PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA "IMPLANTACIÓN DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD DE LA RED CORPORATIVA DEL AYUNTAMIENTO DE SEVILLA (HISPALNET)"

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. Componente 11, Inversión 3, del PRTR, gestionado por el Ministerio de Política Territorial.

Contenido

1. INTRODUCCIÓN

Ante el contexto creciente en complejidad y número de los ciberataques a los que se ve expuesta la sociedad en la actualidad, agravado si cabe por la pandemia, es imprescindible que las Administraciones Públicas Locales puedan contar con las capacidades de un Centro de Operaciones de Ciberseguridad que les permita gestionar de forma adecuada la seguridad de sus infraestructuras, comunicaciones y servicios digitales prestados a empresas y ciudadanos, mejorando sus capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad.

Todo ello ligado a los requerimientos reflejados en el Esquema Nacional de Seguridad para GARANTIZAR los servicios prestados a la ciudadanía, PROTEGIENDO la información que estos servicios tratan, cuando se apoyan directa o indirectamente en medios electrónicos.

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

Todo ello es necesario, porque la implementación del ENS es la garantía para mantener la validez legal de las transacciones electrónicas desarrolladas por medios presenciales o telemáticos. Los incidentes relacionados con eventos en los Sistemas de Información del Organismo, así como una inadecuada custodia y gestión de la vigencia de los documentos electrónicos que intervienen en las transacciones electrónicas, pueden derivar en problemas legales y pueden constituir un serio inhibidor en el uso de medios electrónicos en la Administración.

El eslabón más débil de la seguridad es siempre el empleado, al que los ciberatacantes dedican especialmente su atención, por lo que cualquier estrategia completa de seguridad debe tener en cuenta su adecuada capacitación y concienciación en materia de seguridad y ciberamenazas (de los empleados públicos).

El proceso de modernización que se está llevando a cabo en el Ayuntamiento de Sevilla, conlleva obviamente la mejora y ampliación de los servicios digitales ofertados a la ciudadanía, así como la automatización de los procesos internos. Esto nos ha obligado tanto a la renovación y mejora de las infraestructuras, como a la renovación y ampliación de los sistemas de información y de los sistemas de atención y relación con la ciudadanía. Evidentemente en todo este proceso la ciberseguridad juega un papel esencial, por lo que es imprescindible contar con un Centro de Operaciones de Ciberseguridad adecuado a los nuevos servicios que se prestan, y adecuar la Política de Seguridad, que data del año 2014, a las nuevas circunstancias.

2. ALCANCE DEL PLIEGO

El Ayuntamiento de Sevilla constituyó formalmente la Red Corporativa Hispalnet que engloba al propio Ayuntamiento, todos sus OOAA y Empresas Municipales mediante acuerdo de Junta de Gobierno de 27 de julio de 2018.

Las Entidades que componen la red HISPALNET son:

- Ayuntamiento de Sevilla.
- Patronato del Real Alcázar.
- Agencia Tributaria de Sevilla.
- Gerencia Municipal de Urbanismo.
- Instituto Municipal de Deporte.
- Empresa Metropolitana de Abastecimiento y Saneamiento de Aguas de Sevilla, S.A (EMASESA).
- Empresa Municipal de Vivienda, Suelo y Equipamiento de Sevilla, S.A. (EMVISESA).
- Limpieza Pública y Protección Ambiental, S.A.M. (LIPASAM).
- Transportes Urbanos de Sevilla, S.A.M. (TUSSAM).
- Corporación de Empresas Municipales de Sevilla (CEMS).

Dicho conjunto de entidades se referirá, en adelante, indistintamente como Red Corporativa Hispalnet, red Hispalnet o Ayuntamiento de Sevilla, bien entendido que se refiere al conjunto de las anteriores.

La Red Corporativa HISPALNET es, en la actualidad, la base de la prestación de servicios al ciudadano, empleados municipales y visitantes, permite integrar todos los servicios por la misma infraestructura física sirve de soporte para la gestión unificada de todos los servicios del Ayuntamiento de Sevilla, sus Organismos Autónomos y Empresas Municipales, facilitando el acceso a las aplicaciones y bases de datos actuales, y permitiendo el desarrollo de aplicaciones y bases de datos comunes para el entorno municipal de Sevilla.

En esta licitación el Ayuntamiento de Sevilla busca, como objetivo principal, mejorar la situación en materia de Ciberseguridad de toda la red Hispalnet ya que, siguiendo la estrategia del proteger al eslabón más débil, el estado de seguridad de cualquiera de los miembros de la red afecta a la red Hispalnet completa.

El proyecto incluye el despliegue de las infraestructuras esenciales de un Centro de Operaciones de Ciberseguridad que incorporará los elementos fundamentales para su funcionamiento, como barreras de seguridad perimetral, sistema de recolección y correlación de logs, y también tecnología de detección y respuesta, contemplando además las tareas obligatorias para su integración en la Red Nacional de Centros de Operaciones de Ciberseguridad, así como la adecuación al Esquema Nacional de Seguridad que servirá como marco para promover un modelo homogéneo de la seguridad y permitirá establecer la política de seguridad en la utilización de medios, así como garantizar adecuadamente la seguridad de la información tratada.

Se persigue mejorar la Ciberseguridad de las redes y sistemas de información manejados por la red Hispalnet y las Entidades que la integran, para una mejor protección de la información tratada y de los servicios digitales prestados, en un contexto de exposición cada vez más intenso a la materialización de amenazas del ciberespacio, a los ciberincidentes, y que siguen una pauta de crecimiento en frecuencia, sofisticación, alcance y severidad del impacto.

En esta línea cabe el desarrollo de actuaciones encaminadas a mejorar la adecuación al Esquema Nacional de Seguridad (ENS) y orientadas a alcanzar la certificación de la conformidad de sus sistemas de información con esta norma.

En esta misma línea, caben inversiones para implantar servicios de ciberseguridad destinados a mejorar las capacidades de prevención, protección, detección y respuesta ante incidentes de ciberseguridad, contando con un sistema de seguimiento que permita, entre otras, monitorizar los principales indicadores en este ámbito.

Ante el incremento de la complejidad en la infraestructura IT y la gran variedad y sofisticación de los ataques a los cuales se encuentran expuesta las organizaciones, resulta imprescindible determinar el nivel de seguridad y de exposición frente a las amenazas, a través de una detección oportuna y gestión adecuada de los riesgos que afectan a los activos.

Finalmente, debe reforzarse la cultura de la seguridad en la organización mediante su integración en el proceso organizativo y considerarse un objetivo permanente de todo el personal. Para mantener y reforzar este nivel de madurez es necesario contar con herramientas de capacitación, concienciación y divulgación que, aprovechando las nuevas tecnologías, permitan disponer de mecanismos eficientes para la capacitación y formación de los usuarios en materia de seguridad de la información, de forma planificada, permanente y con conocimiento objetivo de los resultados obtenidos.

Todos los recursos hardware necesarios para la implantación de servicios y/o sistemas serán proporcionados por el Ayuntamiento de Sevilla salvo aquellos que, por su diseño, se sirvan desde nubes públicas o privadas. El licitador deberá especificar completamente las capacidades del hardware necesario para cada servicio y/o sistema.

Del mismo modo el Ayuntamiento busca rebajar, en el uso futuro, los recursos presupuestarios asociados a las licencias de los servicios a utilizar, teniendo como prioridad el uso de herramientas de libre uso para la Administración y/o el uso de licencias Open Source.

3. OBJETIVOS PRINCIPALES

El objetivo principal del proyecto abordado en esta línea de Ciberseguridad es **garantizar la seguridad** de las infraestructuras, comunicaciones y servicios digitales prestados por la Red Corporativa Hispalnet y mejorar las capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad. Para ello se propone el **despliegue de las infraestructuras base de un Centro de Operaciones de Seguridad** que preste servicios horizontales de ciberseguridad aumentando la capacidad de vigilancia y detección de amenazas en las transacciones de los sistemas de información y comunicaciones de la Red Corporativa Hispalnet, así como la mejora de su capacidad de respuesta ante posibles ataques.

Se pretende mejorar la **protección en el ámbito de la seguridad perimetral** frente a ciberamenazas mediante la correcta gestión de su configuración, administración, control y gestión. Se marca como otro de los objetivos la evolución hacia un modelo integral que favorezca la **coordinación interorganizacional e interdepartamental ante incidentes** de seguridad complejos y la **compartición e intercambio de inteligencia de ciberseguridad**, fijando para ello la implantación de herramientas, procesos y servicios de vigilancia, prevención, detección, análisis, respuesta y asesoramiento.

Con el alcance de la propuesta se contribuirá a mejorar la situación de seguridad de la Red Corporativa Hispalnet y su grado de conocimiento

El Proyecto persigue también el cumplimiento de la regulación en materia de seguridad de la información, concretamente del Esquema Nacional de Seguridad (ENS), incluyendo los análisis y estudios necesarios para determinar las carencias en relación con el cumplimiento y, sobre esta base, proponer las adaptaciones, modificaciones y configuraciones necesarias en la infraestructura, aplicaciones, servicios, procesos y procedimientos para garantizar el cumplimiento de las exigencias del ENS. Si aplica, se perseguirá obtener la certificación de conformidad correspondiente.
Asimismo, se pretende obtener más visibilidad e información sobre vulnerabilidades, fallos de configuración e incidentes, a la vez que se mejoren las capacidades de protección y respuesta.

Finalmente, el Proyecto pretende promover y reforzar la cultura de seguridad del Ayuntamiento de Sevilla a través del desarrollo e implementación de un Plan tanto de Concienciación y Sensibilización como de Formación en el que se transformarán e interiorizarán comportamientos y hábitos en seguridad en el día a día de los empleados. Con ello, conseguimos una mayor percepción del riesgo, resultando en la disminución de incidencias e incidentes de seguridad.

Se incluye, como anexo al presente pliego de prescripciones técnicas, las características técnicas y las volumetrías asociadas a las Entidades constituyentes a la red Hispalnet en lo relativo a los requisitos del Pliego. Las empresas licitadoras podrán encontrar dicha información en el "**Anexo I. Especificaciones técnicas y volumetrías de las Entidades de Hispalnet**", **que será entregado previa firma del correspondiente acuerdo de confidencialidad**, puesto que se trata de información de carácter reservado que no debe difundirse públicamente.

