Pliego de Prescripciones Técnicas para la implantación de un Centro de Operaciones de Seguridad para la Transformación Digital y Modernización del Ayuntamiento de Mérida, en el marco del Plan de Recuperación, Transformación y Resiliencia

Tabla de contenido

1. Suministro de licencias y servicios de despliegue e implantación de un Centro de Operaciones de Seguridad (SOC)

1.1. Objeto del Contrato.

El objeto de este contrato es la implantación de un Centro de Operaciones de Seguridad para la Transformación Digital y Modernización del Ayuntamiento de Mérida, en el marco del Plan de Recuperación, Transformación y Resiliencia, que dé respuesta a las necesidades actuales, de acuerdo con los requerimientos recogidos en este documento.

Las actuaciones previstas se enmarcan del Plan de Recuperación, Transformación y Resiliencia, Financiado por la Unión Europea-NextGenerationEU, Mecanismo de Recuperación y Resiliencia, establecido por el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, para la consecución de resultados, hitos y objetivos indicados definidos en el Componente 11, Inversión 3, dirigida a la transformación digital y modernización de las distintas administraciones públicas, gestionada por el Ministerio de Política Territorial.

En este mismo sentido, los trabajos están alineado con la Estrategia Digital 2025, el Plan de Digitalización de las Administraciones Públicas 2021-2025 y otras acciones de modernización dirigidas al sector público.

El objetivo principal del proyecto es el Alineamiento con la Estrategia Nacional de Ciberseguridad que implicará:

- Seguridad y resiliencia de las redes y sistemas de información y comunicaciones del Ayuntamiento y de sus servicios esenciales.
- Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.

El proyecto apoya el objetivo de invertir en medidas destinadas a garantizar un elevado nivel de seguridad de sus redes y sistemas de información. El Ayuntamiento considera que sus redes y sistemas de información desempeñan un papel crucial en la sociedad. Por eso su confiabilidad y seguridad son esenciales para las actividades económicas y sociales, y en particular para el funcionamiento de la ciudad. El Ayuntamiento considera necesaria la seguridad y resiliencia por el potencial carácter transnacional de los tratamientos, valorando que una perturbación grave de las redes y sistemas ya sea o no deliberada, podría afectar más allá de su ámbito de influencia directa.

Por lo tanto, la solución ha de contemplar el suministro de dispositivos, licencias y los servicios de despliegue e implantación para los siguientes componentes, independientemente de otras necesidades que se especifiquen a lo largo de este pliego:

- Implantación y despliegue de las herramientas del CCN LUCIA, SAT-INET y MICROCLAUDIA.
- Implantación de una solución de recolección y correlación básica de los registros de trazabilidad (logs) necesarios para la vigilancia.
- Implantación de infraestructuras de ciberseguridad para mejorar la protección y asegurar el acceso y el perímetro de la red.
- Plan de adecuación al Esquema Nacional de Seguridad.
- Implantación de una plataforma que permita desarrollar un plan de concienciación y formación para todos los usuarios y empleados del Ayuntamiento en materia de ciberseguridad.

A su vez, y esto aplica a todos los componentes a implantar y que están descritos en este pliego, los trabajos de instalación y puesta en marcha incluirán los servicios profesionales relacionados con la instalación y configuración de la solución en los dispositivos del Ayuntamiento incluidas en el alcance de esta. Las tareas que realizar estarán encaminadas al correcto despliegue de la solución en el Ayuntamiento y reporte de información de seguridad, pudiendo incluir:

- Tareas de diseño, despliegue e integración de la solución contratada en el Ayuntamiento, tareas que comprenden la realización de una configuración personalizada por cada organismo para optimizar la detección de eventos.
- Ajuste fino (“Fine tuning”) de las herramientas instaladas para su correcta adaptación al ciclo actualizado del estado de la seguridad.
- Configuración y pruebas del adecuado reporte de la información y eventos relevantes desde el punto de vista de seguridad a los sistemas de monitorización de seguridad del Ayuntamiento (SIEM, etc.).
- Transferencia de conocimientos al Ayuntamiento relacionados con el proceso de instalación y configuración en la entidad.

Se opta por herramientas del CCN-CERT por su carácter gratuito al día de redacción del presente PPT, así como su compatibilidad e incorporación a la Red Nacional de Operaciones de Ciberseguridad, para notificación y seguimiento de Ciberincidentes para intercambio automático y fluido de éstos con la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, mediante la implantación y operación de herramientas de gestión de incidentes siguiendo las recomendaciones del CCN-CERT (Centro Criptológico Nacional).

1.2. Requisitos Funcionales de la Solución requerida.

1.2.1. Implantación y despliegue de las herramientas del CCN LUCIA, MICROCLAUDIA y SAT-INET.

1.2.1.2 Implantación y operación de la herramienta de gestión de incidentes LUCIA del CCN-CERT que operará en modo federado con el de la Plataforma Nacional.

Con el fin de poder gestionar de un modo eficaz los incidentes en cualquier organismo público se encuentra disponible en el portal del CERT Gubernamental Nacional la versión 2.5 de la herramienta LUCIA.

La herramienta permite, además, cumplir con dos de los requisitos del Real Decreto 3/2010 del Esquema Nacional de Seguridad (ENS): la obligatoriedad de notificar los incidentes (acorde con la Guía CCN-STIC 817 de Gestión de Ciberincidentes) y cargar los datos en INES (CCN-STIC 824 de Información del Estado de Seguridad).

LUCIA se distribuye como máquina virtual en formato OVF lista para ser configurada y ejecutada, cuyo despliegue puede realizarse en cualquier servidor de virtualización que acepte este formato como por ejemplo VMWare ESXi o KVM. La distribución consta de un primer disco que contiene el sistema operativo (lucia- so.vmdk - 55GB) y de un segundo disco donde se encuentra toda la configuración y la instalación del software de gestión de tickets (lucia-data.vmdk - 50GB).

Las tareas asociadas a este servicio serán las de instalación, implantación y administración de la herramienta LUCIA.

Como parte de la instalación e implantación de LUCIA se requerirá:

- La máquina virtual de LUCIA en formato OVF que incluye los dos discos proporcionados con la distribución oficial del software.
- Configuración de red para la máquina.
- Establecer el nombre de dominio para la máquina, es decir, la URL del servicio LUCIA.
- Configurar una o varias cuentas de correo para la recepción de correos.
- Configurar el servidor SMTP para el envío de correos.
- Instalar el certificado digital válido perteneciente a una CA junto a su cadena de certificación para el servidor.

> Configurar el navegador con el certificado de Ayuntamiento instalado que se genera durante la instalación.

Una vez instalada LUCIA, el servicio requerirá las siguientes tareas de administración durante la vigencia del contrato:

> Gestionar grupos de usuarios y sus roles.
> Gestión de usuarios.
> Administración de colas de trabajo. Estas engloban una serie de propiedades y procesos para su correcto funcionamiento.
> Controlar los permisos otorgados a colas y demás objetos de LUCIA.
> Gestionar usuarios gestores externos, que son aquellos a los que se desea dar acceso a alguno de los tickets creados manteniendo oculto el resto. Tal sería una empresa subcontratada que brinda apoyo en la resolución de ciertos incidentes a una entidad pero que no quiere que vea el resto de los incidentes.
> Monitorizar y controlar la sincronización con el servidor central de LUCIA en el CCN-CERT.
> Gestionar campos personalizados, notificaciones y plantillas de procesos.
> Exportación de tickets a terceras plataformas.
> Copias de seguridad.

1.2.1.3 Despliegue de la herramienta microCLAUDIA del CCN-CERT en toda la organización.

MicroCLAUDIA es una capacidad basada en el motor de CLAUDIA que proporciona protección contra código dañino de tipo ransomware a los equipos de una entidad. Para ello, hace uso de un agente ligero para sistemas Windows que se encarga del despliegue y ejecución de vacunas.

