1.- Nombre de la Administración solicitante del proyecto:

Ayuntamiento de Murcia

2.- Circunscripción de la entidad.

Provincia: Murcia

Comunidad Autónoma: Región de Murcia

3.- Unidad administrativa a la que se circunscribe

Servicio Municipal de Informática

4.- Persona de contacto

Nombre y apellidos: Santiago Domínguez Barrios

Teléfono: 619905880

Correo electrónico: Santiago.Dominguez@ayto-murcia.es

5.- Título del proyecto

Despliegue de un Centro de Operaciones de Ciberseguridad.

6.- Descripción del proyecto (incluir fases y tareas del proyecto)

El proyecto viene como proyecto obligatorio en la Guía de requisitos para proyectos de Entidades Locales del PRTR componente 11, así como la integración en la red nacional de centro de operaciones de ciberseguridad.

El objetivo es garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por esta administración. Este proyecto mejorará nuestra capacidad de prevención, detección y respuesta ante incidentes de ciberseguridad.

Podemos distinguir tres grandes hitos en la estrategia de Ciberseguridad del ayuntamiento de Murcia:

Consultoría de adecuación al ENS.

Despliegue del Centro de Operación de Seguridad: que constituye el objeto del proyecto que presentamos y consiste en el despliegue e implantación de las soluciones de protección, detección y respuesta frente a los ciberataques y del mismo modo las medidas y servicios necesarios para garantizar el correcto funcionamiento y operación 24 horas 7 días a la semana de los mismos para responder ante cualquier incidente.

Podemos distinguir las siguientes fases: una primera hasta el momento de la firma de los contratos pertinentes. En dicha fase se redactarán los pliegos técnicos y se realizan todas las tareas del procedimiento de contratación.

Una segunda fase a partir de la firma de los contratos donde se llevarán a cabo la implantación de los servicios y sistemas de los que consta el proyecto:

Implantación de LUCIA
despliegue de microCLAUDIA

instalación de los cortafuegos de segundo nivel
despliegue del SIEM (y de la oficina correspondiente, no presupuestado)
renovación de la electrónica de red y
realización de actividades de formación y concienciación.

Seguimiento. Donde se realizará la valoración de los resultados obtenidos y se sacarán conclusiones para la evolución de los servicios y sistemas implantados.

7.- Evidencia, análisis y datos que motiven la necesidad del proyecto.

Nos encontramos en un contexto donde la sociedad está expuesta cada vez a un mayor número de ciberataques y de mayor complejidad. La administración local debe garantizar los servicios digitales que se ofrecen a la ciudadanía, protegiendo a su vez la Información tratada directa o indirectamente por medios electrónico.

Es una realidad que, para garantizar y proteger los servicios y la información tratada por éstos, no es posible actuar directamente en ellos, sino que se debe realizar sobre el sistema de información que los soporta. Y esa actuación, en base al riesgo evaluado y a la categorización del sistema, partiendo de la valoración de los servicios y la información, consistirá en aplicar determinadas medidas de seguridad que habrán de permitir reducir el referido riesgo respecto a la seguridad a niveles aceptables.

Por todo lo anterior es imprescindible poder contar en esta Administración con las capacidades de un Centro de Operaciones de Ciberseguridad que nos permita gestionar de forma adecuada la seguridad de nuestras infraestructuras TIC, mejorando nuestras capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad.

Surge además una necesidad normativa al ser necesaria la implantación de un SOC para poder acceder a los fondos Next Generation asignados.

8.- Alineamiento con las prioridades establecidas para los proyectos

PRIORIDADES	Marcar con una X
Prioridad 1. Puesta en marcha de un Centro de Operaciones de Ciberseguridad	X
Prioridad 2. Desarrollo de los tres servicios más utilizados	
Prioridad 3. Puesta en marcha de un proyecto de automatización	
Prioridad 4. Desarrollo o adaptación de servicios exentos de barreras transfronterizas	
No aplica	

9.- Descripción de las actuaciones

Nombre de la actuación y descripción. Se deberá tener en cuenta las tipologías de actuaciones subvencionables para cada línea estratégica de acuerdo con los apartados 6 a 10 de la Guía de requisitos para EELL.

Nombre de la actuación	Descripción
Oficina Técnica	La oficina desde donde se opera el SOC.