4. PLAN DE IMPLEMENTACIÓN

El proyecto contempla tres grandes Actuaciones que incluyen:

1. Despliegue del Centro de Operación de Seguridad.
2. Adecuación al ENS del Ayuntamiento de Sevilla.
3. Plan de formación y concienciación en Ciberseguridad.

Incluimos a continuación los suministros, configuraciones, características mínimas y acciones a realizar por el adjudicatario, en cada una de estas actividades.

4.1 Actuación 1: Despliegue del Centro de Operación de Seguridad

La transformación digital del Sector Público ha de ir acompañada de medidas organizativas y técnicas de seguridad que protejan la información manejada y los servicios prestados, proporcionadas a los riesgos provenientes de acciones malintencionadas o ilícitas, particularmente de las ciberamenazas, errores o fallos y accidentes o desastres.

Los servicios a implantar dentro de esta Actuación y los requisitos de integración de éstos con la Red Nacional de Centros de Operaciones de Ciberseguridad son los siguientes:

- Implantación y configuración de la herramienta de gestión de incidentes LUCIA
- Despliegue de las herramientas CLAUDIA y MicroCLAUDIA
- Suministro e implantación y ajuste de plataforma de recolección y correlación de logs. Implantación de herramientas que sirvan para la detección, análisis ante posibles incidentes de seguridad
- Integración de las infraestructuras existentes al SIEM
- Implantación de cuadro de mandos de ciberseguridad.
- Establecer un Plan de Gestión y Operaciones en materia de ciberseguridad

Como normal general en cuanto a la implantación de servicios y herramientas, todas las soluciones actuales generarán registros para su remisión a los sistemas de tratamiento de logs (SIEM, sistemas de salud y monitorización, etc.) para su posterior análisis. Además, contarán con sistemas de actualizaciones de software que permitan configurar la fuente de las actualizaciones.

4.1.1 Implantación y Configuración de la herramienta de gestión de incidentes LUCIA del CCN-CERT que operará en modo federado con el de la Plataforma Nacional para el Intercambio automático y fluido de ciberincidentes con la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

Con el fin de poder gestionar de un modo eficaz los incidentes en cualquier organismo público (sobre todo aquellas que colaboran con el CCN-CERT) el Adjudicatario implantará la última versión disponible de la herramienta LUCIA publicada por el CERT Gubernamental Nacional. Gracias a ella, es posible comunicar y sincronizar los incidentes provenientes de una entidad con LUCIA Central, la instancia del CCN-CERT desde la que se gestionan todos los ciberincidentes.

La herramienta permite, además, cumplir con dos de los requisitos del Real Decreto 311/2022 de 3 de mayo por el que se regula actualmente el 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).

Otras ventajas de la herramienta son:

- Contar con una herramienta interna parametrizada para la gestión de incidentes Hispalnet y las Entidades que la integran
- Tener una plataforma única y distribuida para la gestión de incidentes
- Contar con un lenguaje común de peligrosidad y clasificación de incidentes
- Mantener la trazabilidad y el seguimiento de los incidentes.
- Automatizar las tareas (notificaciones, recordatorios, cierres automáticos...)
- Construir una base de datos de conocimiento
- Soporte y actualizaciones de LUCIA por parte del CCN-CERT
- Integración con otras herramientas del CCN-CERT como REYES o MARTA

Las tareas asociadas a este punto serán las de instalación, implantación y el traspaso de conocimiento de administración de la herramienta LUCIA. La instalación se realizará en infraestructuras proporcionadas por el Ayuntamiento de Sevilla y la implantación contemplará la dimensión de Hispalnet y su constitución en forma de Entidades.

Una vez instalada LUCIA, el proyecto permitirá las siguientes tareas de administración:

- 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 (en particular, integración con la herramienta de ticket de la red Hispalent, Proactivanet).
- Copias de seguridad utilizando las herramientas propias del Ayuntamiento de Sevilla.
- Realizar la integración con Integración con la herramienta del CCN-CERT REYES.

4.1.2 Despliegue de las herramientas CLAUDIA/CARMEN y microCLAUDIA del CCN-CERT en toda la organización

CLAUDIA es una solución de endpoint integrada con la herramienta CARMEN que permite tener una visión más completa de lo que ocurre dentro de una red, siendo su objetivo principal la detección de malware complejo y movimiento lateral relacionado con APT..

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 de Sevilla 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 de Sevilla. Asimismo, el servicio ofrece la actualización automática de las mismas para cubrir adaptaciones a las nuevas formas de ejecución del ransomware.

CARMEN es la solución de threat hunting del CCN para la identificación de Amenazas Persistentes Avanzadas (APT) y actividades hostiles en la infraestructura. Adquiere, procesa y analiza información para la elaboración de inteligencia a partir del tráfico de red y de los puestos de usuario y servidores. Para su funcionamiento, requiere de la instalación de un agente en todos los puestos de usuario de la organización, CLAUDIA. CARMEN se distribuye libre de costes de licencia para todos los organismos públicos.

Las tareas incluidas en este punto serán:

- Inventariado del parque objetivo (ordenadores de trabajo, servidores…)
- Descarga del SW CLAUDIA, microCLAUDIA y CARMEN
- Generación y prueba del plan de implantación de dichas herramientas: manual o automatizado (vía GPO)
- Implantación de los agentes apropiados
- Verificación del despliegue sobre el parque inventariado
- Verificación del funcionamiento de las herramientas

4.1.3 Suministro e Implantación de una Plataforma de recolección y correlación básica de los registros de trazabilidad (logs) necesarios para la vigilancia (Mediante productos recogidos en el catálogo CCN-STIC 105).

El objetivo principal de contar con un sistema con capacidad de recolección y correlación básica de logs es la detección de cualquier violación o amenaza inminente de la Política de Seguridad de la red HISPALNET y las Entidades que la integran, cuya dirección 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) incluido en el alcance del presente apartado donde se integran los logs generados por los activos adscritos al sistema.

Dentro del mercado se encuentran varias posibilidades de suministro del software de SIEM y de almacenamiento de la información recogida. Se permite ofertar soluciones que puedan corresponder a las siguientes categorías:

- Software bajo licencia privativa y almacenamiento bajo licencia privativa.
- Software bajo licencia privativa y almacenamiento bajo licencia Open Source.
- Software con licencia de uso gratuita para la Administración Pública u Open Source con almacenamiento bajo licencia Open Source.

En caso de ofertar soluciones que requieran del uso de licencia privativa por suscripción el Licitador incluirá en su oferta dicha licencia por un plazo mínimo de tres años desde la fecha de aceptación de los trabajos.

Se admitirán soluciones de despliegue en las organizaciones, en modo on-premise, virtual o entorno cloud. En el caso de ofertarse un entorno cloud cualquier coste adicional derivado de dicho despliegue correrá a cargo del Adjudicatario durante los tres años siguientes a la fecha de aceptación de los trabajos.

Se tendrán que realizar las labores de análisis, diseño e implementación del sistema SIEM ofertado, listado en el catálogo CCN-STIC 105 a fecha de presentación de oferta, y que debe estar 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 adjudicatario dará de alta los activos en el SIEM, generando los trabajos de desarrollo necesarios para ello. La recolección de eventos se podrá realizar por varias formas, de las cuales son como mínimo necesarias el uso de Agente específico, lectura de Syslog y SNMP

Este sistema SIEM dispondrá de varios componentes para garantizar la recopilación y las capacidades de recolección:

- **Capa de recolección de datos:** Se desplegarán en la infraestructura del Ayuntamiento de Sevilla las sondas necesarias para recolectar y normalizar los distintos tipos de fuentes para su posterior envío e ingesta. Este componente se ubicará lo más cerca posible de la fuente de la que se va a ingestar para que la transferencia del dato ocurra de manera eficiente y garantizada. Entre las características más relevantes de la sonda están: Buffering, encriptación y compresión.

- **Capa de monitorización, análisis y detección:** En la capa de monitorización, análisis y detección, se utilizará una solución mediante la cual se obtendrán capacidades para la gestión de datos operacionales en tiempo real durante todo su ciclo de vida, desde la ingesta, tratamiento, visualización y archivado, en los casos que así lo requiere.

- **Capa de custodia**: Esta capa permite el almacenamiento y visibilidad de datos a largo plazo, si fuera preciso para una investigación.

La implantación del sistema requerirá mínimo de las siguientes fases:

- *Diseño detallado.* Esta actividad realizará la identificación de fuentes de logs y definición de la arquitectura final, seleccionando la ubicación, direccionamiento y conectividad de los diferentes componentes de la herramienta SIEM a desplegar.

- *Despliegue y configuración inicial.* En base al diseño detallado, se realizará el despliegue y configuración inicial del HW o SW

- *Configuración y creación de plugins.* Esta actividad se encargará de configurar y crear, en caso de ser necesario, los plugins que permitan la recolección de los logs de las plataformas incluidas en el alcance del proyecto. En todo caso, el Adjudicatario deberá realizar las tareas de programación y normalización de datos para la ingesta correcta desde las diferentes fuentes definidas.

- *Configuración y ajustes de política de correlación*. Una vez se comiencen a recibir logs de los distintos dispositivos en la plataforma de prestación del servicio, se realizará el despliegue y configuración del catálogo de directivas de seguridad en función de las tecnologías incluidas en el alcance del proyecto sirvan para la detección, análisis ante posibles incidentes de seguridad.

- *Plan de pruebas y puesta en producción*. Se ejecutará el plan de pruebas definido en fase de diseño detallado.

4.1.4 Integración de las infraestructuras existentes al SIEM

El adjudicatario deberá proporcionar una plataforma para la recolección y análisis en tiempo real de las alertas de seguridad generadas por los componentes hardware o software que conforman los diferentes sistemas de información y telecomunicaciones de HISPALNET.

El servicio incluirá las actualizaciones periódicas del mismo. El personal de seguridad de

HISPALNET tendrá acceso a la plataforma a nivel totalmente funcional (creación de secuencias de búsqueda y correlación de eventos, elaboración de cuadros de mando, configuración y generación de alertas, etc.).