La conexión del agente al servicio central de microCLAUDIA, ubicado en la nube del CCN-CERT, permite descargar y ejecutar las vacunas que el Ayuntamiento 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 el Ayuntamiento. Asimismo, el servicio ofrece la actualización automática de las mismas para cubrir adaptaciones a las nuevas formas de ejecución del ransomware.

Por otro lado, el CCN-CERT administra el servicio central en su nube y se encarga de la generación de nuevas vacunas, permitiendo a el Ayuntamiento acceder a este servicio y, de esta forma, revisar el estado general de vacunación de sus equipos e incluso configurar su aplicación.

El despliegue de las vacunas se realizará desde cualquier herramienta de gestión de distribución de software o mediante políticas de Windows. No requerirá modificaciones adicionales en la red del Ayuntamiento.

Las tareas incluidas en este punto serán:

> **Descarga** del SW microCLAUDIA
> **Generación de plan de implantación**: manual o automatizado (vía GPO)
  - En caso del despliegue manual, incluirá soporte a la instalación que realizará el propio Ayuntamiento.
  - En caso de despliegue automatizado, incluirá la generación de las tareas de distribución.
> Una vez instalado, se hará un **seguimiento** y **soporte** de la actualización de licencias durante la vigencia del contrato.

1.2.1.4 Despliegue de la herramienta SAT-INET del CCN-CERT en toda la organización.

El Sistema de Alerta Temprana (SAT) de Internet es un servicio desarrollado e implantado por el Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (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. Su misión es detectar patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico y sus flujos. En ningún momento se centra en el análisis del contenido del tráfico, que no sea relevante en la detección de una amenaza.

Para su puesta en marcha es necesaria la implantación de una **sonda individual** en la red del Organismo, que se encarga de recolectar la información de seguridad relevante que detecta y, después de un primer filtrado, enviar los eventos de seguridad hacia el **sistema central** que realiza una correlación entre los distintos elementos y entre los distintos dominios (organismos). Inmediatamente después, el Organismo adscrito recibe los correspondientes avisos y alertas sobre los incidentes detectados.

Todos los trabajos a realizar, licencias, etc., para su puesta en marcha y buen funcionamiento serán asumidos por el adjudicatario.

1.2.1.2 Plan de formación

Para la correcta explotación de las herramientas del CCN desplegadas al amparo de este concurso, el Adjudicatario deberá desarrollar, planificar e impartir una formación de manera que el personal, que el Ayuntamiento designe para ello hasta un máximo de 5 personas, sea capaz de operar, mantener, configurar y si fuese necesario reinstalar cualquier subsistema implicado.

Los licitadores presentarán en su oferta técnica una planificación detallada con contenidos y duración de los cursos a impartir, que deberá ser aprobada por el responsable del contrato tanto en contenido como planificación horaria. La formación propuesta deberá comprender al menos lo siguiente:

- Operación. Los contenidos se orientarán a obtener las habilidades necesarias para operar con el subsistema implicado y deberá incluir el perfil requerido y/o conocimientos previos de los usuarios destinatarios del mismo.
- Técnico. Con contenidos orientados a obtener el detalle técnico, instalación, mantenimiento, configuraciones, parametrizaciones, máquinas virtuales, direccionamiento IP, etc. de la infraestructura implicada.

Será obligación del adjudicatario el suministro de toda la documentación y material necesario para la realización de los cursos.

La persona adjudicaría deberá considerar lo siguiente para la impartición del plan de formación:

- Los formadores serán los implantadores o estarán respaldados por ellos.
- La transferencia se realizará en la sede del Ayuntamiento, de forma presencial o mediante videoconferencia, según calendario acordado entre las partes.
- Deberá contar con un mínimo de 16 horas de formación.

1.2.2. Implantación y despliegue de una solución de protección del puesto de trabajo EDR.

El Ayuntamiento requiere mejorar la protección de su parque de puestos de trabajo, mediante una solución avanzada basada en tecnología EDR (Endpoint Detection and Response) que aporte capacidades de detección y bloqueo de actividades maliciosas, incluido el ransomware, que se pudieran producir en los endpoints (dispositivos de usuarios) y servidores del Ayuntamiento, cuyas características principales serán:

- Detección automatizada de amenazas enmascaradas.

- Reducción del tiempo medio de identificación de amenazas (MTTI – Mean Time To Identify).
- Disminución del tiempo medio para la contención (MTTC – Mean Time To Contain).
- Visión completa de la amenaza, incluyendo la cadena de causalidad, es decir, determinar su procedencia y mecanismo de generación e infección.
- Optimización del volumen de alertas de seguridad y su gestión, gracias al análisis automatizado de las causas principales.
- Recopilación de información para un posible análisis forense.

Por ello, se valorará el suministro e implantación de una solución de EDR que contemple las siguientes funcionalidades:

1.2.2.1. Requisitos técnicos de la solución de EDR

- La solución EDR se deberá desplegar en los servidores y endpoints del Ayuntamiento de Mérida, debiendo soportar todos los sistemas operativos existentes en los diferentes equipos, sin que ello suponga una merma en las capacidades y nivel de seguridad ofrecida por la solución.
- El despliegue, se realizará sobre un total de 500 dispositivos entre endpoints (PC) y servidores.
- Los agentes deberán ser compatibles al menos con los siguientes sistemas operativos: Windows para desktop versión 10 y posteriores, Windows Server versión 2008R2 y posteriores, Linux Debian versión 9.1 y posteriores, Linux CentOS versión 6.7 y posteriores, Linux Red Hat versión 6.7 y posteriores, Oracle Linux 7 y posteriores, IOS 13 y posteriores y Android 8 y posteriores, Mac OS.
- Estará incluido en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación editado por el CCN en su Guía de Seguridad de las TIC CCN-STIC 105 o en su defecto dispondrá de una acreditación sobre su próxima inclusión, debiendo haber concluido satisfactoriamente, las pruebas de homologación correspondientes por parte del CCN.
- La solución debe almacenar los eventos y de manera automatizada, generar inteligencia desde los mismos para identificar las amenazas más relevantes, simplificando su gestión y disminuyendo el tiempo de respuesta a los incidentes.
- Dispondrá de sensores o agentes que además de recopilar la información del endpoint (telemetría), deben ofrecer la capacidad de responder automáticamente a los incidentes conforme a las políticas establecidas, incluso cuando no dispongan de conexión con Internet, garantizando la seguridad del

dispositivo en todo momento y en cualquier condición, ofreciendo prevención avanzada frente a malware/exploits desconocidos (zero day).

- Los agentes no podrán ser desinstalados o inhabilitados por el usuario, ni cuando disponga de privilegios como administrador del endpoint, por lo que la solución deberá incorporar medidas adecuadas para ello.
- El agente debe soportar la recolección continuada de los datos a nivel del sistema, aplicación y usuario siendo capaz de recolectar al menos los siguientes eventos:
  - Eventos de creación y terminación de procesos
  - Modificaciones del registro
  - Carga de imágenes
  - Información de conexión/desconexión de sesiones
  - Logon/Logoff
  - Creación/modificación/lectura de ficheros
  - Sesiones en red
  - Arranque del endpoint
  - Cambio de hora del endpoint
- Los eventos se podrán ingestar en un data lake local o en cloud, donde se almacenarán en caliente por un periodo mínimo de 7 días, durante el cual estarán on-line para realizar sobre ellos acciones de búsqueda, análisis e investigaciones de tipo forense.
- La solución incorporará algoritmos basados en inteligencia artificial detecte automáticamente las amenazas, clasificándolas y agrupándolas por incidentes, permitiendo realizar la gestión y respuesta.
- La solución debe poseer la certificación SOC2 Tipo II para garantizar la seguridad física sobre los sistemas que van a almacenar los datos. Además, se debe garantizar la privacidad de éstos de modo que no puedan compartirse con otras empresas u organismos, debiendo residir los datos dentro de la Unión Europea.
- Se requiere que todas las comunicaciones sean cifradas entre los componentes que forman parte del servicio de base de datos (tanto los de ingesta de logs como los de reenvío, con Syslog sobre TLS). Es necesario que los datos en tránsito sean encriptados utilizando al menos el método de encriptación TLS 1.2.
- Deberá disponer de una alta capacidad de respuesta siendo necesario que al menos pueda realizar las siguientes acciones de respuesta:
  - Aislar un endpoint.
  - Escanear.
  - Poner en cuarentena ejecutables involucrados en un incidente.
  - Terminar procesos involucrados en un incidente.

