PLIEGO DE PRESCRIPCIONES TÉCNICAS

DEL CONTRATO DE SERVICIOS

“DISEÑO, IMPLANTACIÓN Y DESPLIEGUE

DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

EN EL AYUNTAMIENTO DE PAMPLONA”,

EN EL MARCO DEL PRTR

1.- INTRODUCCIÓN

El constante aumento de los ciberataques, unido a las posibles consecuencias que para el Ayuntamiento de Pamplona tendría que un incidente de seguridad afectase a sus sistemas, conlleva la necesidad de incrementar y mejorar las capacidades de prevención, monitorización, vigilancia y respuesta.

Con este contrato se pretende implantar una serie de herramientas que el CCN-CERT pone a disposición de las administraciones públicas con el fin de mejorar la seguridad de las infraestructuras, comunicaciones, así como de los servicios digitales que el Ayuntamiento de Pamplona presta, mejorando con ello la capacidad de reacción ante incidentes de seguridad y la disponibilidad de los servicios municipales, dotándole de una mayor capacidad en la detección y respuesta ante sus compromisos de ciberseguridad.

Este proyecto pretende poner en marcha un Centro de Operaciones de Seguridad (en adelante SOC) en el Ayuntamiento de Pamplona dentro del marco del Plan de Recuperación, Transformación y Resiliencia y las ayudas Next Generation de la Unión Europea.

Este proyecto está vinculado a la Línea Estratégica 5: Ciberseguridad, con el objetivo de garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por el Ayuntamiento de Pamplona y mejorar sus capacidades de prevención, detección y respuesta ante incidentes de seguridad. Este proyecto cubre la Prioridad 1 establecida en la Orden TER/1204/2021, de 3 de noviembre, por la que se aprobaron las bases reguladoras de subvenciones destinadas a la transformación digital y modernización de las Administraciones de las Entidades Locales.

2.- ANTECEDENTES

La Asociación Navarra de Informática Municipal (ANIMSA) actúa como departamento TIC del Ayuntamiento de Pamplona y dispone de dos certificaciones en ENS, obtenidas en 2019 y renovadas en 2021, que son:

- *Sistema de Información de la Asociación Navarra de Informática Municipal S.A. (ANIMSA), asociado a los procesos de diseño, desarrollo, instalación, administración de sistemas, mantenimiento y soporte técnico, implicados en los servicios corporativos de ANIMSA.*
- *Sistema de Información de la Asociación Navarra de Informática Municipal S.A. (ANIMSA), asociado a los procesos de diseño, desarrollo, instalación, administración de sistemas, mantenimiento y soporte técnico, implicados en los servicios de la Nube Privada proporcionados por ANIMSA a las Entidades Locales.*

Asimismo, ANIMSA tiene un acuerdo de colaboración con el Centro Criptológico Nacional (en adelante CCN), que viene desarrollándose desde el año 2020, con el que están llevando a cabo trabajos de adecuación al ENS en Entidades menores. Se tiene establecida la estructura de un marco de gobernanza que coordina los diferentes actores de seguridad u órganos relacionados con la ciberseguridad. Se asumen funciones de asesoría legal y operativa en materia de ENS, Protección de Datos y otras regulaciones del entorno de la seguridad de las TIC, la resiliencia y la privacidad. Y es la unidad encargada de impulsar y asesorar a las Entidades en el proceso de adecuación al Esquema Nacional de Seguridad en cumplimiento con lo dispuesto en la norma que lo regula.

ANIMSA desea dar un tratamiento homogéneo a la ciberseguridad en todos sus ámbitos de actuación: Ayuntamiento de Pamplona, Ayuntamientos menores y en su propia organización. Para ello se requerirá el apoyo institucional y económico de la Diputación Foral (o del Gobierno de Navarra por tratarse de una Autonomía uniprovincial) para dar cabida a las Entidades Locales que no están asociadas a ANIMSA.

Para futuros ejercicios las estrategias de desarrollo sostenible deberán estar alineadas de manera coherente con las inversiones, medidas y funciones específicas en esta materia. Adoptar este concepto significará pensar en el papel que la ciberseguridad tiene en la agenda municipal y en cómo debería mejorarse para cubrir las infraestructuras corporativas, así como asegurar que los empleados municipales sigan las prácticas de ciberseguridad adecuadas.