Dicha plataforma será aprovisionada, instalada, configurada y optimizada por el Adjudicatario para, posteriormente ser operada y gestionada por el futuro SOC de HISPALNET.

La plataforma deberá recoger y centralizar los registros y logs que contengan información y eventos de seguridad, normalizará, categorizará, agregará, correlacionará y almacenará dichos eventos por un período de retención inicial de 365 días, detectando incidentes de seguridad y generando alertas.

Dispondrá de una herramienta de toma proactiva de decisiones y proporcionará una única consola web accesible que permita a HISPALNET realizar consultas y generar informes y cuadros de mando a partir de las políticas y métricas de riesgo definidas.

La implementación de este servicio, por parte del Adjudicatario, deberá permitir mantener un equilibrio entre la detección de alertas de seguridad y el esfuerzo preciso para solucionarlas y documentarlas.

En general, deberá:

- Proporcionar un análisis de los eventos en tiempo casi real.
- Correlacionar y analizar información compleja procedente de diferentes fuentes y sistemas (entornos heterogéneos como activos de red, dispositivos de seguridad, sistemas operativos, aplicaciones, bases de datos y productos de gestión de accesos e identidades.).
- Generar alertas basadas en anomalías observadas y en cambios en el comportamiento de los flujos de red y en los eventos de seguridad, así como poder añadir anomalías definidas por HISPALNET.
- Proporcionar alertas en base a políticas establecidas (por ejemplo, tráfico de mensajería instantánea no permitido, almacenamiento en la nube no permitido, uso de protocolos no autorizados, etc.). y aplicaciones potencialmente peligrosas (file sharing, P2P, etc.).
- Configurar y transmitir alertas a través de diferentes mecanismos hacia otras soluciones de ticketing y herramientas de terceros.
- Establecer sinergias con herramientas de seguridad de terceros (feeds de inteligencia, plataformas de Cyber Threat Intelligence, etc.).
- Correlacionar resultados proporcionados por herramientas de escaneos de vulnerabilidades integradas o de terceros.
- Monitorizar y alertar cuando se produzca una interrupción en la recopilación de registros de una fuente o dispositivo supervisado.

- Descubrir y clasificar automáticamente los activos de la red mediante diferentes técnicas de escaneo (ping, fingerprinting de puertos y de sistemas operativos, etc.) y de consultar a repositorios de activos externos (como Directorio Activo, LDAP, CMDB, etc.).

- Soportar y mantener un histórico de la actividad de la autenticación de usuarios en función de cada activo, que permita la generación de informes de auditoría y trazabilidad.

- Permitir la correlación de valores añadidos en el tiempo (por ejemplo, enviar una alerta cuando una IP origen envía más de un volumen de datos configurado a un solo servicio publicado en una IP destino desde una ventana de tiempo configurada).

- Proveer información relacionada con los perfiles de tráfico en términos de número de bytes, frecuencia de paquetes, número de activos en comunicación por aplicación, puertos protocolos, amenazas u otros posibles puntos de monitorización en la red.

- Ser capaz de detectar ataques de tipo DoS (Denial of Service) y DDoS (Distribute Denial of Service).

- Ser capaz de detectar y mostrar el tráfico relacionado con una amenaza específica observada en la red.

- Soportar la creación de perfiles de tráfico asociados con el diseño lógico de la red, tanto a nivel de dirección IP individual como de rango de redes (por ejemplo, subred/CIDR).

- Ser capaz de perfilar comunicaciones procedentes de, o dirigidas hacia internet por regiones geográficas y en tiempo real.

- Permitir la creación de perfiles claramente independientes y diferenciados del tráfico local y del tráfico con origen y destino a internet.

- Soportar la creación de perfiles de tráfico basados en direcciones IP, grupos de direcciones IP, parejas de direcciones IP origen/destino, etc.

- Permitir el acceso a los detalles de los eventos de seguridad y de los flujos de red almacenados, al menos durante tres meses en caliente (datos a los que se accede de mantera inmediata, por ejemplo para la correlación en tiempo real, por lo que deben almacenarse en almacenamiento rápido) y doce meses en frio (datos a los que no se accede con frecuencia o que no se usan activamente, pero que se pueden traspasar a datos en caliente mediante un sencillo proceso de recuperación, con objeto de garantizar el análisis forense. Se pueden almacenar en un medio de almacenamiento más lento y económico).

Los logs, una vez configurados, estarán disponibles para realizar consultas y análisis forense para investigar incidentes de forma ágil, buscar indicadores de amenazas persistentes avanzadas (APT) y facilitar la superación de las debilidades detectadas por las auditorías de cumplimiento. Se combinará el acceso a datos históricos con la posibilidad de ver los detalles de cada evento específico.

La plataforma permitirá incluir las fuentes de información que HISPALNET decida emplear para llevar a cabo la monitorización, de modo que sea sencilla y transparente la inclusión de nuevas fuentes como consecuencia de los cambios que se puedan producir en la infraestructura con el paso del tiempo e incluirá como mínimo el listado final de los activos (servidores, bases de datos, aplicaciones, etc.) definidos como esenciales en el Anexo I.

El personal técnico del adjudicatario se encargará de incorporar las fuentes de información, realizando para ello las labores de programación y normalización de datos que sean precisos. La plataforma deberá ser compatible con amplia gama de dispositivos y productos de diferentes tipologías y fabricantes, así como soportar un volumen de, al menos, 10000 EPSs.

Además, como parte del despliegue de la herramienta, el adjudicatario elaborará y configurará una completa relación de casos uso de uso, basados en las fuentes disponibles, que generen alertas ante eventos de seguridad significativos. Del mismo, elaborará una completa relación de la configuración de alarmas e informes.

4.1.5 Implantación de Cuadro de Mandos de Ciberseguridad.

El adjudicatario realizará, tomando en cuenta todos los servicios e infraestructuras desplegadas, la implantación de un cuadro de mandos de ciberseguridad que contemple:

- La definición, diseño e implementación de indicadores y alarmas de seguridad, tanto a nivel de gestión como de tecnología.

- Los Requerimientos y Objetivos de Seguridad de la Información Definición de Métricas de Seguridad.

Para ello deberá suministrar una plataforma de gestión y visualización estructurada que soporte el cuadro de mandos de ciberseguridad

4.1.6 Establecer un Plan de Gestión y Operaciones en materia de ciberseguridad

Con la implantación de los sistemas anteriores, más aquellas disponibles actualmente (como la herramienta de ticketing Proactivanet), la Red Corporativa Hispalnet estará en disposición de gestionar la ciberseguridad de sus infraestructuras desde su futuro SOC.

A este objeto, el adjudicatario deberá elaborar una documentación completa para la gestión de la ciberseguridad por parte de dicho SOC, debiendo contener, al menos, los siguientes documentos:

- Estructura de gobierno del futuro SOC de Hispalnet; definición de roles y responsabilidades.

- Procedimiento de gestión de ciberincidentes; que incluya todas las fases de gestión del ciclo de vida del ciberincidente, (detección y análisis, taxonomía y categorización, priorización, escalado y coordinación, contención, erradicación y respuesta, y actividades post-incidente).

- Libro de respuesta (Playbook) a ciberincidentes tipo; workflow para el manejo de los

ciberincidentes.

- Procedimiento de gestión de vulnerabilidades; que incluya todas las fases de gestión del ciclo de vida de la vulnerabilidad, (detección, evaluación e inventariado de vulnerabilidades, categorización y priorización, plan de remediación, notificación y reporte de vulnerabilidades).
- Procedimiento de gestión de la capacidad; que incluya todas las fases de gestión del ciclo de la capacidad (monitorización de rendimiento y throughput de los servicios, elaboración de previsiones en función de la demanda, gestión de incidentes en la infraestructura, planificación de la capacidad y actividades de optimización, planificación, ejecución de pruebas de capacidad, informes y gestión de seguimiento, etc.).
- Procedimiento de gestión de la disponibilidad; que incluya todas las fases y requisitos para garantizar la continuidad y recuperación del servicio de SOC (Plan de contingencia, Plan de Recuperación, etc.).
- Desarrollo del catálogo de servicios del futuro SOC de Hispalnet; detalle del servicio, procesos y flujos
- Plan de entrenamiento y formación del personal del SOC.

Finalmente, deberá redactar cualquier otra documentación (norma, procedimiento, etc) que se estime pertinente y todas las instrucciones técnicas operativas que complementen dichos procedimientos, para disponer de un exhaustivo cuerpo documental para la gestión del futuro SOC de Hispalnet. La elaboración de la documentación tendrá en cuenta las mejores prácticas, así como los marcos de referencia universalmente aceptados (series ISO 27000 e ISO 20000, ITIL, Guías STIC, Guías NIST, Guías SANS, OWASP SOC Framework Project, etc.), así como las regulaciones aplicables en materia de ciberseguridad (ENS, NIS, PIC, RGPD u otras).

4.2 Actuación 2: Adecuación al ENS

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El ENS contempla unos Principios Básicos que definen los fundamentos que deben regir toda acción orientada a asegurar la información.

Así mismo, el ENS establece unos Requisitos mínimos que deben cumplirse para asegurar una protección adecuada de la seguridad de la información. Estos Requisitos se desarrollan y aplican mediante la implementación de las Medidas de Seguridad incluidas en el Anexo II del ENS.

Los trabajos para la elaboración del Plan de Adecuación de Ayuntamiento de Sevilla al ENS incluirán:

- Revisar la política de seguridad de la información de Ayuntamiento de Sevilla, para identificar las necesidades de modificar o incluir elementos para dar cumplimiento a las exigencias del ENS en esta materia.
- Categorizar los sistemas de información de Ayuntamiento de Sevilla atendiendo a la valoración de la información manejada y de los servicios prestados.
- Realizar un análisis de los riesgos para la seguridad de la información, incluyendo la valoración de las medidas de seguridad existentes.
- Elaborar la Declaración de Aplicabilidad de las medidas del Anexo II del ENS y someterla a aprobación.
- Verificar y evaluar el grado de cumplimiento de las medidas actualmente implementadas en Ayuntamiento de Sevilla en relación con las medidas identificadas en la Declaración de Aplicabilidad.
- Elaborar el Plan de Adecuación de Ayuntamiento de Sevilla para la mejora de la seguridad de la información, a partir del diferencial de cumplimiento con el ENS y otras oportunidades de mejora identificadas.
- Elaborar un cuadro de mandos para el seguimiento del grado de implementación del Plan de Adecuación del Ayuntamiento de Sevilla y del cumplimento del ENS.
- Elaborar una proyección del estado de riesgo prevista tras la aplicación del Plan de Adecuación.