  - Ejecutar un terminal remoto seguro desde la consola de administración que permita al menos gestionar los procesos en ejecución, sistema de ficheros y ejecutar comandos/scripts de forma remota.
  - Remediar cambios de actividad maliciosa, enumerando qué archivos y claves de registro desencadenaron la cadena de causalidad, disponiendo de sugerencias de corrección de al menos: Terminar cadena de causalidad, borrar archivo, restaurar archivo, renombrar archivo, liminar valor de registro, restaurar valor de registro.
  - Ejecutar un script, tanto desde un repositorio de la herramienta, con scripts preestablecidos, como tener la posibilidad de añadir nuevos scripts en Python. Debe permitir tratar de manera especial los scripts de alto riesgo para prevenir daños en el sistema.
- La solución debe poder desplegarse desde Directorio Activo, mediante un ejecutable ligero. Es necesario disponer del instalador en formato MSI para que pueda ser distribuido bien usando políticas GPO de Directorio Activo u otras herramientas de distribución similares.
- Permitirá actualizar manual y automáticamente los agentes ya desplegados.
- Los datos recopilados deben poder utilizarse para la detección basándose en artefactos, threat intelligence o analítica (machine learning / comportamiento).
- Debe permitir la detección de IOCs estáticos y de comportamiento (basados en TTPs y Analíticas).
- Deberá admitir la creación de grupos virtuales para la fácil aplicación de políticas, acciones en los agentes y reglas de configuración a grupos de equipos que compartan características similares mediante técnicas estáticas o dinámicas.
- Permitirá identificar amenazas en base a su comportamiento (Indicadores de Compromiso de Comportamiento), para poder detectar y responder a tácticas, técnicas y procedimientos. Estos deben poder referirse al menos a procesos, registro, ficheros y actividad de red.
- Dispondrá de una librería actualizada continuamente con indicadores de compromiso por comportamiento. Permitiendo la modificación o cambio de prioridad de los mismos y añadir nuevos indicadores customizados. Estos indicadores de comportamiento estarán asociados con las distintas tácticas y técnicas MITRE que les afecten.
- Debe disponer de la capacidad de convertir una regla de detección (basada en comportamiento y TTPs) en una regla de prevención en el agente.
- Podrá utilizar motores analíticos en combinación con los indicadores de compromiso de comportamiento para detectar comportamientos sospechosos en una cadena de causalidad determinada tanto sobre endpoints gestionados, gracias a la telemetría de los mismos, como sobre dispositivos no gestionados

gracias a la telemetría de red.

- Debe ser posible asimismo realizar búsquedas manuales de IOCs en la base de datos de forma que permita comprobar de una manera sencilla y directa la afectación de la organización a IOCs obtenidos desde esta aplicación u otra externa (por ejemplo, recibidas a través de un CERT o MSSP).
- La aplicación debe ser capaz de realizar el profiling de los equipos, IPs y usuarios y calcular el baseline sobre el que detectar anomalías, utilizando para ello algoritmos de Machine Learning, que estudien al menos:
  - Comportamiento Actual (actividad actual del usuario y del dispositivo)
  - Perfil Temporal (actividad pasada del usuario y dispositivo)
  - Perfil de relación con otros peers
  - Perfil de la entidad (tipo de dispositivo, usuario, ...)
- Deberá soportar RBAC (Role Based Access Control), para la identificación del nivel de acceso que un usuario puede tener sobre la aplicación. Estos roles podrán definirse de forma predefinida o personalizados y podrán aplicarse a un conjunto concreto de endpoints al menos para la administración, cuadros de mandos e informes.
- Soportará el registro de acciones permitiendo la monitorización de tareas tales como las actualizaciones, desinstalación, scans, recuperación de datos críticos (eventos de seguridad, ficheros de soporte técnico) y restauración de ficheros en cuarentena, proporcionando visibilidad de los fallos o errores ocurridos.
- En el caso de producirse algún incidente de seguridad, la solución debe proporcionar acciones de respuesta y remediación que se aplicarán sobre los endpoints tales como:
  - Terminación de un proceso.
  - Eliminación o poner en cuarentena un fichero.
  - Ejecución de scripts.
  - Aislamiento de equipos infectados en la red.
  - Acceso a los ficheros de forma remota mediante la descarga o subida por parte del analista.
  - Ejecución de comandos y código interactivamente en cualquier equipo utilizando scripts de Python o CMD.
  - Creación de IOCs basados en el comportamiento para la generación de nuevas alertas.
  - Blacklisting/Whitelisting
- Para malware desconocido, la solución debe permitir el análisis en un sandbox. Este debe ser una solución en la nube que debe disponer de capacidad para gestionar hasta 1.000.000 de detonaciones por día. Así mismo, debe soportar al

menos:

- Cualquier ejecutable portable incluyendo: Ficheros ejecutables, Código objeto, FON (Fuentes), Salvapantallas de Microsoft Windows (.scr)
- FIcheros de Microsoft Office conteniendo macros abiertas en Excel o Word: Microsoft Office 2003 a Office 2016 (.doc y .xls), Microsoft Office 2010 y versiones posteriores (.docm, .docx, .xlsm, y .xlsx)
- Ficheros Portable Document Format (PDF)
- Ficheros de Librerías Dinámicas incluyendo: Ficheros .dll y .ocx
- Android application package (APK)
- Ficheros Mach-o
- Ficheros DMG

- Debe permitir definir fácilmente políticas para restringir escenarios de ejecución específicos con el fin de reducir la superficie de ataque de cualquier entorno.
- La solución propuesta debe soportar la recolección de telemetría y datos forenses, capturando la información desde la solución de endpoint a una localización centralizada, recopilando al menos la siguiente telemetría e información forense para fines de investigación:
  - Procesos en ejecución inyectados, incluyendo nombre y hash.
  - Creación, escritura, lectura, borrado y renombrado de ficheros, incluyendo nombre y path.
  - Comunicaciones de red salientes y entrantes, incluyendo nombre y puerto.
  - Módulos cargados por los eventos de proceso, incluyendo identificadores de módulos.
  - Escrituras, renombrados y borrados de valores del Registro.
  - Datos de logs de eventos de Windows, incluyendo descripción y event ID.
  - Eventos de autenticación por identidad y objetivo.

1.2.2.2. Implantación de la solución de EDR

Para el despliegue el adjudicatario deberá realizar en colaboración con el equipo técnico del Ayuntamiento un análisis sobre la mejor estrategia de despliegue de los agentes de EDR y la sustitución del actual software de protección instalado en los puestos de trabajo, así como identificar los requisitos necesarios para ello.

Como resultado de este análisis, el adjudicatario deberá presentar un plan de implantación en el que se detallarán:

- Las fases del proceso de implantación con indicación de las tareas a realizar en cada fase, las ventanas de intervención y los requisitos y dependencias que deban ser satisfechos por parte del Ayuntamiento.
- Propuesta del modelo de despliegue y la realización de una maqueta de prueba, que permita verificar el proceso e identificar posibles problemas, antes del despliegue general.
- Propuesta de las configuraciones sobre las reglas y políticas a configurar, tomando como partida las configuraciones actualmente en producción.