3.- IDENTIFICACIÓN INICIAL DE LOS PROBLEMAS O RETOS DETECTADOS

El SOC del Ayuntamiento de Pamplona formará parte de la Red Nacional de Centros de Operaciones de Ciberseguridad, en la que el CCN ya está trabajando, y que integrará otros Centros de Operaciones de Ciberseguridad de otras administraciones públicas del ámbito nacional para optimizar sus recursos en función de la información manejada y los servicios prestados.

La coordinación de los centros integrados en esta red nacional se llevará a cabo a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, prevista en el artículo 11 del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

A través de este SOC el Ayuntamiento de Pamplona tendrá más visibilidad e información sobre vulnerabilidades, fallos de configuración e incidentes, mayor capacidad de despliegue, protección y actuación, al disponer de una gestión centralizada que permitirá aumentar el número de entidades adscritas a la Red Nacional.

Los servicios a implantar serán:

- Intercambio automático y fluido de ciberincidentes con la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.
- Implantación de las tecnologías necesarias que permitan la vigilancia del perímetro y de la red interna desplegados por el CCN-CERT.
- Monitorización de la herramienta microCLAUDIA del CCN-CERT ya desplegada en toda la organización municipal del Ayuntamiento de Pamplona.
- Capacidad de recolección y correlación básica de los registros de trazabilidad necesarios para la vigilancia.
- Actividades de formación y concienciación en materia de ciberseguridad entre los empleados del Ayuntamiento de Pamplona.

4.- HERRAMIENTAS Y SOLUCIONES QUE DEBERÁN QUEDAR IMPLANTADAS

Se desplegará una solución tecnológica basada en las herramientas del catálogo del CCN-CERT orientadas a la monitorización, detección y gestión de incidentes de seguridad. Las herramientas a implantar son:

- GLORIA para la gestión integral del SOC, con sus capas de recolección de eventos, correlación, gestión y cuadro de mando.
- CARMEN para la búsqueda proactiva de amenazas avanzadas.
- CLAUDIA para la monitorización de actividad en los puestos de usuario y servidores y la alimentación de CARMEN con telemetría derivada de esta monitorización.
- microCLAUDIA para la prevención de infecciones por ransomware mediante la inoculación de vacunas en clientes y servidores.
- LUCIA para la comunicación de incidentes a CSIRT nacional CCN-CERT.

5.- TECNOLOGÍA A UTILIZAR POR HERRAMIENTA

A continuación, se describe la tecnología a utilizar:

5.1.- GLORIA

Las organizaciones, de forma general, disponen de un conjunto de equipamiento, tanto hardware como software, capaz de generar registros de su actividad. El volumen de información global es inmanejable sin una herramienta que ayude a la recolección, normalización, almacenamiento, análisis y correlación de logs, y que permita una reducción muy significativa del volumen de información a tratar finalmente por el personal técnico de la Organización.

GLORIA *(Gestor de LOgs para Respuesta ante Incidentes y Amenazas)* es una plataforma de gestión integral de Centros de Operaciones de Seguridad articulada en torno a una base de datos de configuración (CMDB) y con un modelo de procesamiento basado en el análisis y extracción de la información relevante. Dispone de capacidades de monitorización de seguridad y recolección, inteligencia avanzada mediante técnicas de correlación compleja de eventos o análisis de patrones para la identificación de anomalías, y gestión de los procesos ligados al servicio con una consola única diseñada de acuerdo con las mejores prácticas de ITIL.

El funcionamiento de GLORIA se basa en un proceso de detección, priorización y resolución de eventos. La detección se realiza monitorizando de forma automática los elementos de seguridad. Todos los eventos se categorizan según una estructura definida por la organización y se les asigna una criticidad y nivel de calidad de servicio automáticamente. En función de la categorización del evento, se notifica al área de conocimiento responsable de su resolución. La resolución es la fase intensiva en conocimiento que involucra a los expertos de la organización y a la base de datos de conocimiento del sistema. Se basa pues en un proceso básico de gestión de eventos definido mediante un flujo de trabajo. Este proceso garantiza una gestión correcta de los niveles de calidad de servicio y permite el escalado funcional y jerárquico de los eventos.