	Administra el conjunto de servicios de los que consta el SOC.
SIEM	Todo el SOC se sustenta sobre un sistema de análisis y correlación de eventos de seguridad. Esta actuación consiste en la implantación de dicho instrumento que consta como obligatorio en el requisito d. La implantación requiere también la existencia de la Oficina anterior, bien como servicio, o presencialmente.
MicroCLAUDIA	microCLAUDIA . Herramienta del CCN-CERT que proporciona protección contra código dañino tipo ransomware a los equipos de un organismo.
LUCIA	Herramienta de gestión de incidentes del CCN-CERT que operará en modo federado con el de la plataforma Nacional.
Cortafuegos	En cumplimiento del ENS para separar servidores del resto de la red. En la actualidad sólo tenemos perimetrales.
Electrónica de Red	La red actual es de capa 2 y con la electrónica existente, que tiene una antigüedad de 10 años, no se puede evolucionar hacia una red segmentada en capa 3 que permite una mejor adecuación al ENS.
Actividades de formación y concienciación	Para promover y reforzar la cultura de seguridad de la entidad a través del desarrollo e implementación de un Plan de concienciación y Sensibilización, y formación, en el que se transformarán e interiorizarán comportamientos y hábitos en seguridad en el día a día de los empleados

10.- Descripción de los indicadores asociados al proyecto

Nombre del indicador y descripción. Se deberá tener en cuenta los indicadores para cada línea estratégica de acuerdo con los apartados 6 a 10 de la presente Guía.

Nombre del indicador	**Descripción**
Nº de entidades usuarias del SOC y servicios.	El ayuntamiento de Murcia y sus organismos autónomos (4).
Obtención de la certificación de la conformidad con el ENS	Adecuación de infraestructuras de comunicaciones en conformidad al ENS.
Número de fuentes monitorizadas por SIEM	20

de la infraestructura	
Número de empleados afectados por acciones de formación y concienciación.	2.000

11.- Colectivo objetivo del proyecto

El ayuntamiento de Murcia, sus trabajadores y organismos asociados: Museo Ramón Gaya, Urbamusa.

12.- Implementación del proyecto

El Esquema Nacional de Seguridad está enmarcado en un Sistema de Gestión de Seguridad de la Información (SGSI) de ciclo continuo que refleja el proceso de "Mejora Continua" recogido en el "Art. 26. Mejora continua del proceso de seguridad" del RD 3/2010 (ENS): "*El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.*"

Por lo anterior la metodología y planificación del proyecto debe estar basada en los cuatro pasos del Ciclo de Deming: Plan (Planificar), Do (Ejecutar o hacer), Check (Controlar o verificar) y Act (Actuar para mejora), permitiendo su alineamiento con otras metodologías y sistemas de gestión de la organización:

INICIO: Definición de objetivos y equipo de trabajo. Definir alcance y resultados. Estimación de costos.

PLANIFICACIÓN: Identificación de actuaciones, tareas y plazos de las mismas. Realización de un plan de Recursos, plan de calidad plan de riesgos y plan de Comunicación.

EJECUCIÓN: Durante la ejecución se procederá con la redacción de pliegos, licitación, adjudicación e implementación de los suministros y servicios adquiridos.

SEGUIMIENTO: Revisión y mejora continua.

CIERRE

13.- Distribución anual del coste total estimado del proyecto

El coste total del proyecto se estima en 772.586,01 € más 162.243,06 € de IVA lo que supone un importe total de 934.829,07 €.

Coste total (con IVA)	2020	2021(con IVA)	2022(con IVA)	2023 (con IVA)
934.829,07 €	0€	0€	0€	934.829,07€

14. - Cronograma general del proyecto (nueva previsión a fecha 02/05/23 dados los retrasos acumulados y motivados en el nuevo informe de solicitud de ampliación de esta línea 5 que acompaña a este documento)

Denominación de la tarea	Fecha de inicio	Fecha de finalización
Planificación	01/07/2023	03/07/2023
Suministro e implantación de equipamiento de protección perimetral y red interna (Firewall, electrónica de red)	03/07/2023	31/10/2023
Suministro e implementación de sistema de recolección y correlación de log (SIEM)	03/07/2023	31/10/2023
Implantación de LUCIA	Ya realizado	
Implantación de microCLAUDIA	Ya realizado	
Suministro de plataforma de formación y concienciación	01/07/2023	31/08/2023
Soporte y Gestión de dispositivos y sistemas	01/07/2023	31/10/2023
Monitorización Plataforma SIEM	01/07/2023	31/10/2023