El adjudicatario pondrá a disposición del proyecto personal técnico cualificado in situ durante la ejecución del plan de instalación y puesta en servicio, con el objeto de llevar a cabo, entre otras, las siguientes tareas:

- Asistencia en la planificación y definición del despliegue de los agentes.
- Información sobre posibles incompatibilidades.
- Atención a las incidencias generadas durante el proceso de implantación, ya sea directa o indirectamente, y comprobación de la resolución de estas
- Asesoramiento al Ayuntamiento en materia de gestión de las comunicaciones y la seguridad de la información.
- Parametrización de la visualización de estadísticas y generación de informes.

El adjudicatario deberá disponer de acceso a un soporte avanzado de fabricante, para la solución de EDR propuesta, de manera que se intente minimizar, como consecuencia de la aparición de imprevistos, incidencias o problemas, el posible impacto sobre los sistemas de información productivos o la propia ejecución del plan de configuración, instalación y puesta en servicio.

Este soporte se deberá mantener durante toda la vigencia del contrato de cara a la resolución de posibles incidencias, así como para el mantenimiento de las actualizaciones de software y servicios de seguridad que el fabricante ofrezca sobre la tecnología desplegada.
El adjudicatario deberá realizar todas las actividades precisas para el correcto despliegue y configuración completa de la solución EDR.

Así mismo deberá realizar la integración con el sistema de directorio del Ayuntamiento.

A la finalización de la implantación, deberá entregar al Ayuntamiento una completa documentación de fin de proyecto, donde se incluya como mínimo, la siguiente información:

- Arquitectura de la Plataforma desplegada.
- Configuraciones realizadas y políticas

- Integraciones realizadas con sistemas del Ayuntamiento y/o externos.

1.2.3. Implantación de una solución de recolección y correlación básica de los registros de trazabilidad (logs) necesarios para la vigilancia.

El objetivo principal de contar con capacidad de recolección y correlación básica de logs es la detección de cualquier violación o amenaza inminente de la Política de Seguridad del Ayuntamiento que pueda ser informada en base al análisis de la información generada por los sistemas monitorizados. Dicha detección se realizará mediante el análisis de las alarmas, eventos e información relevantes para la seguridad informados a través del sistema de gestión de eventos SIEM (Security Information and Event Management) incluido en el alcance del presente apartado donde se integran los logs generados por los activos adscritos al sistema.

Por tanto, se requiere el suministro, análisis, diseño e implementación de un sistema SIEM del catálogo CCN-STIC 105, basado en la correlación de eventos en tiempo real que permita proporcionar información sobre eventos tomando como fuente los datos que generan los dispositivos y sistemas de la organización. El listado final de los activos (servidores, bases de datos, aplicaciones, etc.) a monitorizar será definido de mutuo acuerdo con el integrador durante la fase de consultoría inicial.

1.2.3.1. Requisitos técnicos de la solución de SIEM

Un sistema de gestión de eventos de seguridad (SIEM) está orientado a recopilar información en tiempo real sobre los eventos de seguridad generados por la red de una organización, para procesarla posteriormente con el fin de generar informes y/o alertas que puedan ayudar a la organización en la toma de decisiones en materia de seguridad. Entre las funciones principales de seguridad se encuentran la gestión de múltiples fuentes de datos, la correlación de datos, servicio de alertas y repositorio de datos sobre eventos de seguridad.

El objetivo principal de contar con capacidad de recolección y correlación básica de logs es la detección de cualquier violación o amenaza inminente a los sistemas de información o tecnológicos del Ayuntamiento que pueda ser informada en base al análisis de la información generada por los sistemas monitorizados.

Dicha detección se realizará mediante el análisis de las alarmas, eventos e información relevantes para la seguridad informados a través del sistema de gestión de evento SIEM (Security Information and Event Management) donde se integran los logs generados por los activos adscritos al sistema.

Se requiere que el adjudicatario suministre, despliegue, configure y parametrice en los sistemas de virtualización del Ayuntamiento una solución de gestión de eventos de seguridad SIEM con licencias gratuitas para la administración pública (como las proporcionadas por el CCN-CERT para la gestión y correlación de eventos de seguridad GLORIA o MONICA). De este modo se aprovecha la gratuidad de la herramienta en términos de licenciamiento y además se cumplen las premisas de reutilización de sistemas y aplicaciones de la administración pública.

La plataforma SIEM suministrada debe formar parte del catálogo del Esquema Nacional de Seguridad publicado por el Centro Cristológico Nacional (CCN-STIC-105) en la categoría "Sistema de gestión de eventos de seguridad" con categoría ENS ALTO.

EL SIEM suministrado deberá permitir, al menos, las siguientes funcionalidades:

- Procesamiento centralizado de grandes volúmenes de información de eventos.
- Detecta y resuelve amenazas en tiempo real.
- Aplica técnicas de automatización y orquestación entre múltiples fuentes. Capacidad SOAR. Responde de forma automática.
- Analiza el comportamiento del usuario
- Ciberinteligencia de Amenazas
- No limitará las capacidades de escalado aun si se monitoriza un número elevado de fuentes.
- Soportará un modelo de correlación distribuida, en el que los eventos pueden ser recolectados y correlados en origen.
- Deberá posibilitar un intercambio automático y fluido de ciberincidentes con la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (LUCIA).
- Utilizará solo alertas previamente correladas para identificar amenazas que afecten de forma coordinada a varias fuentes.
- Aportará capacidades avanzadas de búsqueda y detención de amenazas junto con análisis de comportamiento (threat hunting, threat detection y Behavioural Analytics).
- Dispondrá de un paquete base de casos de uso.
- Dispondrá de cuadro de mandos.
- Estará Integrado con soluciones del CCN-CERT como LUCIA, REYES o CARMEN.

El sistema debe analizar y correlacionar en tiempo real las informaciones, eventos y logs recopilados, tipos y vulnerabilidades de activos, comportamiento histórico, junto con acceso a información actualizada sobre bases de datos de vulnerabilidades, de amenazas, reputación, estándares de configuración y cumplimiento, etc., determinando y ponderando los riesgos, filtrando falsos positivos y detectando posibles incidencias y

amenazas para la seguridad, tales como ataques, configuraciones inseguras, incumplimientos normativos, vulnerabilidades.

El Ayuntamiento proporcionará la infraestructura de virtualización necesaria para el despliegue de la solución SIEM, debiendo los licitadores indicar en sus ofertas el dimensionamiento y requisitos técnicos que deberá cumplir la infraestructura para el correcto funcionamiento de la solución.

El adjudicatario será el responsable de todo tipo de mantenimiento, a saber, correctivos, preventivos, evolutivos, etc., así como actualizaciones o cualquier tipo de actuación que se requiera para garantizar el correcto funcionamiento de la(s) VM(s) proporcionadas por el Ayuntamiento de la solución SIEM, incluyendo en las labores descritas todo lo relacionado con el Sistema Operativo, software o herramientas software instaladas proporcionadas por el CCN para el correcto funcionamiento de la plataforma.

1.2.2.2 Servicios de instalación avanzada asociados a los suministros a adquirir

Como parte del servicio de instalación se requiere la implantación de la solución de recolección y correlación básica de los registros de trazabilidad (logs) necesarios para la vigilancia que ha de contemplar como mínimo los siguientes servicios de implantación:

El adjudicatario aportará el apoyo y colaboración al personal de integración en el proceso de análisis y puesta en marcha de la plataforma, incluyendo la realización de posibles cambios de configuración en los sistemas y fuentes de datos que resulten necesarios para el envío de eventos al SIEM.