Todas las actividades anteriores se sustentarán sobre las herramientas del CCN PILAR y AMPARO que deberán ser implantadas mediante los trabajos del Adjudicatario.

La adecuación al Esquema Nacional de Seguridad tendrá la metodología y modelos establecidos en:

- CCN-STIC-883 Guía de implantación del ENS para Entidades Locales
- Anexo III de la anterior guía. Plan de Adecuación Diputaciones, Cabildos, Consejos insulares u órgano competente equivalente

En concreto se realizarán las siguientes tareas:

- Análisis detallado del estado de situación, definición de la estrategia de mejora de la adecuación al ENS y planificación de la adecuación
- Asegurar la recogida y estructuración de la información para el uso de las herramientas del CCN, AMPARO y REYES
- Implantación de la herramienta del CCN PILAR
- Identificación y Categorización de los activos y sus deficiencias en materia de ciberseguridad
- Definición del Plan de Mejora en base a las deficiencias encontradas, su gobernanza y el desarrollo normativo necesario.

4.2.1 Análisis detallado del estado de situación, Definición de la estrategia de mejora de la adecuación al ENS y Planificación de la Adecuación.

El ENS establece la necesidad de definir formalmente una Política de Seguridad de la Información que contemple:

- Los objetivos o misión de la organización.
- El marco legal y regulatorio en el que se desarrollarán las actividades.
- Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

En esta Actuación el Adjudicatario abordará el análisis de las Políticas de Seguridad y cuerpo normativo de HISPALNET y las Entidades que la integran para identificar aquellos aspectos establecidos en el ENS y no suficientemente desarrollados en éstas.

En particular, para cada Entidad se realizará un análisis de la organización para la seguridad y los roles establecidos, teniendo en cuenta lo requerido en el ENS para las distintas funciones implicadas en los sistemas, servicios, y seguridad de la información.

El análisis y propuestas relativos a la Política de Seguridad se realizarán teniendo en cuenta lo establecido en la “Guía de Seguridad CCN-STIC 805 Política de Seguridad de la Información” u otras guías vigentes del catálogo STIC.

Como resultado de esta fase se elaborará una Política de Seguridad de la Información de HISPALNET y una específica para cada Entidad.

Finalmente se realizará en esta fase:

- La definición de la estrategia de mejora de adecuación al ENS siguiendo lo establecido en la Guía CCN-STIC 883 Implantación del ENS para Entidades Locales
- La Planificación de dicha Adecuación al ENS en las fases y alcance establecidas en el Proyecto

4.2.2 Asegurar la recogida y estructuración de la información para el uso de las herramientas del CCN, AMPARO y REYES.

El Adjudicatario realizará, en colaboración con el Responsable de cada Entidad, los trabajos de acopio y análisis de información para dar respuesta a la encuesta anual INES, solución desarrollada por el CCN para la gobernanza de la ciberseguridad, que permite evaluar regularmente el estado de la seguridad de los sistemas TIC de las entidades y su adecuación al Esquema Nacional de Seguridad (ENS). Estos trabajos se realizarán sólo para el ejercicio el curso.

El siguiente paso será la implantación de medidas de seguridad, a través de las soluciones del CCN AMPARO y REYES.

AMPARO es una solución centralizada, desarrollada por el CCN, para la gobernanza de la ciberseguridad, que permite la implantación y gestión de la seguridad en entidades y organismos. Incorpora diversas funcionalidades para facilitar estos procesos sirviendo de asistente para los mismos, evaluando automáticamente la conformidad del sistema y orientando al usuario en las fases de certificación y gestión continua de la seguridad.

El Adjudicatario realizará, en colaboración con el Responsable de cada Entidad, los trabajos necesarios para mantener actualizada la Plataforma AMPARO para cada Entidad. Estos trabajos se realizarán sólo para el ejercicio el curso.

El Adjudicatario utilizará adicionalmente el asistente creado por el CCN para llevar a cabo todas las acciones relacionadas con la creación de un Plan de Adecuación para priorizar y planificar las tareas a realizar en las primeras fases de la adecuación al ENS. La empresa adjudicataria deberá comprobar que se puede:

- Determinar el Alcance de la Certificación, mediante la identificación de los servicios prestados y los sistemas en los que están alojados.
- Categorizar el Sistema, atendiendo a la valoración de las dimensiones de seguridad de los servicios prestados y de la información que manejan.
- Obtener la Declaración de Aplicabilidad Provisional.
- Integración con INES-AR para llevar a cabo o revisar, en su caso, el Análisis de Riesgos, incluyendo la valoración de las medidas definidas en la Declaración de Aplicabilidad.
- Validar la Declaración de Aplicabilidad definitiva y/o Perfil de Cumplimiento Específico.
- Preparar y elaborar la Política de Seguridad, incluyendo la organización del Comité de Seguridad.

La empresa adjudicataria deberá comprobar que esta herramienta permitirá en fases posteriores de evolución elevar el grado de adecuación de la Red Corporativa Hispalnet al ENS, entre otras cosas:

- Llevar a cabo el proceso de implantación y así adecuarse al ENS de forma guiada gracias a su Asistente de Implantación, que señala los pasos que se deben seguir, muestra ayudas a lo largo de todo el proceso y evalúa automáticamente la conformidad del sistema para detectar carencias.

- Evaluar el sistema y obtener automáticamente la Declaración de Conformidad del sistema para categoría BÁSICA del ENS, o solicitar una Auditoría de Conformidad a una Entidad de Certificación acreditada.
- Descargar desde la sección de Soporte todos los modelos de procedimientos y normativas necesarios para la adecuación al ENS, y gestionar la documentación del marco normativo.
- Gestionar la Conformidad, mantener la comunicación con la entidad auditora, ver el estado del sistema, y facilitar todo el proceso de auditoría.
- Gestionar la Seguridad del sistema, donde será posible llevar a cabo los registros de usuarios, registros de soportes, formación, y cualquier otro registro necesario para mantener la seguridad en el ENS.

REYES es una solución centralizada, desarrollada por el CCN, para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas. A través de este portal centralizado de información puede realizarse cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes. Una información contextualizada y correlacionada con las principales fuentes de información, tanto públicas como privadas.

El Adjudicatario realizará, en colaboración con el Responsable de cada Entidad, los trabajos necesarios para integrar la herramienta como parte de los protocolos de respuesta a los Ciberincidentes.

4.2.3 Implantación de la herramienta del CCN PILAR

El Adjudicatario instalará la herramienta PILAR del CCN en su versión PILAR RM - Análisis y Gestión de Riesgos que permitirá el análisis de los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (accountability)

4.2.4. Identificación y Categorización de los sistemas de información

El Adjudicatario llevará a cabo las labores de identificación de los activos establecidos en su oferta, su categorización, analizará sus riesgos, etc. siguiendo lo establecido en el ENS. En concreto:

A. Realizar la Identificación de activos

Para cada entidad se verificará si existe una adecuada identificación y categorización de los sistemas de información, en cuyo caso se revisará y actualizará, o bien si no se existiera, se elaborará el correspondiente inventario que se empleará posteriormente para el desarrollo del mapa de dependencias y el análisis de riesgos.

En primer lugar, se deberá realizar una labor de inventariado de servicios electrónicos suministrados en materia de administración electrónica, teniendo que identificar para ello los siguientes aspectos:

- Organismos y servicios electrónicos incluidos según el alcance de la propuesta. Para cada uno de ellos se deberá inventariar:
    - Conjunto de procedimientos o servicios electrónicos propios contemplados.
    - Conjunto de procedimientos o servicios electrónicos de terceros u otros organismos de la Administración utilizados.
- Tratamientos de datos de carácter personal realizados en la prestación de los servicios incluidos en el alcance de la propuesta.
- Sistemas de información propios que sustentan dichos servicios e informaciones, y sus categorías ENS.
- Sistemas de información horizontales y corporativos que sustentan dichos servicios e informaciones, y sus categorías ENS.
- Activos de soporte de las capas de aplicación y tecnología que constituyen las dependencias de esos sistemas de información.

Como resultado de esta fase se obtendrá un detallado Mapa de dependencias en la herramienta PILAR, que permita llevar a cabo los trabajos subsiguientes.

B. Realizar la Categorización de sistemas

En aplicación del principio de proporcionalidad del ENS, las medidas de seguridad, deben ser proporcionadas a la naturaleza de la información que se maneja, de los servicios que se prestan y de los riesgos a los que están expuestos.

Para ello, el ENS contempla la clasificación de los sistemas en tres categorías, BÁSICA MEDIA y ALTA, en función del impacto que tendría un incidente que afectara a la seguridad de la información o los servicios, en alguna de las dimensiones de seguridad: autenticación, integridad, confidencialidad, disponibilidad y trazabilidad.

Este impacto se mide atendiendo a la repercusión que tendría el incidente para la organización respecto a:

- Alcanzar sus objetivos.
- Proteger los activos a su cargo.
- Cumplir sus obligaciones diarias de servicio.
- Respetar la legalidad vigente.
- Respetar los derechos de las personas.

Para realizar la categorización del sistema de información de HISPALNET se partirá del inventario de activos y Mapa de dependencias elaborado con los trabajos de identificación de activos.

El ENS basa el análisis de la categorización en determinar qué consecuencias o daños podría provocar un incidente de seguridad. Para determinar el impacto que tendría sobre la organización un

incidente de seguridad que afectara a un Sistema de Información se tendrán en cuenta cada una de las siguientes dimensiones de seguridad:

- Disponibilidad [D]
- Autenticidad [A]
- Integridad [I]
- Confidencialidad [C]
- Trazabilidad [T]

La información y los servicios se valorarán para determinar si los requisitos de seguridad a aplicar son de nivel ALTO, MEDIO o BAJO en cada una de las dimensiones de seguridad.

Esta valoración realizará conforme a lo establecido en el Anexo I del ENS, y teniendo en cuenta las pautas y criterios indicados en la "Guía de Seguridad CCN-STIC 803 Valoración de los Sistemas".

