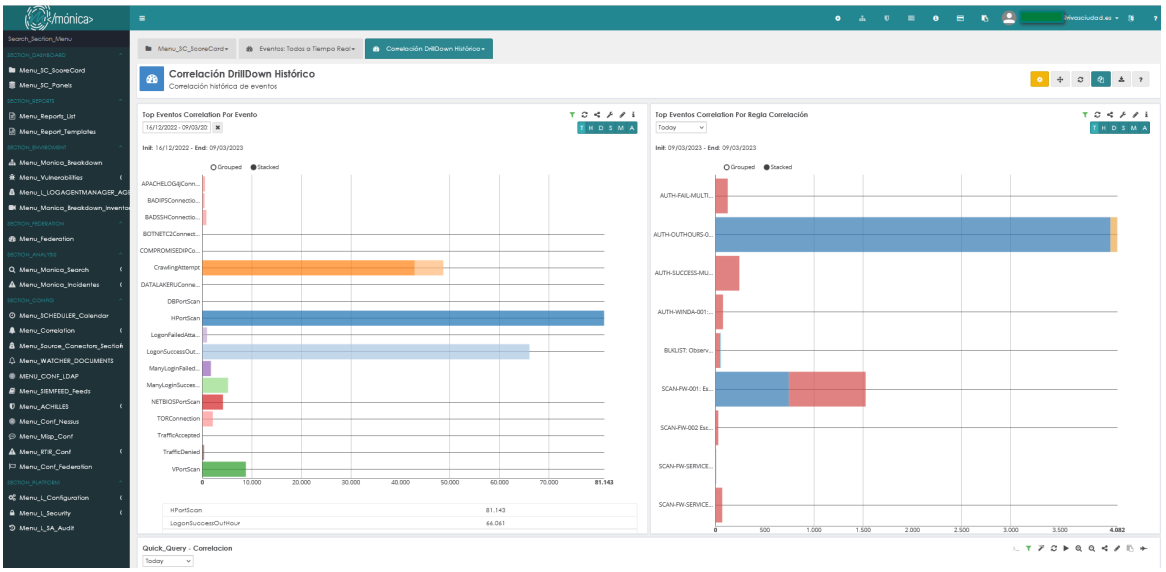

Figura 1: Muestra de ejemplo : Histórico de correlación de eventos.

Interface de las dos sondas BoxICA

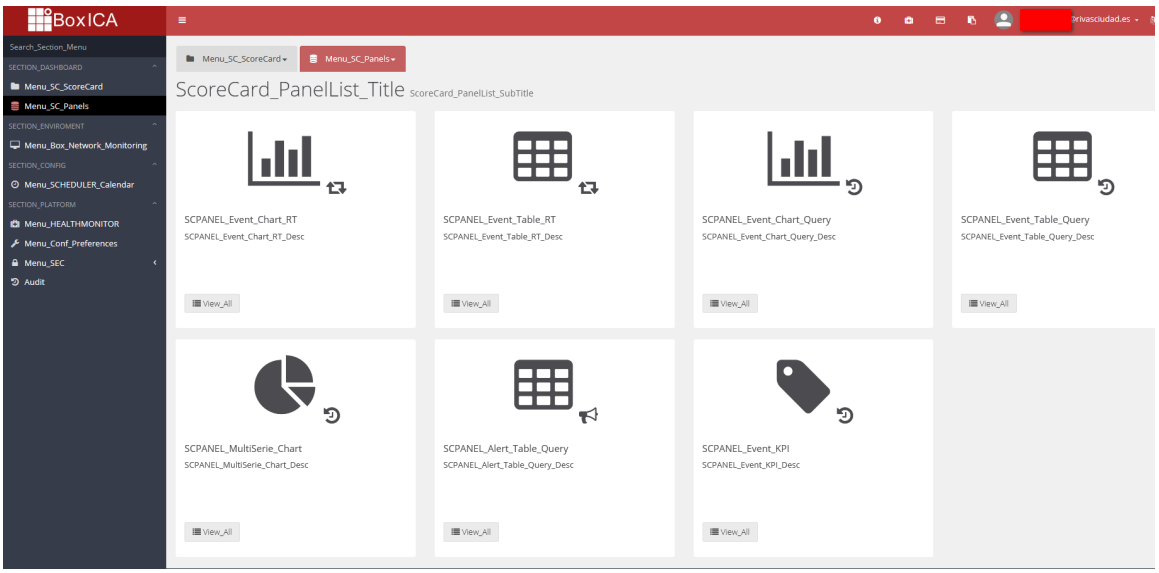

Figura 2: Menús de vistas por paneles

Integración con herramientas CCN Cert

Figura 3: Fotografía de la interfaz del equipo del NOC de Rivas conectado con el CCN-CERT