Se garantizará el suministro de las licencias necesarias para atender el flujo de eventos generado por todos los activos identificados durante la fase inicial, así como la inclusión de fuentes de actualizaciones, de inteligencia de seguridad, de vulnerabilidades, etc., necesarias para que el SIEM se encuentre permanentemente actualizado.

Se incluyen las tareas que serán tenidas en cuenta cuando se haga la planificación inicial del proyecto, identificando aquellas que requieren reunión, aquellas que son responsabilidad del Ayuntamiento o aquellas que requieren un coste en tiempo muy intenso. La planificación se realizará como una de las primeras actividades a realizar en la fase de implantación y deberá ser aprobada por la Entidad. En todo momento se tendrán en cuenta las siguientes premisas:

- El adjudicatario deberá realizar un análisis de la arquitectura de seguridad y sistemas del Ayuntamiento para determinar qué elementos proporcionarán eventos de seguridad al SIEM.

- Se ofrecerá apoyo a la configuración de los sistemas para la correcta implementación del envío de eventos de seguridad desde estas al SIEM. Adicionalmente se deberán proporcionar instrucciones para que puedan configurarse correctamente los sistemas de logs de forma que se obtenga información suficiente para analizar incidentes de ciberseguridad.
- Los licitadores deberán incluir en sus propuestas un plan de implantación para el sistema en el que como mínimo se contemplará el desarrollo de las siguientes actividades:
  - Diseño detallado. Esta actividad realizará la identificación de fuentes de logs y definición de la arquitectura ~~final~~, seleccionando la ubicación, direccionamiento y conectividad de la herramienta SIEM a desplegar.
  - Despliegue y configuración inicial. En base al diseño detallado, se realizará el despliegue y configuración inicial de la plataforma de virtualización y el despliegue del software base del SIEM sobre la misma.
  - Configuración y ajustes de política de correlación. Una vez se comiencen a recibir logs de los distintos dispositivos en la plataforma, se realizará el despliegue y configuración del catálogo de directivas de seguridad en función de las fuentes integradas.
  - Plan de pruebas y puesta en producción. Se ejecutará el plan de pruebas definido en fase de diseño detallado y que habrá sido corroborado por el Ayuntamiento. Se incluirá toda la documentación asociada al proyecto.

1.2.4. Plan de adecuación al Esquema Nacional de Seguridad.

1.2.4.1. Antecedentes

El Ayuntamiento, en la implementación de los sistemas de información, debe cumplir los diferentes marcos normativos relacionados con las TIC, de manera que se garantice la confianza en el uso de los medios electrónicos por parte de la ciudadanía.

Los sistemas de información, en el ámbito del sector público, están sujetos a los siguientes marcos normativos de obligado cumplimiento:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 39/2015 de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público.
- Metodología de Análisis y Gestión de Riesgos IT (MAGERIT v3).

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad (ITS) de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad (ITS) de Notificación de Incidentes de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad (ITS) de Informe del Estado de la Seguridad (INES).
- Guías CCN STIC serie 800. Esquema Nacional de Seguridad. Centro Criptológico Nacional.

En base a estos criterios, el objetivo de este servicio se dirige hacia el cumplimiento del Ayuntamiento respecto de estas obligaciones, aportando con ello la necesaria cobertura técnica, legal y organizativa requerida para cimentar las garantías que deben sustentar estas nuevas formas de relación entre el Ayuntamiento y la ciudadanía.

1.2.4.2. Objetivo del plan de adecuación al ENS

La Administración Pública española mantiene históricamente altos niveles de automatización en su Modelo de Servicio. En este contexto, el Ayuntamiento proporciona un catálogo de servicios electrónicos a todos sus interlocutores y partes interesadas, aportando mediante las Tecnologías de la Información y las Comunicaciones (TIC en adelante) las funcionalidades en las que se basa el desempeño de sus actividades.

La Ley 40/2015 (LRJSP) supuso un impulso decisivo para la generalización de los "servicios electrónicos" a los Ciudadanos y, dentro de ella, se recogen las referencias sobre su marco de seguridad (ENS), interoperabilidad (ENI) y cumplimiento de LOPD-RDLOPD que deben mantener los derechos y garantías de los Ciudadanos en los entornos TIC de las AAPPs.

Estas altas capacidades TIC requieren, en consecuencia, las correspondientes iniciativas de securización, de forma que las transacciones de todo tipo que desarrolla

el Organismo a través de aquéllas lo hagan sobre entornos gestionados y controlados en las dimensiones de seguridad aceptadas como referentes (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad).

Estas iniciativas de securización pueden formar parte de un Plan Global de Cumplimiento Normativo y vienen reflejadas en los Marcos Normativos citados.

Por este motivo, el Ayuntamiento incluye entre las actividades a desarrollar un servicio de consultoría en seguridad de la información para labores de asistencia técnica para la adecuación a los requisitos y medidas del Esquema Nacional de Seguridad, de acuerdo a la última actualización derivada de la aprobación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En dicho servicio es necesario que se proporcione una herramienta online especializada en la Seguridad de la Información que permita dar una visión integrada de los distintos requisitos de gobierno, riesgo y cumplimiento sobre el dominio de seguridad objeto del pliego. El adjudicatario deberá proporcionar un cuadro de mando a la Oficina de Seguridad que cumpla las siguientes características:

- Cuadro de mando "multinorma": Deberá disponer de la posibilidad de dar soporte al cumplimiento del ENS, RGPD y LOPD-GDD. Incluirá la licencia del mismo durante el período de prestación del servicio.
- Asimismo, la plataforma permitirá la adecuación a otros marcos normativos (ISO 27001, 22301, ENI…). por si el Ayuntamiento decide adecuarse a los mismos en un futuro.
- Estará integrada con PILAR (herramienta de análisis y gestión de riesgos) y permitirá la generación de informes para enviar al CCN según la guía CCN-STIC824.

1.2.4.3. Alcance de trabajos a realizar

En este apartado se definen las tareas identificadas como trabajos mínimos que debe realizar la empresa adjudicataria.

1.2.4.3.1. FASE 1: REVISIÓN O ELABORACIÓN DEL PLAN DE ADECUACIÓN

En relación con el cumplimiento del ENS, las actividades también comenzarán con un diagnóstico inicial para determinar el grado de cumplimiento presente. Además, el Real Decreto 311/2022 y la Guía Técnica CCN-STIC-806, elaborada por el Centro Criptológico Nacional, establecen que el contenido mínimo del Plan de Adecuación será el siguiente:

- Se establecerá la estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.
- Una Política de Seguridad, que deberá cumplir los requisitos establecidos en el Anexo II del R.D. 311/2022, o detallar las acciones y contenidos previstos para que sea conforme con el mismo. Sus contenidos y características se describen en el documento CCN-STIC 805.
- Un inventario de la Información que se maneja, con su valoración conforme a los requisitos del R.D. 311/2022, detallados en la Guía Técnica CCN-STIC-803.
- Un inventario de los Servicios que se prestan, con su valoración conforme a los requisitos del R.D. 311/2022, detallados en la Guía Técnica CCN-STIC-803 y las guías CCN-STIC 883 Perfil de cumplimiento.
- Información detallada acerca de los datos de carácter personal que son tratados, aun cuando la Guía CCN-STIC 806 admite que el Plan de Adecuación simplemente direccione al Registro de Actividades del Tratamiento.
- La categoría del Sistema, conforme a los requisitos del R.D. 311/2022, detallados en la Guía Técnica CCN-STIC-803 y guías CCN-STIC 883 Perfil de cumplimiento
- Una Declaración de Aplicabilidad y perfil de cumplimiento específico de las medidas de seguridad incluidas en el Anexo II del R.D. 311/2022, y detalladas en las Guías Técnicas CCN-STIC 883 Perfil de cumplimiento.
- Un Análisis de Riesgos conforme a los requisitos del R.D. 311/2022 y a la categorización del Sistema, conforme a la Guía Técnica CCN-STIC-803. En este punto se aplica la metodología MAGERIT V3 en toda su extensión, criterios, catálogos, etc.
- Un Plan de Mejora de la Seguridad, incluyendo plazos estimados de ejecución para subsanar las insuficiencias detectadas.
- Consideraciones y medidas a adoptar derivadas de la interconexión entre Sistemas de una misma organización o de organizaciones distintas.
- El adjudicatario deberá de volcar y actualizar toda la información recabada en la auditoría en la herramienta puesta a disposición por parte del CCN-CERT, con el objeto de garantizar el 100% del cumplimiento en el desarrollo e implantación del ENS.