Como producto de esta fase, se elaborará un Informe de Valoración y Categorización del Sistema con el detalle de los niveles de seguridad alcanzados en cada una de las dimensiones antes indicadas (D, A, I, C y T) para cada información y servicio analizado, y con la categoría asignada a cada sistema considerado.

C. Realizar el Análisis de Riesgos

El análisis de riesgos permite enfocar los esfuerzos y los recursos de seguridad sobre los aspectos en los que resultan más necesarios, por lo que resulta esencial para la eficacia y la eficiencia de un sistema de seguridad.

El principio del ENS de gestión basada en riesgos persigue el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad

De esta forma, tras la selección de las medidas apropiadas de acuerdo al ENS, será posible graduarlas o asignarles un determinado nivel (p. ej. para el control del acceso a un sistema de información, decidir entre usar un mecanismo de usuario/contraseña, tarjeta con certificados, o sistemas biométricos de identificación).

El ENS exige la utilización de una metodología fundamentada y reconocida para la realización del análisis de riesgos. En esta fase se realizará un análisis de riesgos realizados desde la perspectiva del ENS. Para ello se utilizará, como ya se ha indicado, la metodología MAGERIT, apoyada en la herramienta PILAR.

De esta forma y tras valorar el estado actual de las salvaguardas existentes, será posible determinar

el nivel de riesgo residual actual para cada amenaza y activo analizado.

Teniendo en cuenta los criterios establecidos para el tratamiento y gestión del riesgo en función del nivel alcanzado (retener, mitigar, transferir, o evitar), los resultados del análisis de riesgos permitirán tomar decisiones en relación a:

- Validar el conjunto de medidas de seguridad implantado.
- Detectar la necesidad de medidas adicionales.
- Justificar el uso de medidas de protección alternativas.

Como producto de esta fase, se elaborará un Informe de Revisión de Análisis de Riesgos, con el detalle de los niveles de riesgo alcanzados, así como la identificación de los riesgos que alcanzan niveles no tolerables que requieren un tratamiento.

D. Elaboración de la Declaración de Aplicabilidad

El cumplimiento de los requisitos mínimos establecidos en ENS se logra mediante la implementación de las medidas de seguridad aplicables indicadas en su Anexo II.

Para seleccionar las medidas aplicables se tendrán en consideración:

- Los activos que constituyen el sistema.
- La categoría asignada al sistema.
- Las decisiones que se adopten para gestionar los riesgos identificados.

Teniendo en cuenta estas consideraciones, en esta fase se revisarán todas las medidas indicadas en el Anexo II del ENS para determinar su aplicabilidad a los Sistemas de Información del Ayuntamiento de Sevilla. Para ello se contemplarán los criterios establecidos en el propio Anexo II del ENS, así como las recomendaciones del documento CCN-STIC 804 Guía de Implantación.

Como resultado de esta fase se elaborará la Declaración de Aplicabilidad, que identificará la relación de medidas de seguridad seleccionadas.

E. Evaluación inicial del cumplimiento del ENS

En esta fase se realizará una verificación para evaluar el diferencial entre las medidas establecidas en la Declaración de Aplicabilidad, y las medidas actualmente implementadas en el Ayuntamiento de Sevilla.

Para realizar esta evaluación se utilizará la Guía CCN-STIC 808 Verificación del Cumplimiento de las Medidas en el ENS, así como cualquier otra guía de la serie 800 que resulte de aplicación.

Esta Guía proporciona un listado sistemático de comprobación para cada medida, y facilita el registro de evidencias del cumplimiento. La sistemática establecida en la Guía permite la cuantificación del grado de cumplimiento de las medidas del ENS, así como la identificación de las medidas no suficientemente cubiertas con las actuaciones ya implementadas en el Ayuntamiento de Sevilla.

Como resultado de esta fase se elaborará un Informe de Evaluación Inicial de Cumplimiento del ENS, que detallará tanto el grado de cumplimiento, como la relación de medidas de la Declaración de Aplicabilidad no suficientemente cubiertas en la actualidad.

También se incluirá la relación de oportunidades para la mejora de la seguridad del sistema de información identificadas durante la evaluación.

Toda la información recogida, categorizada y estructurada se añadirá a la herramienta PILAR y AMPARO.

4.2.5. Elaboración de la documentación resultante del Plan de Mejora de la Seguridad. Normativas y Procedimientos

En esta fase, se deberán poner en marcha las tareas para garantizar el cumplimiento. Para ello, los diferentes proyectos establecidos contarán con una planificación y asignación de responsables. El equipo del proyecto, como parte del soporte a estas tareas, realizará las siguientes actuaciones:

A. Elaboración del plan de adecuación al ENS

A partir del diferencial de cumplimiento con el ENS y otras oportunidades de mejora identificadas, se elaborará un plan con el detalle de las actuaciones, responsables, plazos de ejecución y recursos asignados para alcanzar el cumplimiento previsto.

Como resultado de esta fase, se formalizará el documento Plan de Adecuación al ENS del HISPALNET y las Entidades que la integran.

Para la elaboración de este documento se tendrá en cuenta la metodología y contenidos indicados en la Guía CCN-STIC 806 ENS Plan de Adecuación:

- Política de seguridad.
- Información que se maneja, con su valoración.
- Servicios que se prestan, con su valoración.
- Datos de carácter personal.

- Categoría del sistema.
- Análisis de riesgos.
- Declaración de aplicabilidad de las medidas del Anexo II del ENS y las requeridas por el tratamiento de datos de carácter personal, si los hubiera.
- Insuficiencias del sistema (gap analysis).
- Plan de mejora seguridad, incluyendo plazos estimados de ejecución.

B. Elaboración del marco normativo y procedimental de desarrollo del ENS

Para garantizar un adecuado cumplimiento y poder evidenciar la definición de las medidas de seguridad, se revisará toda la estructura del marco normativo existente, la Política de Seguridad y normativas de seguridad o procedimientos existentes. En base a esta revisión de documentos, se formalizará un nuevo marco normativo que concreten los requisitos técnicos a satisfacer en cada caso y los procedimientos operativos que deben implantarse como parte del cumplimiento del ENS.

Como objetivo de las tareas a realizar estará el desarrollo de esta documentación (la que sea necesaria para el caso concreto), con sus anexos o plantillas relacionadas, siguiendo los criterios de prioridad establecidos por la Guía de CCN-STIC 883 Implantación del ENS para Entidades Locales.

Finalmente, los entregables de esta actuación son:

- Política de Seguridad de la Información y Marco Normativo
- Informe de Valoración y Categorización del Sistema
- Informe de Revisión de Análisis de Riesgos
- Declaración de Aplicabilidad
- Informe de Evaluación Inicial de Cumplimiento del ENS
- Plan de Adecuación al ENS del Ayuntamiento de Sevilla
- Cuadro de Mandos de Implantación del ENS

4.3 Actuación 3: Actividades de formación y concienciación en Ciberseguridad

Mediante las actividades de formación y concienciación se consigue promover y reforzar la cultura de seguridad del Ayuntamiento de Sevilla a través del desarrollo e implementación de un Plan tanto de Concienciación y Sensibilización como de Formación, en el que se transformarán e interiorizarán comportamientos y hábitos en seguridad en el día a día de los empleados, que se ejecutará a partir de la finalización de la implantación de las diferentes herramientas.

El Adjudicatario deberá proporcionar, durante un mínimo de tres años desde la fecha de aceptación de los trabajos, un conjunto de plataformas tecnológicas que se suministrarán en modalidad de "Software como servicio" (SaaS), sin que Ayuntamiento de Sevilla tenga que asumir ningún tipo de

coste adicional al importe de la oferta.

La plataforma deberá cubrir un mínimo de 8000 usuarios concurrentes con independencia del tipo de acceso que se realice (web, dispositivo móvil ...).

Dentro del sistema de actividades de concienciación dirigido a los empleados y empleadas públicos: se ofertará el desarrollo de un mínimo de:

- Número de acciones de concienciación disponibles: 20 acciones de concienciación en ciberseguridad.

Dentro del sistema de actividades de formación dirigido a los empleados y empleadas públicos responsables de los Sistemas de Información se ofertará la realización de un mínimo de:

- Número de acciones de formación disponibles: 20 acciones de conceptos básicos de ciberseguridad

La plataforma deberá permitir el acceso de administración y de usuario mediante una interfaz web. Deberá soportar, al menos las últimas versiones de los siguientes navegadores:

- Internet Explorer
- Microsoft Edge
- Firefox
- Chrome
- Safari

Deberá tener capacidad de almacenamiento ilimitada para el desarrollo del material formativo por parte del Ayuntamiento de Sevilla durante un periodo de tres años.

La plataforma será 100% responsiva e incorporará las mejores prácticas de desarrollo seguro.

Dicha Plataforma permitirá:

A) Gestión de usuarios

La plataforma deberá contar con un módulo para la gestión de usuarios, con capacidad al menos para:

- Creación y configuración de usuarios de forma manual durante todo su ciclo de vida (creación, eliminación, activación, desactivación del usuario, reseteo de contraseña, incorporación de datos personales, asignación de grupos, etc.).
- Integración con LDAP y Directorio Activo.
- Importación masiva de usuarios desde un archivo externo (texto plano, CSV o Excel).
- Organización de usuarios mediante grupos, según sus características. Estos grupos deberán poder utilizarse posteriormente para la configuración de las acciones de formación y capacitación.
- Exportación de la relación de usuarios a fichero Excel o CSV.

B) Planificador de campañas

La plataforma deberá incluir un módulo de planificación que permita al administrador planificar y programar en el tiempo y mediante un asistente de uso sencillo e intuitivo, las actividades de capacitación (campañas).

La planificación se facilitará a través de una vista de calendario donde se presente para cada mes, las campañas programadas y el estado en el que se encuentran (finalizada, no iniciada, etc.).

La actividad definida para una determinada campaña podrá asignarse a uno o varios usuarios o grupos de usuarios, y durante un intervalo preestablecido a criterio del administrador.

El inicio de una campaña previamente programada se ejecutará de forma automática, siendo la propia plataforma la que se encargue, de forma autónoma, de enviar correos electrónicos de aviso a los usuarios con el contenido sobre la actividad que deben completar.

