

Expediente nº **2026-038772**

Área **Cultura y Gobernanza. Dirección de Modernización**

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

Objeto: **Consultoría para obtener la Certificación del Esquema Nacional de Seguridad (ENS)**

ELABORADO POR:

Por el Ayuntamiento de Bilbao:

Área de Cultura y Gobernanza: Dirección Modernización y Subdirección de Servicios Generales de Alcaldía

Por BILBAOTIK S.A.:

Dirección Técnica: **Dirección General, Subdirección de Transformación Digital, Subdirección de Smart Data y Servicios Corporativos y Dirección de Infraestructuras y Ciberseguridad.**

Índice

1. INTRODUCCIÓN	4
2. OBJETO DEL CONTRATO	6
3. PARTE 1: CERTIFICACIÓN EN ENS DEL AYUNTAMIENTO DE BILBAO.....	7
3.1. ALCANCE DEL CONTRATO.....	7
3.1.1. ADECUACIÓN CON EL ESQUEMA NACIONAL DE SEGURIDAD	7
3.1.1.1. <i>Plan de Adecuación.</i>	7
3.1.1.2. <i>Implantación de la Seguridad.</i>	8
3.1.1.3. <i>Declaración/ Certificación de Conformidad</i>	9
3.1.1.4. <i>Informar sobre el estado de Seguridad. Métricas e Indicadores.</i>	9
3.1.1.5. <i>Vigilancia y Mejora Continua.</i>	9
3.1.2. SERVICIOS ORIENTADOS AL CUMPLIMIENTO DEL NIS2	10
3.1.3. DESPLIEGUE DE HERRAMIENTAS ORIENTADAS A MEJORAR EL NIVEL DE PROTECCIÓN Y CUMPLIMIENTO NORMATIVO.....	10
3.1.3.1. <i>Identificación de necesidades de seguridad</i>	10
3.1.3.2. <i>Plataforma de formación al personal.</i>	10
3.1.4. AUDITORÍA INTERNA	12
3.1.5. ACOMPAÑAMIENTO EN LA AUDITORÍA EXTERNA DE CERTIFICACIÓN	13
3.2. ENTREGABLES	13
3.3. EQUIPO HUMANO: DIRECCIÓN Y EQUIPO TÉCNICO DEL TRABAJO	14
3.4. PLANIFICACIÓN Y GESTIÓN DEL PROYECTO	16
3.4.1. COMITÉ PARA COORDINACIÓN/ DIRECCIÓN DEL CONTRATO/ PROYECTO	16
3.4.2. IDENTIFICACIÓN Y GESTIÓN DE ACCIONES CORRECTORAS FRENTE A RIESGOS IDENTIFICADOS.....	16
3.4.3. PLANIFICACIÓN.....	16
3.4.4. CALIDAD, SEGUIMIENTO Y CONTROL DE LOS TRABAJOS.....	19
3.4.5. DOCUMENTACIÓN A ENTREGAR	21
3.5. CONTEXTO DEL ENTORNO TECNOLÓGICO E INFRAESTRUCTURA TECNOLÓGICA MUNICIPAL.....	21
3.7. PROTECCIÓN DE DATOS	24
3.8 SEGURIDAD DE LA INFORMACIÓN	24
4. PARTE 2: CERTIFICACIÓN EN ENS DE LAS ENTIDADES MUNICIPALES ADHERIDAS.....	24
4.1. ALCANCE DEL CONTRATO.....	24
4.1.1. ADECUACIÓN CON EL ESQUEMA NACIONAL DE SEGURIDAD	25

4.1.1.1. Plan de Adecuación	25
4.1.1.2. Implantación de la Seguridad.....	26
4.1.1.3. Declaración/ Certificación de Conformidad	27
4.1.1.4. Informar sobre el estado de Seguridad. Métricas e Indicadores.....	27
4.1.1.5. Vigilancia y Mejora Continua.	27
4.1.2. SERVICIOS ORIENTADOS AL CUMPLIMIENTO DEL NIS2	28
4.1.3. DESPLIEGUE DE HERRAMIENTAS ORIENTADAS A MEJORAR EL NIVEL DE PROTECCIÓN Y CUMPLIMIENTO NORMATIVO.....	28
4.1.3.1. Identificación de necesidades de seguridad	28
4.1.3.2. Plataforma de formación al personal.....	28
4.1.4. AUDITORÍA INTERNA	30
4.1.5. ACOMPAÑAMIENTO EN LA AUDITORÍA EXTERNA DE CERTIFICACIÓN	31
4.2. ENTREGABLES	31
4.3. EQUIPO HUMANO: DIRECCIÓN Y EQUIPO TÉCNICO DEL TRABAJO	32
4.4. PLANIFICACIÓN Y GESTIÓN DEL PROYECTO	34
4.4.1. COMITÉ PARA COORDINACIÓN/ DIRECCIÓN DEL CONTRATO/ PROYECTO	34
4.4.2. IDENTIFICACIÓN Y GESTIÓN DE ACCIONES CORRECTORAS FRENTE A RIESGOS IDENTIFICADOS.....	34
4.4.3. PLANIFICACIÓN.....	35
4.4.4. CALIDAD, SEGUIMIENTO Y CONTROL DE LOS TRABAJOS.....	38
4.4.5. DOCUMENTACIÓN A ENTREGAR	39
4.5. CONTEXTO DEL ENTORNO TECNOLÓGICO E INFRAESTRUCTURA TECNOLÓGICA MUNICIPAL.....	39
4.6. PRESUPUESTO.....	40
4.7. PROTECCIÓN DE DATOS	42
4.8. SEGURIDAD DE LA INFORMACIÓN.....	43