Para ofrecer esta funcionalidad, la solución está compuesta por cuatro módulos: argos®, tritón®, emas®, y hera®, cada uno con sus funciones específicas dentro de la solución:

- argos® es el sistema de monitorización y recolección de eventos de seguridad dentro de la arquitectura. Su misión es la monitorización de seguridad del entorno, así como la recolección y normalización de logs.
- tritón® es la plataforma de correlación especializada de eventos recibidos de argos® y otros agentes que son desarrollados ad-hoc cuando las necesidades de la operación de seguridad lo requieren.
- emas® es el núcleo de la plataforma tecnológica, proporciona la consola única de gestión de eventos e incidentes y recoge todas las incidencias o alertas automáticos generados por el sistema de correlación.
- hera® es el cuadro de mando que analiza información en tiempo real y ofrece los indicadores clave del funcionamiento.

De esta forma, mediante las diferentes capas, GLORIA permite cubrir todos los niveles de operación de un SOC, facilitando además la integración sencilla y flexible con soluciones de terceros.

Por otra parte, GLORIA cuenta con capacidades de orquestación y la automatización para mejorar la productividad del SOC. En primer lugar, la automatización permite recoger información monitorizada en tiempo real y a partir de datos de contexto realizar la detección de los incidentes realmente relevantes, realizando una clasificación del incidente y catalogando automáticamente su criticidad gracias a la información de contexto. Además, mediante un proceso de correlación se consigue la agrupación automáticamente de alertas relacionadas, con lo que se reduce el número de eventos a gestionar, permitiendo que los operadores del SOC se centren en lo verdaderamente importante y que un incidente

múltiple sea gestionado de forma agrupada, lo que se traduce en un incremento del porcentaje de verdaderos positivos con respecto al total de eventos detectados.

Adicionalmente, esta detección incluye la generación automática en tiempo real de un informe completo y totalmente contextualizado, ligado al incidente y notificado en LUCIA, que contiene todas las alertas relacionadas, incluyendo las últimas comunicaciones relacionadas con el incidente, información sobre las direcciones IP del organismo afectadas, así como las direcciones externas que han realizado el ataque y la pertenencia a listas negras de dichos atacantes.

De acuerdo con los requisitos de interoperabilidad, GLORIA se integra con otras herramientas del ecosistema del CCN-CERT como CARMEN y CLAUDIA para la detección de amenazas avanzadas, microCLAUDIA para la detección de infecciones por ransomware conocido, LUCIA para la gestión de incidentes del CCN-CERT y REYES para intercambio de información y conocimiento de ciberamenazas.

5.2.- LUCIA

LUCIA supone la interfaz del Ayuntamiento de Pamplona con el CCN-CERT para la declaración y gestión de incidentes de seguridad. Es una herramienta desarrollada por el CCN-CERT especializada en el proceso de gestión de incidentes, diseñada y parametrizada conforme a las directrices de la guía CCN-STIC 817 Gestión de ciberincidentes.

En la arquitectura de GLORIA, emas® se configura como la consola de análisis e investigación de eventos y alertas. Una vez el analista de seguridad confirma el incidente, este es escalado de forma automática a LUCIA para ponerlo en conocimiento del organismo con todo su contexto y así poner en marcha el proceso de remediación.

5.3.- CARMEN

CARMEN (Centro de Análisis de Registros y Minería de EveNtos), es la herramienta para la identificación del compromiso por parte de Amenazas Persistentes Avanzadas (APT), constituyendo la primera herramienta española, basada en conocimiento y tecnología nacionales, con estas capacidades.

Dispone de capacidades para la protección avanzada ante amenazas en la organización vigilada, de forma que tanto los tráficos de red salientes e internos de la organización como los tráficos de red entrantes son adquiridos, procesados y analizados para la defensa de ésta: la existencia de usos indebidos, la detección de anomalías o los intentos de intrusión son identificados, organizados y representados para facilitar el desempeño del equipo de seguridad.