La vista de calendario permitirá el acceso a detalles estadísticos específicos de cada campaña en curso o finalizada, interaccionando para ello con el resto de módulos que se describen posteriormente.

C) Módulos interactivos

Los módulos interactivos son una forma de presentación de contenidos que combinan diversos métodos de interacción, contenido multimedia y GBL (Game-Based Learning). Esto

permite a los usuarios asimilar de una forma fluida y divertida los diferentes tópicos de capacitación.

La plataforma deberá incluir una extensa biblioteca de módulos interactivos que traten sobre los aspectos más significativos de la seguridad de la información (por ejemplo, temas como ingeniería social, malware, phishing, buenas prácticas en el uso de contraseñas, etc.). En particular, deberá contemplar los indicados en 4.3 Actuación 3: Actividades de formación y concienciación, cuyo contenido concreto se definirá conjuntamente con los técnicos encargados del Ayuntamiento.

Estos módulos deberán ser de tipo responsivo, permitiendo el acceso desde cualquier tipo de dispositivo. Además, cualquier módulo podrá ser tomado como plantilla y modificado, adaptado y personalizado por el administrador a través de una herramienta de edición sencilla e intuitiva que permita, al menos incrustar imágenes, vídeos, textos, preguntas interactivas, actividades de arrastrar y soltar, y actividades de unir mediante flechas.

D) Boletines de concienciación (Newsletters)

Los Boletines de concienciación o “Newsletters” son correos electrónicos diseñados para reforzar los contenidos de capacitación de una forma amena y mantener la atención de los usuarios en los diversos tópicos enseñados.

La plataforma incluirá una biblioteca de boletines pre configurados sobre temas de actualidad relacionados con seguridad de la información listos para su uso. Asimismo, el administrador dispondrá de una herramienta de edición que le permita crear nuevos boletines personalizados, bien tomando como plantilla alguno de la librería o bien desarrollando otros totalmente nuevos.

El editor, intuitivo y de fácil uso (debe ser similar a cualquier editor de texto de uso ofimático), permitirá incluir texto con diferentes características en cuanto a tipo, tamaño y características de la fuente y de los párrafos empleados, incrustación de imágenes, capacidad para incluir enlaces a URL’s, tablas, etc. de forma que el boletín desarrollado sea rico gráfica y visualmente. Además, deberá permitir la inclusión de una o varias preguntas de control que el usuario tendrá que responder, de forma que sirva como control del resultado de la acción formativa o de sensibilización. Estas respuestas se recogerán en el módulo de auditoría.

E) Simulador de ataques mediante correo electrónico (Phishing y Ransomware)

La plataforma incluirá una biblioteca preconfigurada de modelos de correos que simulen diferentes tipos de ataques, en particular correos de phishing o envío de ransomware.

El administrador dispondrá de una herramienta de edición que le permita crear nuevos correos personalizados de ambos tipos, ya sea tomando como plantilla alguno de la librería o bien desarrollando uno totalmente nuevo.

El editor, será intuitivo y de fácil uso (similar a cualquier editor de texto de uso ofimático), y permitirá definir el asunto del correo y el remitente, incluir texto con diferentes características en cuanto a tipo, tamaño y características de la fuente y de los párrafos utilizados, incluir imágenes, enlaces a URL's, tablas, etc., con objeto de poder generar correos lo más realistas posibles (similares a un correo malicioso real).

El envío de correos simulando phishing o ransomware se programará como una campaña más mediante el Planificador de Campañas. La plataforma deberá contar con un servidor de correo propio preparado para poder enviar dichos correos sin que por ello pueda ser incluida listas de spam u otros servicios que puedan afectar a su funcionamiento.

Además, y complementariamente, se dispondrá de un editor que permita configurar de forma sencilla la página web que será vinculada a los enlaces incluidos en el cuerpo del correo que simula el ataque, de forma que el comportamiento sea totalmente realista. Este editor permitirá incluir, además de texto e imágenes, formularios de registro en el que el usuario deba introducir sus credenciales, o botones de aceptación, de forma que se asemeje a todos los efectos a un ataque real. Esta página web se alojará en el propio servidor de la plataforma y se presentará al usuario en caso de que este acceda a alguno de los enlaces incluidos en el correo.

El editor deberá permitir previsualizar el correo o la web que se está desarrollando para poder realizar labores de depuración.

La actividad del usuario al recibir una campaña de phishing deberá quedar registrada en el módulo de auditoría con todo detalle (usuario, fecha de la campaña y datos de actividad como apertura del correo, acceso al enlace, e ingreso de datos en el formulario, como mínimo).

F) Herramienta de evaluación

La plataforma deberá incluir una herramienta para la creación, por parte del administrador, de exámenes tipo test. Dicha herramienta, permitirá la elaboración de cuestionarios compuestos por preguntas con asignación de una serie de respuestas preconfiguradas, siendo una de ellas válidas.

La corrección se realizará automáticamente a partir de las respuestas que fueron marcadas como válidas por el administrador durante la elaboración del test. Los resultados para cada usuario quedarán automáticamente recogidos en el módulo de auditoría.

Los exámenes se podrán programar, como una actividad más, a través de la herramienta de planificación.

G) Herramienta de auditoría

La plataforma deberá contar con una herramienta de auditoría y cumplimiento que permita:

- Registrar automáticamente las actividades correspondientes a las diferentes actividades; partiendo de un cuadro de mandos general como resumen ejecutivo, donde se recojan las campañas programadas (pasadas o futuras) según tipología (Módulo interactivo, exámenes, etc.). Se deberá poder acceder a un resumen general por cada tipología de campaña, y desde este, avanzar por cada una de ellas para profundizar en el detalle de cada campaña concreta (fecha de inicio y de finalización, contenido, usuarios incluidos, etc.), llegando incluso al nivel de un usuario concreto incluido en la campaña. Para un usuario específico se podrá acceder a su historial detallado de actividad (campañas recibidas por tipologías, acciones realizadas por cada campaña, fecha de realización, etc.).
- Registrar automáticamente las actividades de administración y del sistema como, por ejemplo; creación o modificación de usuarios o grupos, creación o modificación de campañas, etc.

Toda la información deberá presentarse de forma sencilla y gráfica mediante cuadros de mando. Los datos de los diferentes cuadros de mandos (general, por campañas, por usuarios) deberán poder exportarse hacia formatos de uso habitual, en particular a Excel o CSV, para su tratamiento fuera de la plataforma.

H) Soporte

El adjudicatario debe proporcionar soporte sobre el uso de la plataforma durante la duración del contrato, sin coste adicional para el Ayuntamiento de Sevilla. Este soporte consistirá en la resolución de dudas, consultas, actualizaciones de los módulos disponibles (plantillas) o desarrollo de otros nuevos (según su propia planificación), así como cualquier otra actividad relacionada con la explotación de la solución.

4.3.1 Actividades de concienciación

Como parte del Plan de Concienciación, el Adjudicatario llevará a cabo Las características de las siguientes actividades:

- Servicio de Consultoría para la definición, implementación y evaluación del Plan de Concienciación.
  - Coordinación del Proyecto para la definición y seguimiento del proyecto.
  - Evaluación del nivel de madurez de los participantes tanto al inicio como al final.

- Coordinación de acciones de refuerzo a usuarios vulnerables.
- Realización de una campaña de ataque dirigido genérico de suplantación con una página web genérica con registro de un dominio similar al objetivo. El objetivo de esta campaña es obtener la mayor captación de usuarios vulnerables.
- Organización de sesiones con profesor de concienciación para participantes de todos los niveles en las que se desarrollen los principios de la ciberseguridad y las mejores prácticas para prevenir ataques e incidentes de seguridad.
- Organización de talleres sobre distintas temáticas de ciberseguridad para un grupo hasta 30 participantes seleccionados. Estos talleres deberán tener una duración de 6 horas.
- Plataforma online de formación y concienciación con 2 cursos interactivos de concienciación en ciberseguridad y 20 cursos interactivos de conceptos básicos de ciberseguridad. Cada curso no deberá tener una duración superior a una hora y estará estructurado en módulos o píldoras de 5 a 15 min de duración.
- Realización de una campaña de ataque dirigido personalizado de suplantación con una página web personalizada con registro de un dominio similar al objetivo. Para ello se fabrican mensajes realistas que llamen la atención y confianza del grupo de usuarios. Este tipo de campañas aumentan las probabilidades de captación y complementaria toda la técnica utilizada en la campaña de ataque dirigido genérico.
- Realización de un reporte de riesgos integrando los resultados de las actividades desarrolladas de ataques dirigidos y de la plataforma de concienciación. Además, se deberá realizar un análisis de riesgos basándose en la inteligencia de fuentes abiertas (OSINT) para evaluar como de expuestos están los datos de los empleados y el nivel de privacidad y seguridad del Ayuntamiento de Sevilla.
- Organización de una sesión con profesor de concienciación para personas en puestos de decisión y con un gran acceso a información y datos en la Red Corporativa Hispalnet. Durante la sesión se mostrarán ejemplos prácticos de los contenidos para que los participantes puedan verlo en vivo y participar de manera activa.
- Desarrollo de un plan de comunicación con el envío de infografías mensuales a los participantes para reforzar los conceptos desarrollados en la plataforma de formación y concienciación. Las infografías deberán cubrir las siguientes temáticas:

    - Seguridad en el puesto de trabajo
    - Navegación segura
    - Dispositivos móviles
    - Seguridad en redes wifi
    - Teletrabajo
    - Malware
    - USB Maliciosos
    - Ingeniería social
    - Phishing
    - Redes sociales
    - Teletrabajo

- Geolocalización

Estas actividades estarán disponibles, al menos, durante tres años en la Plataforma.

4.3.2 Actividades de formación

Adicionalmente al suministro de la Plataforma y, en particular, como parte del Plan de Concienciación específico para el personal TIC, el Adjudicatario llevará a cabo las siguientes actividades:

- Plataforma online de formación especialista con 45 cursos avanzados de entre 60 y 80 minutos de duración por curso. Los cursos deberán cubrir como mínimo las siguientes temáticas:
  - Forense digital
  - Respuesta a incidentes
  - OWASP
  - Red Team
  - Pentesting
  - Exploits
- Los cursos se complementarán con un acceso por VPN a una red de laboratorios en el que los participantes podrán poner en práctica en un entorno simulado los conocimientos adquiridos con la formación especialista.
- Organización de talleres sobre distintas temáticas de ciberseguridad para un grupo hasta 30 participantes seleccionados. Estos talleres deberán tener una duración de 6 horas

Estas actividades estarán disponibles, al menos, durante tres años en la Plataforma.