El manejo de información de terceros y la prestación de servicios a terceros se evaluará de acuerdo con lo establecido en el apartado 4 de la guía de seguridad CCN-STIC-806 ESQUEMA NACIONAL DE SEGURIDAD. PLAN DE ADECUACIÓN

1.2.4.3.2. FASE 2: DESARROLLO DEL PLAN DE ADECUACIÓN DEL E.N.S.

Para el desarrollo y avance del plan de adecuación del ENS del Ayuntamiento, deberán suministrarse servicios de consultoría externa que complementen el despliegue de las medidas tecnológicas en los siguientes ámbitos:

1. Gestión de los riesgos de seguridad de la información: Desarrollo del modelo de riesgos vinculados a la administración electrónica y las amenazas a los sistemas de información que los soportan.
2. Soporte a los requisitos documentales derivados del ENS: políticas, normas y procedimientos requeridos:
   Para garantizar un adecuado cumplimiento y poder evidenciar la definición de las medidas de seguridad, se debe revisar la estructura del marco normativo existente teniendo en consideración si las hubiera, la Política, normativas de seguridad o procedimientos existentes. En base a esta revisión de documentos, se debe formalizar un nuevo marco normativo (normas y procedimientos de seguridad) que concreten los requisitos técnicos a satisfacer en cada caso y los procedimientos operativos que deben implantarse como parte del cumplimiento del ENS.

   Marco normativo:
   - Normativa de control de acceso lógico
   - Normativa de acceso a internet
   - Normativa de uso del correo electrónico
   - Normativa para trabajar fuera de las instalaciones
   - Normativa de uso de dispositivos móviles
   - Normativa de gestión de soportes
   - Normativa de seguridad de los equipos
   - Normativa de control de seguridad en la operativa
   - Normativa de conformidad legal
   - Normativa de gestión de terceros u outsourcing
   - Normativa de clasificación de la información
   - Normativa de seguridad física en salas CPD y edificios
   - Normativa de gestión de incidencias
   - Normativa de gestión de claves criptográficas

   Marco procedimental:

- Procedimiento de gestión y aprobación de la documentación
- Procedimiento de clasificación, marcado y etiquetado de información y soportes
- Procedimiento de contratación de personal
- Procedimiento de contratación y seguimiento de servicios externos
- Procedimiento de gestión de la formación y concienciación
- Procedimiento de altas, bajas y modificaciones de usuarios
- Procedimiento de gestión del cambio y configuración segura de los sistemas
- Procedimiento de gestión del mantenimiento hardware y software
- Procedimiento de entrada y salida de equipamiento y soportes
- Procedimiento de copias de seguridad y restauración
- Procedimiento de gestión de incidentes y brechas de seguridad
- Procedimiento de paso a producción
- Procedimiento de control de acceso físico

3. Formación y concienciación en materia de seguridad: Desarrollo de actividades de concienciación, formación y entrenamiento al personal del Ayuntamiento en materia de seguridad de la información, de forma que mejore el conocimiento de esta problemática y permita al personal la colaboración en la prevención y detección de este tipo de incidentes.
4. Seguimiento de la implantación de las medidas de seguridad derivadas del E.N.S.
5. Definición de métricas e indicadores relevantes para determinar la eficacia de las medidas de seguridad requeridas.
6. Asesoramiento técnicas para la resolución de dudas relativas al desarrollo e implantación del ENS.
7. El adjudicatario deberá de entregar todo el desarrollo del marco normatizo y procedimental.
8. El adjudicatario será el responsable de actualizar toda la información de la auditoría del ENS en las plataformas dispuestas por el Ministerio a tal fin.

1.2.4.3.3. Herramienta de gestión

Con el objetivo de ayudar al Ayuntamiento en el seguimiento de los cumplimientos normativos y buenas prácticas en el ámbito de la seguridad los licitadores deberán

incluir en sus propuestas un portal especializado en Seguridad de la Información que permita dar una visión integrada de los distintos requisitos de Gobierno, Riesgo y Cumplimiento sobre el dominio de seguridad objeto del pliego.

Por tanto, también es objeto de este pliego la puesta a disposición del Ayuntamiento de una herramienta informática que permita hacer una implementación lo más automática posible, así como el seguimiento posterior de los marcos normativos. Dicha herramienta debe estar instalada totalmente en los sistemas del proveedor y funcionar íntegramente online, web o en la nube sin necesidad alguna de instalación en local.

Se requiere una herramienta que proporcione el soporte adecuado y adaptado a las necesidades actuales y futuras impuestas por el ENS, tanto para la elaboración inicial del Análisis Diferencial respecto al R.D. 3/2010 y R.D. 951/2015, del Análisis Diferencial y del Análisis de Riesgos complementario requerido, así como para las obligaciones que éste establece tras su aprobación, hasta poder disponer finalmente de un Documento de Conformidad.

Adicionalmente, el ENS orienta a la organización hacia la implementación efectiva de soluciones técnicas en diversos ámbitos, como el inventariado de activos, el registro de incidencias y eventos de seguridad y la gestión, conservación centralizada de documentación y registros o monitorización de sistemas.
Lo anterior requiere que el adjudicatario debe proporcionar una plataforma que cumpla las siguientes características marcadas como OBLIGATORIAS y se valorarán adicionalmente las opcionales:

- Cuadro de mando “multinorma”: Deberá disponer de la posibilidad de dar soporte al cumplimiento del ENS y PROTECCIÓN DE DATOS adaptada al RGPD (OBLIGATORIO)
- Asimismo, la plataforma permitirá la adecuación a otros marcos normativos como por ejemplo ENI o ISO 22301 por si la organización decide adecuarse a los mismos en un futuro (opcional)
- Estará integrada con PILAR (Permitirá la importación y exportación de la información relacionadas con el análisis de riesgos) (OBLIGATORIO)
- Permitirá la gestión centralizada de todas las entidades locales. Permitirá tener visibilidad del progreso individual, pero garantizando en todo momento la segregación de funciones y la confidencialidad de la información de cada una de ellas (opcional)
- Contemplará las sinergias en la gestión unificada del ENS y del RGPD, minimizando el esfuerzo tanto en el despliegue inicial como, especialmente, en el mantenimiento posterior (opcional)

- Posibilidad de definir Cuadros de Mando sobre activos y dependencias, acciones (proyectos y tareas), apreciaciones del riesgo, así como utilizando indicadores alimentados manualmente o leídos automáticamente desde sistemas externos accesibles (opcional)
- Gestión de usuarios (OBLIGATORIO)
- Capacidad para asignar perfiles de acceso a los usuarios.
- Capacidad de definir roles a los responsables (DPO, responsables de seguridad, etc.).
- Capacidad para asignar funciones a los roles de responsables
- Acceso al sistema de los responsables en función de las atribuciones asignadas.
- Capacidad para especificar el organismo en el que se encuentra ubicado el responsable del tratamiento.
- Capacidad de tutela o control por parte del Ayuntamiento que se defina como administradora.