CARMEN aporta capacidades para la detección de la amenaza en la etapa de persistencia, por lo que uno de sus objetivos fundamentales es la identificación de movimientos externos, como filtraciones o comunicaciones con sistemas de comando y movimientos laterales de mantenimiento de persistencia o robo de información en la red corporativa.

Sobre cada una de las fuentes de datos adquiridas, CARMEN permite el análisis automático, semiautomático y manual del tráfico de red de la organización para la detección de usos indebidos y, especialmente, para la detección de anomalías significativas en este tráfico: estadísticas, series temporales, en cadenas de texto o basadas en conocimiento, por ejemplo.

CARMEN adquiere principalmente tráfico de salida a internet de la organización. En concreto, la herramienta está focalizada en la adquisición de los protocolos más habituales para el movimiento externo de una amenaza, tanto en el ámbito de la exfiltración como en el del Command & Control: navegación web, consultas DNS y correo electrónico.

En cada uno de los protocolos considerados, CARMEN presenta capacidades de adquisición pasiva mediante el análisis y extracción del tráfico de red, habitualmente habilitando el uso de port mirroring en la electrónica de red de la organización.

Además, en el caso del tráfico de navegación web, CARMEN dispone de capacidades de integración con los proxy de navegación de la organización mediante la recepción de los registros de navegación tanto en tiempo real, a través de syslog, como en modo offline, mediante la copia periódica de los ficheros de registro de navegación.

En relación a los movimientos laterales de la amenaza, es capaz de adquirir información de los mecanismos más habituales para el mantenimiento de persistencia y el intercambio de información entre sistemas.

Toda la información adquirida de la red, tanto de forma pasiva como mediante la recepción de información de proxy, es normalizada y almacenada para su análisis y procesamiento tanto automático como manual.

Por otra parte, para beneficiarse de la inteligencia generada por todos los despliegues de CARMEN gestionados por el CCN-CERT, la herramienta se integrará con la plataforma CARMEN CENTRAL donde se publican todos los indicadores generados por la Red de Inteligencia Compartida del CCN-CERT.

5.4.- CLAUDIA

Adicionalmente, CARMEN dispone de la capacidad de recolección de información de los puestos de usuario mediante el despliegue de un agente específico denominado CLAUDIA, que permite monitorizar los eventos del registro de eventos de Windows, así como monitorizar directorios, o la existencia de ficheros o de claves de registro.

CLAUDIA ofrece la posibilidad de ejecutar varios sensores que permitirán obtener más información de las máquinas de la red:

- Monitorización de directorios
- Existencia de fichero en ruta determinada
- Existencia de clave de registro

El despliegue de CLAUDIA puede realizarse mediante Directivas de Grupo del Directorio Activo de Microsoft, de forma que puede ser instalado en un amplio parque de equipos de forma fácil y ágil.

Cada uno de agentes desplegados se comunica periódicamente con CARMEN, a través de canales seguros, para actualizar su estado y notificar de situación relevantes desde el punto de vista de seguridad que puedan suponer un riesgo para la organización, por ejemplo:

- Eventos de normativa (perfil Normativa)
  - Controlador de dominio
  - Servidor miembro
- Eventos de seguridad (perfil APT)
  - Microsoft System Monitor

5.5.- microCLAUDIA

Es un agente que proporciona protección contra código dañino de tipo ransomware a los equipos de una organización. Para ello, hace uso de un agente ligero que se encarga del despliegue y ejecución de vacunas.

La conexión del agente al servicio central de microCLAUDIA del CCN-CERT permite descargar y ejecutar las vacunas que el Ayuntamiento de Pamplona haya configurado para sus equipos. Una vez descargadas, el agente no requiere de conectividad a la nube para su ejecución ni de un servicio central o servidor instalado en la organización. Asimismo, el servicio ofrece la actualización automática de las mismas para cubrir adaptaciones a las nuevas formas de ejecución del ransomware.

El despliegue de las vacunas se puede realizar desde cualquier herramienta de gestión de distribución de software o mediante políticas de Windows. Además, no necesita modificaciones adicionales en la red del organismo. Una vacuna es un mecanismo que impide que el malware se ejecute en un equipo. En el caso de microCLAUDIA, estas vacunas se especializan en malware de tipo ransomware.