5. CONDICIONES DE EJECUCIÓN DE LAS ACTUACIONES

Las actuaciones y suministros indicados en el punto 4 del presente documento deberán realizarse de forma paralela en cuanto a las tres líneas de actuación diferenciadas ya que no existen dependencias entre los trabajos de una línea de actuación con otra.

El Adjudicatario deberá presentar una propuesta de planificación en el plazo máximo de 3 días desde la formalización del contrato. Dicha propuesta deberá contemplar un hito parcial a la mitad de periodo total de planificación en el que se deberá comprobar la realización del 50% de los trabajos. Dicha propuesta deberá ser aprobada por Responsable del Contrato.

6. MÉTODO DE GESTIÓN Y DESCRIPCIÓN DE EQUIPO TÉCNICO

Se establecen las siguientes figuras y órganos de dirección del gobierno del proyecto:

- Comité de Dirección del Proyecto
- Comité de Seguimiento y Control
- Responsable del Contrato
- Jefe de Proyecto
- Equipo Técnico

Las funciones y responsabilidades de cada uno de ellos serán:

6.1 Comité de Dirección del Proyecto

Será el órgano superior de gobierno del proyecto desde un punto de vista estratégico y funcional, y el encargado de velar por la globalidad del mismo, siendo el responsable de la toma de las decisiones de nivel estratégico. Su composición y funcionamiento se determinarán al inicio del proyecto.

Las funciones del Comité de Dirección son las siguientes:

- El seguimiento estratégico y funcional del proyecto.
- Alinear el desarrollo del proyecto con los objetivos estratégicos del Ayuntamiento.
- Aprobar el documento que servirá de base para el control y seguimiento del proyecto.
- Aprobar los requisitos funcionales propuestos por el Comité de Seguimiento y Control
- Aprobar las propuestas de cambios normativos que se deban realizar para simplificar y racionalizar procedimientos para que se proceda a su tramitación reglamentaria.
- Evaluar periódicamente el grado de cumplimiento de los objetivos y sus posibles desviaciones e instar al Responsable del Proyecto a tomar medidas para atajar y corregir las posibles desviaciones.
- La coordinación de la difusión y transferencia de los resultados del proyecto.
- Designar a los miembros del Comité de Seguimiento y control.

A las reuniones del Comité de Dirección asistirá cuando se le requiera un representante habilitado de la empresa adjudicataria, con rango superior al Jefe del Proyecto, así como el Responsable del Contrato y el Jefe del Proyecto por parte de la empresa adjudicataria.

6.2 Comité de Seguimiento y Control

Será el órgano encargado de determinar el alcance funcional dentro del marco establecido en este

Pliego de Prescripciones Técnicas.

Las funciones del Comité del Comité de Seguimiento y Control serán las siguientes:

- Validar el documento que servirá de base para el control y seguimiento del proyecto e instar al Responsable del Proyecto a que lo eleve al Comité de Dirección para su aprobación.
- Validar los requisitos funcionales que definitivamente regirán el desarrollo de los trabajos proyecto e instar al Responsable del Proyecto a que los eleve al Comité de Dirección para su aprobación.
- Validar las propuestas de cambios normativos que se deban realizar para simplificar y racionalizar procedimientos proyecto e instar al Responsable del Proyecto a que lo eleve al Comité de Dirección para su aprobación.
- Revisar la situación del desarrollo del proyecto e proyecto e instar al Responsable del Proyecto a que informe al Comité de Dirección de las posibles desviaciones y de las propuestas de medidas para atajarlas y corregirlas.
- Aplicar las directrices establecidas por el Comité de Dirección en relación a los objetivos estratégicos del Ayuntamiento.

Su composición y funcionamiento la determinará el Comité de Dirección al inicio del proyecto. En cualquier caso siempre formarán parte del mismo, el Responsable del Contrato y el Jefe del Proyecto por parte de la empresa adjudicataria.

6.3 Responsable de la actuación

Será designado por el Ayuntamiento y deberá seguir las directrices funcionales marcadas por los diversos comités que existen o que se creen a este efecto, siendo sus funciones y responsabilidades, además de las previstas legalmente, las siguientes:

- Dirigir, supervisar y coordinar la realización y desarrollo de los trabajos.
- Aprobar el programa de realización de los trabajos.
- Velar por el nivel de calidad de los trabajos.
- Coordinar las entrevistas entre usuarios y técnicos involucrados en el proyecto.
- Decidir sobre la aceptación de las modificaciones técnicas propuestas por el Equipo de proyecto los responsables de cada una de las actuaciones a lo largo del desarrollo de los trabajos.
- Asegurar el seguimiento del programa de realización de los trabajos.
- Autorizar cualquier alteración de la metodología empleada, tanto en los productos finales, como en la realización de las fases, módulos, actividades y tareas.
- Aprobar los resultados parciales y totales de la realización del proyecto; a estos efectos deberá recibir y analizar los resultados y documentación elaborados a la finalización de cada etapa, pudiendo introducir las modificaciones o correcciones oportunas antes del comienzo de las siguientes, requiriéndose su aprobación final.
- La realización de replanificaciones de los trabajos y de posibles acuerdos de nivel del

servicio.

- Proponer al Órgano de Contratación la adopción de medidas respecto a la suspensión y/o terminación del proyecto. .

6.4 Jefe de Proyecto

Será aportado por la empresa adjudicataria, siendo su responsabilidad que los trabajos se ejecuten conforme a lo estipulado en el contrato y con las directrices del Responsable de la Actuación. Además tendrá como objetivos específicos los siguientes:

- Organizar la ejecución del proyecto de acuerdo con el programa de realización de los trabajos y poner en práctica las instrucciones del Responsable de la Actuación.
- Ostentar la representación del equipo técnico contratado en sus relaciones con el Ayuntamiento de Sevilla en lo referente a la ejecución de los trabajos.
- Proponer al Responsable del Contrato las modificaciones que estime necesarias, surgidas durante el desarrollo de los trabajos.
- Asegurar el nivel de calidad de los trabajos.
- Presentar al Responsable del Contrato, para su aprobación, los resultados parciales y totales de la realización del proyecto.
- Comunicar al Responsable del Contrato los cambios en la composición del equipo del proyecto con una antelación suficiente y el plan de formación y adaptación correspondiente al cambio propuesto.

6.5 Equipo Técnico de cada una de las actuaciones

El equipo de trabajo estará formado íntegramente por personal de la empresa adjudicataria, que será responsable de la realización de todos los procesos y trabajos detallados en el presente pliego. El personal técnico que realice las tareas correspondientes a los trabajos del proyecto deberá encuadrarse en alguno de los siguientes perfiles y cumplir con los requisitos especificados:

- **Analistas funcionales:** Realizarán la toma de requisitos, elaborarán la planificación y guiarán el desarrollo e implantación de las soluciones. Serán los responsables de asegurar que se cumplen los objetivos de los desarrollos en cuanto a funcionalidad y calidad. Se demanda un mínimo de 4 profesionales con al menos:
  - Titulación universitaria superior en el ámbito de las TICs
  - 5 años de experiencia como analistas en sistemas de gestión de servicios con un alcance similar al del presente contrato

- **Consultores:** realizarán labores puntuales de asesoramiento en aspectos concretos dentro de su área de especialización No se demanda un mínimo de profesionales con este perfil, pero en caso de que la empresa adjudicataria, en algún momento del proyecto, incluyese en su equipo a algún profesional al que encuadrase en este perfil, éste deberá al menos poseer:
  - Titulación universitaria superior en el ámbito de las TICs
  - 4 años de experiencia en trabajos de consultoría relacionados con su área de

especialización.

- **Técnicos de gestión del Cambio:** Serán los responsables de elaborar los planes de capacitación y de divulgación, el material de apoyo utilizado en los mismos, así como de llevarlos a cabo y ejecutarlos en la práctica.

  Se demanda un mínimo de 1 profesional con al menos:

  – Titulación universitaria superior relacionada con los procesos de gestión del cambio.
  – Experiencia de al menos 2 años en proyectos de gestión del cambio con un alcance similar al del presente contrato

6.6 Documentos de Gestión del Proyecto

Se establecen tres documentos estándar de información para el Comité Director: la Agenda de Reunión, el Informe de Progreso y el Acta de Reunión, siendo la empresa adjudicataria encargada del desarrollo del proyecto quien los elaborará, los presentará en cada reunión y posteriormente los enviará, todo ello de acuerdo con las especificaciones establecidas.

Los documentos comentados se definen a continuación:

- Agenda de Reunión.- Es el documento en el que se recogen los principales asuntos a tratar y el orden del día de la reunión, indicando, en la medida de lo posible, y con el fin de poder ejercer cierto control sobre la duración de la reunión, el tiempo estimado de duración en el tratamiento de cada uno de los puntos del orden del día.

- Informe de Progreso.- Es el documento en el que se recoge el estado actual del proyecto a la fecha de celebración del correspondiente Comité. Es el resultado del análisis de los datos que proporciona el equipo de trabajo del proyecto y constituye la principal fuente de información sobre el trabajo realizado y la situación del mismo. Describe las tareas acometidas y por acometer, su grado de consecución, así como sus objetivos. Registra, asimismo, las incidencias acaecidas e identifica los riesgos y oportunidades identificados en relación con el proyecto.

- Acta de Reunión.- Es el documento en el que se recoge la información principal relacionada con el desarrollo de las distintas reuniones de seguimiento (Comité Director, Técnico o Grupo de Trabajo). Los apartados que se deben recoger en el acta de la reunión son la relación de asistentes y ausentes de la reunión, los principales aspectos tratados y las resoluciones adoptadas durante la reunión. Su lectura y, si procede, su aprobación y firma es un requisito indispensable para el adecuado seguimiento del proyecto que se deberá formalizar en la siguiente reunión de seguimiento (Comité Director, Técnico o Grupo de Trabajo).