Para la gestión del Esquema Nacional de Seguridad (ENS) se requiere que la herramienta que disponga de las siguientes funcionalidades:

- Funcionalidades para la gestión de la implantación y el mantenimiento del SGSI (Sistema de Gestión de Seguridad de la Información) requerido por el ENS (OBLIGATORIO)
- Carga de los tipos de información por defecto del Anexo de «Entidades locales» de la guía CCN-STIC-803, incluyendo la valoración por defecto en Confidencialidad, Integridad, Autenticidad y Trazabilidad que aprobó el CCN (OBLIGATORIO)
- Carga de los servicios por defecto del Anexo de «Entidades locales» de la guía CCN-STIC-803, incluyendo la valoración por defecto en la Disponibilidad que aprobó el CCN (OBLIGATORIO)
- Definición de Sistemas de Información «tipo» habituales en las Entidades Locales, mapeados con los Servicios y Tipos de Información más relevantes, de forma que ya se encuentren oportunamente valorados, conforme a los requisitos de la guía CCN-STIC-803 de Valoración de Sistemas (OBLIGATORIO)
- Carga de catálogo de amenazas de Magerit versión 3 (opcional)
- Escenarios de riesgo predefinidos sobre los sistemas más relevantes de las Entidades Locales, con valores por defecto para la probabilidad y el impacto (opcional)
- Iniciativas y proyectos predefinidos que permitan tratar los riesgos inaceptables más habituales de las Entidades Locales (opcional)
- Soporte al Análisis Diferencial de las medidas del R.D. 3/2010 y 951/2015 conforme a la guía técnica CCN-STIC-808 (OBLIGATORIO)

- Definición de Comités y Roles conforme a la guía CCN-STIC-801 (OBLIGATORIO)
- Valoración de Activos según CCN-STIC-803 (OBLIGATORIO)
- Gestión del Riesgo utilizando MAGERIT como metodología (OBLIGATORIO)
- Auditoría de las medidas conforme a las Guías Técnicas CCN-STIC-802, CCN-STIC-804 y CCN-STIC-808 (OBLIGATORIO)

Una vez finalizado el plan de adecuación la plataforma deberá permitir su implantación ofreciendo un gestor documental open source integrado. Posteriormente permitirá revisar y auditar todo lo anterior.

La empresa adjudicataria pondrá a disposición del Ayuntamiento una instancia de la herramienta en modo Saas, para que Ayuntamiento pueda verificar el cumplimiento de las diferentes funcionales requeridas en este pliego.

1.2.5. Formación y concienciación en ciberseguridad.

Con objeto de concienciar a los usuarios digitalizados del Ayuntamiento, se requiere el despliegue de una plataforma de concienciación y formación en el ámbito de la ciberseguridad que, mediante una metodología de formación continua, presente un enfoque cíclico que enseñe a los usuarios las mejoras prácticas y les muestre cómo emplearlas cuando se enfrenten a amenazas de seguridad.

La necesidad viene motivada porque más del 90 % de los ciberataques se dirigen contra los usuarios, por lo que la formación de los empleados es fundamental para la organización. Las tecnologías que detectan y bloquean las amenazas antes de que lleguen a los usuarios no pueden detenerlo todo. Por tanto, los usuarios deben ser conscientes de esta realidad y ser capaces de reaccionar frente a intentos de ataques de phishing y estafas BEC (fraude del CEO) y otras.

En este sentido se persigue una solución que ofrezca el máximo de flexibilidad para desarrollar un programa a lo largo del tiempo adaptado a las necesidades puntuales de cada usuario, que permita identificar áreas de debilidad y proporcione formación dirigida cuando y donde más se necesite.

Adicionalmente se persigue cuantificar los resultados mediante la combinación de exámenes, educación, refuerzo y evaluación, junto con la metodología de formación continua.

En este sentido se requiere una plataforma que reúna las siguientes capacidades y prestaciones, dimensionada para un total de 500 usuarios/empleados municipales disponible durante un período de al menos **12 meses.**

Evaluación del conocimiento

La plataforma debe disponer de la opción de cuantificar el conocimiento de los usuarios mediante cuestionarios de conocimientos.

La plataforma debe permitir generar dichos cuestionarios sin ningún límite, seleccionando preguntas pregeneradas o nuevas.

La plataforma debe permitir el envío de notificaciones a los usuarios cuando se les asigna un nuevo cuestionario, cuando lo han finalizado o recordatorios de finalización.

La plataforma debe de permitir a los usuarios conocer su puntuación ~~en tiempo real~~ del cuestionario que está realizando.

La plataforma debe de permitir a los usuarios a reanudar un cuestionario desde la última pregunta contestada en caso de haberlo abandonado sin finalizar.

La plataforma debe permitir asignar formaciones específicas a los usuarios que no superen el umbral deseado de conocimientos en cada ámbito dentro de un cuestionario.

Material complementario y de refuerzo

La plataforma debe de ofrecer ~~más de 500~~ materiales de refuerzo, que incluyan vídeos, posters, infografías, newsletters, comics, flyers, memes, portcards, artículos y salvapantallas.

Campañas

La plataforma debe permitir generar campañas de simulación de phishing y malware sin ningún límite.

La plataforma debe permitir incluir un momento de aprendizaje cuando un usuario hace click en una simulación de phishing, ofreciendo plantillas con imágenes e infografías en distintos idiomas, mensajes de error, vídeos o una personalización de la compañía, incluida landing pages externas.

La plataforma debe disponer de la opción de la asignación automática de módulos de formación a aquellos usuarios que hayan hecho click en la simulación de phishing.

La plataforma debe permitir anonimizar los datos de los usuarios en los resultados de cualquier campaña de simulación de phishing.

La plataforma debe permitir realizar un seguimiento de qué usuarios han abierto la simulación de phishing, han hecho click, han hecho múltiples veces click, han abierto el adjunto, han visto el momento de aprendizaje y han informado del mensaje sospechoso.

Reporte de mensajes sospechosos

La plataforma debe permitir a los usuarios que puedan informar sobre mensajes de correo sospechosos mediante un simple click.

La plataforma debe realizar un seguimiento de qué usuarios han informado como mensaje sospechoso las simulaciones de phishing enviadas por la propia plataforma.

Módulos de formación

La plataforma debe de contar con módulos de formación precargados, que se deberán actualizar, complementar y mejorar continuamente por parte del fabricante, añadiendo nuevos contenidos formativos de forma habitual.

La plataforma debe de contar con módulos de formación de tipo vídeo, interactivo y gamificado, traducidos en los idiomas soportados por la plataforma además del castellano.

La plataforma debe de poder ofrecer de forma automática, el idioma del contenido formativo reconociendo el idioma del navegador del usuario, o si este activa algún idioma en su configuración particular.

La plataforma debe disponer de contenidos formativos sujetos a los principios de brevedad, presentación de–conceptos y procedimientos, reflejo de la necesidad de interacción, descripción de situaciones reales y seguimiento.

La plataforma debe de permitir activar contenidos formativos de interés, para que cualquier usuario lo pueda realizar siempre que lo desee, sin ser necesario una asignación previa.

Personalización

La plataforma debe permitir realizar personalizaciones en los contenidos formativos. Las personalizaciones deben consistir en la edición de textos visibles, imágenes y pantallas en los contenidos interactivos, como las preguntas o añadir hipervínculos a sitios webs internos de la compañía, como las de cumplimiento normativo u otros contenidos relacionados.

1.2.6. Entregables

El adjudicatario deberá proporcionar, al menos, los siguientes entregables en el ámbito de la instalación avanzada, que deberán ser validados por el Ayuntamiento para su aceptación:

- Elaboración de un Plan de Trabajo detallado.
- Documentación de análisis y diseño incluyendo esquemas de la arquitectura lógica y física.
- Documentación de instalación, parametrización y configuración.
- Planes de pruebas realizadas y sus resultados.
- Plan de Contingencia, detallando las actuaciones para llevarlo a cabo.
- Manuales y otro material relacionado con la transferencia de conocimientos.
- Informes periódicos de las actuaciones realizadas.