5.6.- CAPACIDADES INCLUIDAS EN LA PLATAFORMA A DESPLEGAR

Se contempla el despliegue de las siguientes capacidades en cada una de las herramientas descritas:

- Capacidades de recolección de eventos de GLORIA mediante una sonda argos®
    - Monitorización de disponibilidad de la propia plataforma que conforma GLORIA.
    - Análisis de tráfico NIDS
    - Control de integridad HIDS
    - Integración de fuentes de logs en SIEM
- Capacidades de correlación de eventos de GLORIA en el módulo de inteligencia tritón® mediante el uso de reglas de correlación.
- Consola de gestión de eventos de GLORIA, emas®
- Cuadro de mando de GLORIA, hera®, con información de evolución en el volumen de alertas registradas según criticidad o tipología
- Instancia de LUCIA federada con la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes
- Plataforma CARMEN para el análisis proactivo de:
    - Log de navegación (HTTP)
    - DNS
    - SMTP
    - NetBIOS, en particular, Named Pipes y Mail slots
- Agentes de CLAUDIA para el análisis proactivo de la actividad maliciosa en los puestos de usuario y servidores
- Revisión de agentes de microCLAUDIA para la vacunación anti-ransomware de los puestos de usuario y servidores
- Integración con la Red de Inteligencia Compartida del CCN-CERT, CARMEN CENTRAL y REYES

6.- ARQUITECTURA DE LA SOLUCIÓN

La arquitectura consistirá en lo siguiente:

- En el Centro de Proceso de Datos del Ayuntamiento de Pamplona se instalará:
    - Plataforma hardware para albergar los diferentes módulos de GLORIA (argos, tritón, emas, hera) y LUCIA. Los módulos se despliegan en forma de máquinas virtuales y para su instalación de aprovisionarán máquinas físicas con el sistema de virtualización utilizado por el Ayuntamiento. No

se detallan los requisitos mínimos de dichas máquinas virtuales, quedando el dimensionamiento pendiente de las primeras reuniones a desarrollar una vez adjudicado el contrato.

  - Appliance de CARMEN para la monitorización del tráfico de salida a Internet.

- En los puestos de usuario y servidores del Ayuntamiento de Pamplona se desplegarán diferentes tipos de agentes:
  - Agentes de HIDS
  - Agentes de CLAUDIA

  que convivirán con el agente de microCLAUDIA, que ya está funcionando.

Para la operación de la plataforma se emplearán los equipos informáticos de la Asociación Navarra de Informática Municipal (ANIMSA) como departamento TIC municipal, y se habilitará el espacio físico dedicado para el SOC.

7.- PLAN DE IMPLEMENTACIÓN

La metodología propuesta por ANIMSA para desarrollar el contrato es realizar un plan de implementación del proyecto en las fases que se enumeran a continuación, que se planificará de conformidad con la oferta adjudicataria en la celebración de reuniones de inicio de la contratación:

Fase I – Preparación del despliegue

La primera fase de la implantación consistirá en la preparación de los equipos de trabajo y de los entornos y en la realización de una reunión de lanzamiento.

Fase II – Análisis y diseño de la solución

Previo a la instalación de los productos y su configuración, se llevará a cabo una revisión del diseño de la solución definitiva.

Fase III – Despliegue de la solución

Suministro y despliegue inicial de la solución con una configuración básica y con todos los elementos necesarios para dejar el sistema de monitorización totalmente funcional.

Incluirá el despliegue de módulos de GLORIA, LUCIA y CARMEN.

Incluirá el despliegue de agentes de CLAUDIA y la revisión de los agentes desplegados de microCLAUDIA.

Configuración de usuarios, roles y permisos de personal autorizado del SOC en GLORIA.

Fase IV – Integración de fuentes

En esta fase se integrará la captura de eventos y logs de los sistemas generadores de eventos de seguridad, y se realizará un seguimiento tras la integración de las fuentes para comenzar a recopilar eventos e información, donde se identifiquen posibles mejoras y optimizaciones en el sistema.

Fase V – Formación

Se impartirá formación específica a los técnicos que se determinen por parte de ANIMSA para capacitarles en la gestión y administración, tanto de la plataforma de virtualización a implantar y operar, como de aquellas herramientas instaladas y sobre las que el personal deba realizar acciones para mantener la funcionalidad, monitorización, explotación e integración de las 5 herramientas y servicios desplegados.