7. SISTEMA DE SEGUIMIENTO Y CONTROL

Se realizará un seguimiento continuo de la evolución del servicio por parte del Responsable del Contrato. La Dirección General de Modernización podrá determinar los procedimientos y herramientas a utilizar para poder llevar a cabo la planificación, seguimiento y control del servicio, eligiendo entre los que el adjudicatario haya incluido en su oferta o aquellos que se hayan determinado como estándares en el Ayuntamiento de Sevilla.

Se realizarán reuniones de seguimiento y revisiones técnicas, con una periodicidad acordada por ambas partes, del Jefe de Proyecto/Interlocutor por parte del adjudicatario y del Responsable del Contrato o persona en quien delegue, al objeto de revisar el grado de cumplimiento de los objetivos, las reasignaciones y variaciones de efectivos de personal dedicado al servicio, las especificaciones funcionales de cada uno de los objetivos y la validación de las programaciones de actividades realizadas.

Tras las revisiones técnicas, de las que se levantará acta, el Responsable del Contrato podrá rechazar en todo o en parte los trabajos realizados, en la medida que no respondan a lo especificado en las reuniones de planificación o no superasen los controles de calidad acordados.

El Comité de Dirección se reunirá de forma ordinaria con al menos una periodicidad trimestral para ser informados por el Responsable del Contrato y por el Jefe del Proyecto de la evolución de los trabajos, y de forma extraordinaria -a propuesta de cualquiera de las dos partes- cuando las circunstancias y el desarrollo del proyecto así lo aconsejen.

El seguimiento y control tendrá como objetivo verificar sistemáticamente la calidad de las tareas en curso, medir periódicamente el avance y compararlo con la planificación inicial, y establecer las acciones correctoras ante posibles desviaciones o incidencias surgidas.

Existirá una planificación detallada de la propuesta de puesta en operación de los Servicios, proyectos y actuaciones al inicio de los trabajos.

Dicha planificación se efectuará mediante un Diagrama de Gantt, en el que se especificarán plazos e hitos de entrega aproximados para cada una de las actuaciones a acometer. Asimismo, dicha planificación será actualizada a través de los distintos hitos de decisión, de frecuencia preestablecida o promovidos por cambios no planificados, revisión de resultados o tomas de decisiones no contempladas como parte de la línea base inicialmente acordada entre ambas partes.

8. MEDIDAS DE INFORMACIÓN Y PUBLICIDAD

El Ayuntamiento de Sevilla como entidad beneficiaria de las ayudas cumplirá con las obligaciones de comunicación derivadas de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia. En concreto es de obligado cumplimiento:

Cualquier medida de información, comunicación y visibilidad (banners en webs o aplicaciones informáticas, carteles informativos, placas, publicaciones impresas y electrónicas, material audiovisual, anuncios e inserciones en prensa, certificados, etc.), de las actuaciones derivadas de este pliego deberá incorporar los siguientes logos teniendo en cuenta las normas gráficas y los colores normalizados establecidos en el anexo I del Reglamento de Ejecución 821/2014 de la Comisión de 28 de julio de 2014

- El emblema de la Unión Europea
- Junto con el emblema de la Unión, se incluirá el texto «Financiado por la Unión Europea - NextGenerationEU».
- El logo oficial del Plan de Recuperación, Transformación y Resiliencia del Reino de España, y una referencia a la gestión por el Ministerio de Política Territorial

Igualmente, el Ayuntamiento de Sevilla se asegurará que todos los documentos que sustenten la contratación de los bienes y servicios a prestar o encargo relacionado con la ejecución de la actuación, incluida la subcontratación, se haga constar « 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, así como la referencia al Componente 11, Inversión 3, del PRTR, gestionado por el Ministerio de Política Territorial.

9. DOCUMENTACIÓN Y FORMACIÓN

9.1 Documentación al inicio de la instalación

La propuesta de planificación presentada por el adjudicatario deberá ser aprobada por Responsable del Contrato en el plazo máximo de 3 días desde la formalización del contrato.

9.2 Documentación durante la ejecución

El adjudicatario será responsable de la entrega de la documentación de seguimiento de la instalación que incluirá una entrega quincenal a presentar ante el Comité de Seguimiento, indicando:

- Fecha de petición y entrega del material
- Estado de la entrega de material final de la instalación en porcentaje
- Fecha de inicio de la ejecución y fecha fin prevista para cada uno de los sistemas contemplados en el pliego.
- Porcentaje de avance de la ejecución
- Listado de incidencias y priorización de acciones a realizar para mejorar el correcto funcionamiento de la ejecución del proyecto.

9.3 Documentación final de la instalación

El adjudicatario será responsable de la entrega de la documentación final de la instalación como requisito indispensable para su aceptación. La documentación incluirá como mínimo:

- Memoria técnica de la instalación, en formato Word, con la descripción de cada uno de los subsistemas contemplados en el pliego y las medidas de contingencia contempladas.
- Esquemas generales del sistema en formato PDF, diferenciados por cada uno de los subsistemas contemplados.
- Inventario del equipamiento instalado y especificaciones técnicas para cada uno de los elementos del sistema contemplados en el pliego.
- Documento detalle de las configuraciones y parametrizaciones realizadas para cada uno de los sistemas.
- Documentación de plan de garantía asociado.
- Proyecto final “as built” de las instalaciones ejecutadas, indicando los puntos de conexionado con las instalaciones existentes, incluso integrando en la documentación existente la ejecución realizada.

Como parte de los trabajos objeto del contrato, el adjudicatario proporcionará al STI la documentación técnica en castellano de todos los sistemas y equipos instalados, con una información detallada y exhaustiva tanto de la funcionalidad de los diversos elementos del sistema como de las configuraciones específicas de los mismos, además de la operación y el mantenimiento del sistema.

Toda esta documentación será reportada en formato electrónico al STI a lo largo de la duración del contrato.

9.4 Formación en las herramientas instaladas

Para la correcta explotación de las herramientas y sistemas instalados, el Adjudicatario deberá desarrollar, planificar e impartir una formación de los distintos subsistemas de manera que el personal, que HISPALNET designe para ello hasta un máximo de veinte personas, sea capaz de operar, mantener, configurar y si fuese necesario reinstalar cualquier subsistema implicado.

Cada acción formativa se planificará en dos turnos diferenciados para permitir la asistencia de los técnicos sin dejar sin servicios sus dependencias.

Las acciones formativas podrán ser realizadas en formato online.

El adjudicatario presentará 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. Se tendrán en cuenta los siguientes perfiles:

- Operación para el personal usuario del sistema en cuestión. Los cursos 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 para formación del personal técnico, orientados a obtener el detalle técnico, instalación, mantenimiento, etc. de la infraestructura implicada. De igual forma incluirá perfiles y conocimientos requeridos.

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

10. NORMATIVA APLICABLE

A continuación, se recoge una relación no exhaustiva de normas y regulaciones que tienen relación con el objeto de la contratación:

- 2022: RDL 7/2022 Seguridad 5G - Plan Nacional de Ciberseguridad
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Guía Nacional de notificación y gestión de ciberincidentes", publicada por el Ministerio del Interior.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (Reglamento general de protección de datos).
- Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD).
- Norma UNE-EN ISO/IEC 27001:2017 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (y subsiguientes de la serie ISO/IEC 27000 relativas a los sistemas de gestión de seguridad de la información. Information Technology Infrastructure Library (ITIL)
- 2016: ENS/ITS Conformidad con ENS - Informe ENS - RGPD - Directiva NIS · eGov Action Plan
- 2017: ESN 2017 (Estrategia de Seguridad Nacional) - EIF v2 - Declaración Ministerial de Tallin
- 2018: ENS-ITS (Actualización en materia de Auditorías y Notificaciones de incidentes - RDL 12/2018 NIS - LOPDGDD (antigua LOPD 15/1999)
- 2019: Guía Nacional de Notificación y Gestión de ciberincidentes - Estrategia Nacional de Ciberseguridad 2019 - Cybersecurity Act (EU)
- 2021: RD 43/2021 que desarrolla el RDI-I 12/2018 (NIS) - Plan de Digitalización de las AAPP 2021-2025 - Plan de Recuperación, Transformación y Resiliencia - RD 203/2021 (Reglamento leyes 39 y 40) - Reglamento Centro Europeo de Competencias en Ciberseguridad - NTI SICRES 4 - Carta de derechos digitales - ACM Plan de choque de ciberseguridad

11. PROPIEDAD INTELECTUAL Y CONFIDENCIALIDAD

11.1 Propiedad intelectual

Los módulos de capacitación y formación que hayan sido desarrollados sobre la plataforma íntegramente por parte del personal del Ayuntamiento de Sevilla (nuevos módulos interactivos, correos de phishing o ransomware, etc.), serán propiedad exclusiva de Ayuntamiento de Sevilla. Por otra parte, los módulos que hayan sido desarrollados partiendo de la biblioteca de plantillas disponibles en la plataforma, deberán ser eliminados por el adjudicatario a la finalización del contrato.

El software aportado por el adjudicatario, será de su propiedad; el Ayuntamiento de Sevilla sólo dispondrá del derecho de uso de la plataforma sin límite horario ni de capacidad de almacenamiento en cuanto al contenido propio desarrollado, durante el período de duración del contrato.

11.2 Confidencialidad de la Información

El adjudicatario del servicio objeto de concurso estará obligado a:

- Respetar el buen nombre y prestigio del Ayuntamiento de Sevilla
- Mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este pliego, ni tampoco ceder a otros ni siquiera a efectos de conservación.
- Cumplir lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal.

En todo caso, el adjudicatario será el responsable de cuantos daños y perjuicios se deriven del incumplimiento de esta obligación.

El adjudicatario tendrá acceso a datos de carácter personal, en concreto, nombre, apellidos de los usuarios, así como las calificaciones obtenidas en los módulos evaluables. Por este motivo ostentará, a todos los efectos, la figura de Encargado de Tratamiento, debiendo firmar junto con el resto de documentación del contrato, las cláusulas correspondientes de confidencialidad y cumplimiento de las obligaciones en materia de protección de datos de carácter personal.

EL JEFE DE NEGOCIADO
DE REDES Y COMUNICACIONES