1.2.7. Importe. Duración del contrato. Plazo de ejecución. Garantías

El importe de la licitación es de 115.302,11€ iva incluido.

Base imponible: 95.291
Iva (21%)……..: 20.011,11

Este proyecto está financiado al 100% por los fondos Next Generations.

La duración del contrato será de 12 meses y su plazo de implantación máximo hasta el 30 de septiembre de 2023 que deberá de estar todo instalado y funcionando al 100%.

Mantenimiento del 100% de los servicios será de 1 año a partir de la finalización de la implantación.
Garantías mínimas de 1 año en todos los componentes instalados, así como licencias adicionales que puedan ser necesarias y que correrán a cuenta del licitador.

Las actuaciones de este contrato están financiadas por el Mecanismo de Recuperación y Resiliencia de la Unión Europea, establecido por el Reglamento (UE) 2020/2094 del Consejo, de 14 de diciembre de 2020, y regulado según Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia. "Financiado por la Unión Europea –Next GenerationEU".

1.2.8. CPV

30200000 equipos y material informáticos.

48730000 paquetes de software de seguridad.

48761000 paquete de software de antivirus.

72600000 servicios de apoyo informático y de consultoría.

2. Obligaciones del Adjudicatario.

La empresa adjudicataria deberá ofrecer una bolsa de 5 jornadas para proporcionar al menos el siguiente soporte avanzado durante un mínimo de 12 meses, de cara a garantizar la correcta instalación y optimización de la plataforma SIEM en tanto que el Ayuntamiento adquiere los conocimientos y experiencia para su gestión y operación de forma autónoma:

- Recopilación y tratamiento de eventos.
  - Velar por la correcta recolección de los eventos de las distintas fuentes, comprobando que se realiza una correcta recepción, filtrado, normalización y almacenamiento de los mismos en la plataforma de correlación.
  - Mantenimiento de la configuración de las políticas de correlación adecuadas para la generación de eventos correlados, creando nuevas políticas o aplicando modificaciones en las existentes.

- Monitorización y evaluación de alarmas.
  - Monitorización de las alertas en tiempo real para identificar qué eventos correlados deben convertirse en alarmas.
  - Evaluación del impacto sobre todas las alarmas generadas.
  - Identificación de la acción o acciones a realizar en base a la criticidad del incidente.

- Descarte de alertas, cuando sea considerada como falso positivo tras su correspondiente análisis. Además, se deberá revisar la configuración de las herramientas implicadas para evitar que se vuelva a generar un falso positivo asociado al mismo tipo de actividad identificada y descartada.

- Diseño y mantenimiento de nuevas políticas de correlación o adaptación de las existentes, en base a los requerimientos realizados por el Ayuntamiento y/o en base a la evaluación continua de los mecanismos de filtrado y correlación desplegados, así como del análisis manual de los eventos realizados de forma periódica.

- Comunicación de las alertas al personal designado por el Ayuntamiento, así como de las acciones de respuesta o remediación que pudieran corresponder.

- Atención de las solicitudes realizadas por el Ayuntamiento, con relación a cualquiera de los aspectos del servicio.

- Intercambio automático y fluido de incidentes con la Plataforma Nacional de Notificación y seguimiento de Ciberincidentes mediante la implantación y operación de la herramienta LUCIA del CCN-CERT que operara en modo federado con el de la Plataforma Nacional.

- La empresa adjudicataria deberá acreditar la relación de los servicios realizados en los últimos 3 años de gestión de servicios de centro de operaciones de seguridad (SOC), o similar, en la que se indique el importe, fecha y destinatario público o privado de los servicios. El importe anual referido al mejor ejercicio dentro de los últimos 3 años deberá ser igual superior al 70% de la anualidad media del contrato. La acreditación de este criterio se realizará a través de la aportación de documentación que acredite este cumplimiento (contratos). Se entenderá que los servicios son de naturaleza igual o similar al objeto del mismo,

aquellos contratos que tengan pero objeto la implantación y gestión de un Centro de Operaciones de Seguridad.

- Para poder dar los servicios con unas mínimas garantías se considera necesario que los servicios de despliegue e implantación se presten desde un DataCenter situado en el territorio nacional para evitar posibles latencias a la hora de los servicios y certificado al menos en TIER III. El Datacenter en el que se encuentre alojada la infraestructura del SOC deberá ser gestionado en base a los principales estándares de seguridad que permitan garantizar el cumplimiento de la normativa vigente. El adjudicatario deberá presentar una descripción de las instalaciones técnicas y la ubicación del lugar en el que prestará el servicio. El Datacenter deberá disponer de al menos las siguientes certificaciones de seguridad:
  - ISO 27001, certificación de gestión de seguridad de la información
  - ISO 20000, certificado de calidad de servicios TI
  - ISO 9001, certificación de sistemas de gestión de calidad de servicio
  - ~~Disponer de certificación MEDIA en el Esquema Nacional de Seguridad (ENS), por los servicios de seguridad objeto de esta licitación (SOC y CSIRT).~~

- El adjudicatario deberá ser una empresa certificada en ENS con nivel ALTO para la prestación de los servicios de SOC requeridos (Monitorización y Ciberseguridad.)
- El adjudicatario tendrá que asegurar a lo largo de toda la ejecución del contrato de un equipo mínimo con las certificaciones que se indican:
  - CSA (Analista SOC certificado v1)
  - CDPP (Profesional Certificado en Privacidad de Datos)
  - CEH (Hacker Ético Certificado)
  - CHFI (Investigador forense de piratería informática)
  - CISSP (Profesional certificado en seguridad de sistemas de información)

Se considera que estas son las titulaciones/certificado a nivel tecnológico mínimas necesarias para poder dar el servicio con unas mínimas garantías dentro del marco normativo actual en LOPDGDD, ENS y recomendaciones CCN.

2.1. Acreditación técnica y profesional de la empresa específica para la prestación de la adecuación al ENS.

Las empresas licitadoras deberán acreditar:

1. Experiencia demostrable en proyectos similares. Deberá aportar experiencia en los últimos 3 años, en al menos 10 entidades del ámbito local con una facturación mínima de cada uno de ellos de 10.000 Euros, en proyectos de adecuación al Esquema Nacional de Seguridad.

2. La empresa adjudicataria deberá disponer al menos de la certificación ENS de categoría Alta para la prestación de los servicios de consultoría requeridos.

3. Entre los componentes del equipo humano adscrito a dichos trabajos, deberán figurar como mínimo:

- Un responsable del proyecto. Titulado en Ingeniería en Informática o equivalente, con una experiencia de al menos 10 años como consultor en seguridad de la información, y debe tener como mínimo alguna de las siguientes certificaciones o titulaciones:
  - ✓ Máster relacionado con la seguridad de la información
  - ✓ Certificación CISA o CSIM.
  - ✓ Lead Auditor 27001

- Un consultor con titulación de Ingeniería en Informática o equivalente, con al menos 7 años como consultor en seguridad de la información y debe tener como mínimo una de las siguientes certificaciones:
  - ✓ Certificación CISA o CSIM.
  - ✓ Lead Auditor 27001

- Un consultor Licenciados en derecho, con al menos 5 años como consultor en protección de datos, y debe tener como mínimo alguna de las siguientes certificaciones o titulaciones:
  - ✓ Delegado de protección de datos certificado por ENAC-AEPD.
  - ✓ Máster relacionado con el Derecho de las TI.
  - ✓ Formación acreditada sobre ENS (mínimo 20 horas).

Mérida a fecha de firma electrónica

MOYA VASCO JUAN RAMON - DNI 09170693H

Firmado digitalmente por MOYA VASCO JUAN RAMON - DNI 09170693H
Fecha: 2023.03.20 11:08:05 +01'00'