Esta fase comprende la formación de usuarios y administradores del SOC, con un mínimo de un curso por cada herramienta y un mínimo de 50 horas de formación total, y la entrega de documentación. Se valorará que los licitadores oferten un mayor número de horas de formación.

Fase VI – Soporte técnico

En caso de inconsistencias o incidentes, el Ayuntamiento de Pamplona podrá contar con un nivel mínimo de operación y asistencia por parte del contratista. Así pues, el contratista adjudicatario deberá garantizar el funcionamiento del SOC a del Ayuntamiento de Pamplona en caso de que hubiera alguna incidencia o disfuncionalidad por causa del mal funcionamiento de los servidores instalados por el adjudicatario, su integración con sistemas propios o externos o cualesquiera otros motivos. En cuanto a los productos del CCN, corresponderá al adjudicatario ofrecer íntegramente mediante la documentación pertinente, un Plan de Mantenimiento correctivo, adaptativo y evolutivo de las soluciones y sus derivadas de cara al nivel de funcionalidad operativa.

El adjudicatario prestará un servicio de mantenimiento para asesoramiento y atención especializada, para realización de actualizaciones o requerimientos específicos no derivados del funcionamiento ordinario en base a una bolsa de horas. Dicha bolsa de horas de asistencia y soporte especializado una vez puesto en marcha el SOC en Pamplona tendrá una dimensión mínima de 50 horas anuales. Se valorará que los licitadores oferten un número de horas mayor. Las horas no utilizadas para este fin podrán ser utilizadas para abordar actuaciones orientadas a seguridad como pequeñas auditorías, jornadas de concienciación, análisis específico sobre alguna casuística requerida o necesaria a estudiar, etc.

En caso de no agotarse las horas al finalizar el año, serán trasladadas a la anualidad siguiente. No se podrán imputar sobre esta bolsa de horas de servicios y requerimientos específicos, tareas o trabajos considerados ordinarios y de obligado cumplimiento por parte del contratista, como por ejemplo trabajos de mantenimiento, tareas de revisión o actualización de versiones, resolución de fallos imprevistos, caídas del servicio, etc. Los servicios asociados a la bolsa de horas tendrán que prestarse, como mínimo, de acuerdo con los niveles de servicio definidos en el punto 8 de este pliego. Se podrá hacer uso de estos servicios vía telefónica, correo electrónico o asistencia remota.

8.- NIVELES DE SERVICIO:

Tras la firma del contrato, el Ayuntamiento de Pamplona acordará con el adjudicatario el protocolo de actuación en caso de incidencias en la explotación del sistema. Este protocolo incluirá en todo caso la identificación del personal, tanto comercial como técnico, que harán de interlocutores del servicio de mantenimiento del sistema, así como de la coordinación ante incidencias con la empresa adjudicataria.

Para aquellas incidencias no resueltas dentro del límite temporal acordado en los Niveles de Servicios detallados a continuación, la empresa adjudicataria deberá solucionarla en el menor tiempo posible, independientemente del entorno donde se haya producido ésta.

Se definen los siguientes Acuerdos de Nivel de Servicios:

- Ante la caída o funcionamiento incorrecto de la herramienta LUCIA a causa de una incidencia en el servidor físico o virtual donde están instanciadas estas herramientas, se deberá solucionar la incidencia en un plazo no superior a 72 horas desde la notificación de la misma.
- Ante la caída o mal funcionamiento de la herramienta GLORIA, se deberá solucionar la incidencia en un plazo no superior a 48 horas desde la notificación de la misma.

- En caso de solicitud de una nueva configuración específica o cualquier otro servicio especializado que se solicite en base a la bolsa de horas anual, ésta deberá ser atendida y haberse iniciado el proceso para su resolución en un plazo máximo de 72 horas desde la notificación de la misma.