15.- Objetivos que pretende alcanzar

Objetivos del PRTR (marcar con una X)	Descripción de cómo desarrolla el proyecto los objetivos señalados
Obj 1 Promueve la cohesión económica, social y territorial de la UE (x)	Aquellos instrumentos necesarios para el despliegue de la administración electrónica y demás herramientas que promuevan la cohesión económica social y territorial de la UE, de forma indirecta están facilitando el alcanzar dichos objetivos. El hecho de que se desarrollen actuaciones encaminadas a mejorar la adecuación al Esquema Nacional de Seguridad (ENS), mejorando la ciberseguridad de las redes y sistemas de información manejados por las Administraciones Públicas locales, para una mejor protección de la información tratada y de los servicios digitales prestados, es clave para la atención del ciudadano, ayudando de manera indirecta a la cohesión económica, social y territorial
Obj 2 Fortalecer la resiliencia y la capacidad de ajuste de los Estados Miembros (x)	Vivimos en un momento de exposición cada vez más intensa a la materialización de amenazas del ciberespacio, a los ciberincidentes, que siguen una pauta de crecimiento en frecuencia, sofisticación, alcance y severidad del impacto, por eso las inversiones en esta línea enfocadas a mejorar la ciberseguridad fortalecen la resilencia

	y la capacidad de ajuste de los estados miembros.
Obj 3. Mitigar las repercusiones sociales y económicas de la crisis de la COVID-19 ()	
Obj 4. Apoya las transiciones ecológica y digital (x)	Mejorar la ciberseguridad de las redes y sistemas de información manejados por las Administraciones Públicas locales, para una mejor protección de la información tratada y de los servicios digitales prestados, es necesario basarlo en redes de alta capacidad, como la FTTH (un 85% más eficiente que el cobre) y el 5G (un 90% más eficiente que el 4G), y esto está ligado indirectamente con el impulso a la transición verde. Todas las actuaciones llevadas a cabo basadas en esta línea estratégica, y encaminadas a mejorar la adecuación al Esquema Nacional de Seguridad (ENS) por parte de las Administraciones Públicas locales, es ya en sí un claro impulso a la transición digital marcada por el PRTR.
Objetivos del Componente 11 del PRTR (marcar con una X()	Descripción de cómo desarrolla el proyecto los objetivos señalados
Obj 1. Mejora la accesibilidad de los servicios públicos digitales a los ciudadanos y empresas (x)	La mejora de la ciberseguridad hará que los servicios digitales que prestamos no sufran caídas inesperadas o se tengan que paralizar servicios por tiempo indefinido debido a un ataque a nuestros sistemas.
Obj 2. Reduce la brecha digital ()	
Obj 3. Mejora la eficiencia y eficacia de los empleados públicos (x)	El impedir que nuestros sistemas de información sean atacados o impedir la paralización de los servicios prestados claramente mejoran la eficiencia y eficacia de los empleados públicos.
Obj 4. Reutiliza los servicios y soluciones digitales construidas (x)	En este proyecto ya utiliza soluciones desarrolladas por el CCN-CERT. Adicionalmente este proyecto en la medida de lo posible cumplirá con la obligación de ceder los desarrollos que se hagan para que éstos se puedan replicar en otros sitios, en línea con lo marcado En el Plan de Digitalización de las Administraciones Públicas 2021 -2025, con el objetivo de maximizar el retorno de las inversiones y democratizar el acceso a la tecnología a lo largo de todo el territorio nacional.

16.- Objetivos del plan de digitalización de las AAPP (PDAP)

Objetivos del PDAP (marcar con una X)	Descripción de cómo desarrolla el proyecto los objetivos señalados
Obj 1. Incrementar el número de procedimientos digitales ()	
Obj 2. Incremento del número de servicios públicos para implementar en app ()	

Objetivos del Eje 3 del PDAP (marcar con una X)	Descripción de cómo desarrolla el proyecto los objetivos señalados
Obj 1. Administración Orientada a la ciudadanía ()	
Obj 2. Automatización inteligente de procesos ()	
Obj 3. Transparencia y política basada en datos ()	
Obj 4. Entornos Digitales Líquidos ()	
Obj 5. Ciberseguridad (X)	El proyecto consiste en la implantación de un SOC en el ayuntamiento que es el elemento fundamental en el mundo de la Ciberseguridad. De hecho, se pide como obligatorio en este eje por lo que desarrolla los objetivos señalados plenamente.

17.- Alineamiento con los hitos y objetivos del componente 11.I3 del PRTR

Se trata de un proyecto de carácter horizontal, absolutamente fundamental que se posiciona como facilitador de la ejecución de todos los elementos del componente 11 del PRTR.

Propuesta de Objetivos	Descripción
Ciberseguridad	Garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por las Administraciones Públicas regionales y locales. En esta línea pueden recogerse los servicios de seguridad destinados a proporcionar protección a la Administración regional y/o local correspondiente y mejorar sus capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad.
Propuesta de Hitos	Descripción
Digitalización de las Entidades Regionales y Locales:	Completar proyectos dentro de las líneas estratégicas de la Estrategia Digital 2025 y el Plan de Digitalización de la Administración Pública. En particular en la línea estratégica 5. Ciberseguridad.