Herramienta MicroClaudia

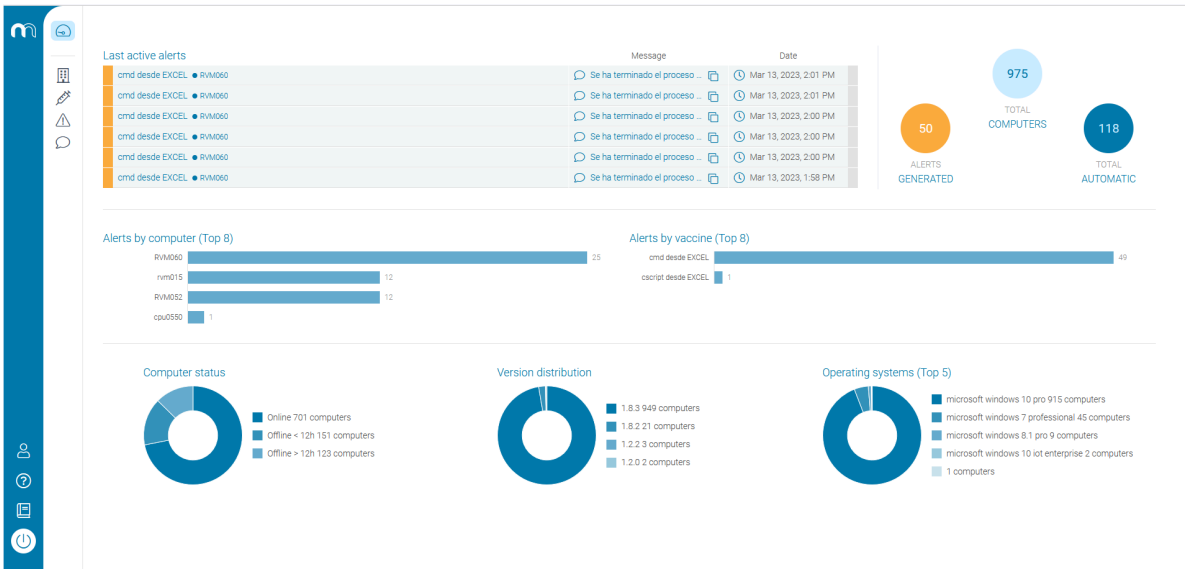

Figura 4 . Informe de alertas

Registro de incidencias y Peticiones

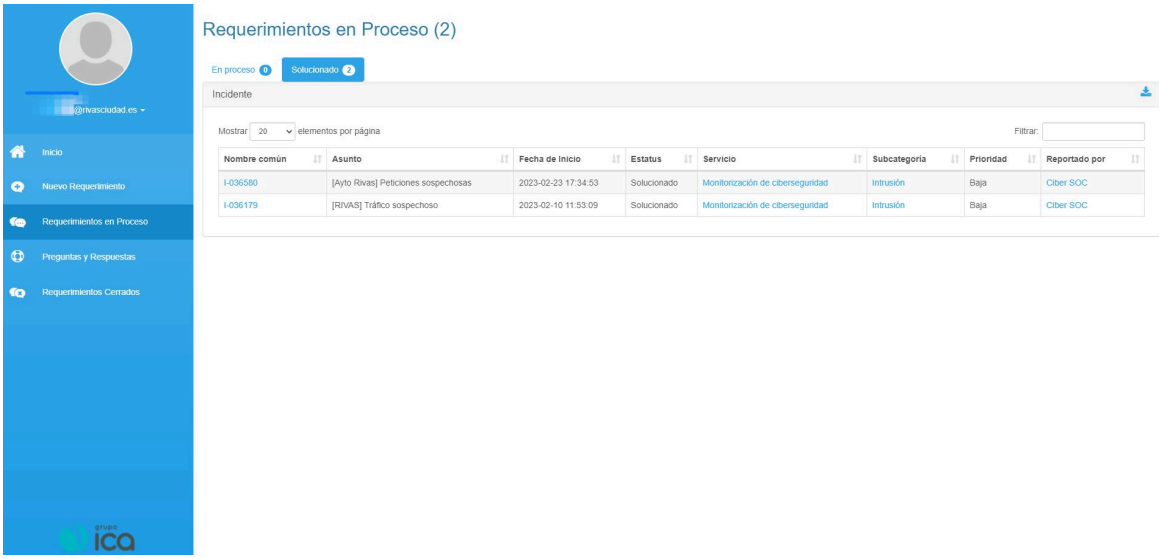

Figura 5: Servicio de requerimientos en proceso.

6. MEDIDAS DE INFORMACIÓN Y PUBLICIDAD

Se ha propuesto al proveedor la implementación del logo conjunto del Ministerio de Política Territorial y de la UE indicado en el inicio del aplicativo. La propuesta está en estudio por el proveedor:

Además de comunicaciones por Redes Sociales y eventos de difusión interna

https://twitter.com/AytoRivas/status/1618240762403254272?s=20

El Técnico Medio de Innovación
El Coordinador de Área de economía y Organización