9.- EQUIPO TÉCNICO

El equipo de trabajo que llevará a cabo el proyecto estará compuesto por al menos 5 profesionales especialistas en seguridad, con los siguientes perfiles:

- **1 Coordinador técnico del proyecto**

  El Coordinador del servicio será el punto de interlocución habitual con los Equipos de Trabajo. Será un consultor con al menos dos años de experiencia en seguridad y la capacitación adecuada a las necesidades particulares de este proyecto.

  Requisitos mínimos de este perfil:

  - Titulación universitaria en Ingeniería de Telecomunicación, Informática o titulación equivalente.
  - Experiencia mínima contrastable de al menos (2) años en coordinación de proyectos similares, además de en servicios de monitorización y gestión de herramientas SIEM y respuesta a incidentes de seguridad, incluyendo la realización de funciones de servicios SOC o análogos y de análisis, priorización, respuesta y acciones para la remediación de incidentes, así como diseño de casos de uso para herramientas SIEM.

- **2 Ingenieros de Seguridad**

  Serán los miembros del equipo técnico encargados de definir la arquitectura y configuración de las plataformas a desplegar. Se encargarán también de llevar a cabo la formación del equipo del SOC.

  Tendrán experiencia en el diseño, despliegue y configuración de todas las herramientas propuestas: LUCIA, GLORIA, CARMEN, CLAUDIA, MICROCLAUDIA.

  Requisitos mínimos de este perfil:

  - Formación Profesional de Grado Medio o Superior en “Informática y Comunicaciones” o “Electricidad y Electrónica” (o equivalente -Ley Orgánica General del Sistema Educativo de 3 de octubre de 1990 o Ley 14/1970 de 4 de agosto General de Educación y Financiamiento de la Reforma Educativa FPI y FPII).
  - Experiencia profesional mínima de (2) años en los servicios relacionados con el objeto del contrato.

- **2 Analistas de Seguridad**

  El equipo de analistas dará soporte y asistirá en la definición de fuentes a integrar, casos de uso y reglas de correlación. Se encargarán también de llevar a cabo la formación del equipo del SOC.

  Los analistas de seguridad tendrán experiencia probada en el despliegue, configuración y operación de las herramientas propuestas: LUCIA, GLORIA, CARMEN, CLAUDIA, MICROCLAUDIA.

  Requisitos mínimos de este perfil:

  - Formación Profesional de Grado Medio o Superior en “Informática y Comunicaciones” o “Electricidad y Electrónica” (o equivalente -Ley Orgánica General del Sistema Educativo de 3 de octubre de 1990 o Ley 14/1970 de 4 de agosto General de Educación y Financiamiento de la Reforma Educativa FPI y FPII).

- Experiencia profesional mínima de (2) años en los servicios relacionados con el objeto del contrato.

Se valorará si se oferta un mayor número de profesionales, así como que cualquiera de los perfiles del equipo de trabajo incluidos en la oferta estén en disposición de:

- Una experiencia superior a dos años en los servicios relacionados con el objeto del contrato.
- Títulos de estudios adicionales a los requeridos como solvencia mínima, que sean específicos de la seguridad de la información, y certificaciones en el ámbito de seguridad de la información que resulten relevantes para el servicio objeto del pliego.

Estos perfiles reportarán al interlocutor nombrado por el Ayuntamiento de Pamplona en ANIMSA para realizar el control interno del proyecto, con el objetivo de garantizar la comunicación y la interlocución con las diferentes partes y asegurar un seguimiento adecuado del proyecto.

10.- CERTIFICACIONES NECESARIAS Y VALORABLES

Las licitadoras deben tener **certificación de empresa o en vías de certificación para operar GLORIA en el sector Público libre de costes de licencias, o equivalente**, como soluciones desarrolladas con el Centro Criptológico Nacional y con experiencia de implantaciones similares en Administraciones Públicas.

Se valorará además que las licitadoras cuenten con otras certificaciones:

- Certificación ISO 9000 o equivalente. Normativa para la Control y Gestión de la Calidad.
- Certificación ISO 20000 o equivalente. Normativa para la Certificación de los Servicios de Gestión y Soporte TI.
- Certificación ISO 27000 o equivalente. Normativa para Auditoría de un Sistema de Gestión de Seguridad de la Información.
- Certificación ISO 22301 o equivalente. Normativa para de Gestión de Continuidad de Negocio.