1. INTRODUCCIÓN

El Ayuntamiento de Bilbao dispone de numerosas actuaciones implantadas, asociadas a la Ciberseguridad para garantizar la **Seguridad Digital**, la **Resiliencia Digital**, la **Continuidad de la prestación de los Servicios Públicos** y la **Privacidad de los Datos de la Ciudadanía**. Nuestra misión, es garantizar que la transformación digital sea una transformación segura.

Por otro lado, el Ayuntamiento de Bilbao dispone de una **Política de Seguridad Municipal**, publicada en nuestra página web www.bilbao.eus, así como una **Estructura de Seguridad** del Ayuntamiento de Bilbao, una **identificación de la normativa en Seguridad** que nos aplica y una **normativa** que desarrolla la Política de Seguridad Municipal.

En el documento que recoge la normativa de Seguridad de la Información que aplica al Ayuntamiento de Bilbao: “**Listado normativo de aplicación en seguridad de la información**”, se recogen dos normativas en las que pondremos foco en este proceso de contratación:

- **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.**
- **Directiva (UE) 2022/2555 del Parlamento Europeo y Del Consejo de 14 de diciembre de 2022 (conocida popularmente como NIS2)** relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

El Esquema Nacional de Seguridad es de Obligado cumplimiento para todas las Administraciones Públicas: estatal, autonómica y local, según se establece en el artículo 2, el ámbito subjetivo de aplicación de ENS, en concreto, determina que es de aplicación a todo el sector público.

El Esquema Nacional de Seguridad (ENS) regulado por el Real Decreto 311/2022 de 3 de mayo, según establece en su artículo 1: “Objeto”:

1.- Este real decreto tiene por objeto regular el Esquema Nacional de Seguridad (en adelante ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público.

2.- El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

3.- Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

El Real Decreto 311/2022 de 3 de mayo en su Capítulo II: “Principios Básicos”, establece:

- Artículo 5: “Principios básicos del ENS”: El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:
 - a) Seguridad como proceso integral.
 - b) Gestión de la seguridad basada en riesgos.
 - c) Prevención, detección, respuesta y conservación.
 - d) Existencia de líneas de defensa.
 - e) Vigilancia continua.
 - f) Reevaluación periódica
 - g) Diferenciación de responsabilidades

Consiguientemente, el ENS tiene como objetivos:

- Crear las condiciones necesarias de seguridad 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 el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Promover la gestión continuada de la seguridad.
- Promover la prevención, detección y corrección para una mejor resiliencia en el escenario de ciberamenazas y ciberatacantes.
- Promover un tratamiento homogéneo de la seguridad, que facilite la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades. Esto supone proporcionar los elementos comunes que han de guiar la actuación de las entidades del Sector Público y de sus proveedores tecnológicos en materia de seguridad de las tecnologías de información.

La finalidad de la implantación del ENS en el Ayuntamiento de Bilbao y sus organismos autónomos dependientes 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 con el objeto de permitir a la ciudadanía y las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Por lo tanto, para cumplir por parte del Ayuntamiento de Bilbao y entidades municipales adheridas al presente contrato, con los requisitos del Esquema Nacional de Seguridad se hace necesario contratar un servicio de consultoría que permita cumplir con los siguientes objetivos:

- 1.- Cumplir la legislación de seguridad.
- 2.- Garantizar la calidad y protección de la información.
- 3.- Garantizar la prestación continuada de los servicios.
- 4.- Desarrollar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que permita la gestión de la seguridad de la información de nuestra organización, asegurando la confidencialidad, integridad y disponibilidad de los datos.
- 5.- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- 6.- Todo ello mediante la definición de las actuaciones pertinentes y medidas correctivas necesarias.

La Certificación en el Esquema Nacional de Seguridad se va a realizar faseada en 2 fases:

- **Fase 1:** La fase 1 se ejecutará mediante la presente licitación cuyo alcance es certificar los sistemas tecnológicos de información y soluciones tecnológicas que están alojados en la infraestructura municipal de BILBAOTIK.
- **Fase 2:** la fase 2, se acometerá a través de otra/s licitación/es/ y procederá a certificar los sistemas tecnológicos de información, soluciones tecnológicas e infraestructuras externas que están alojados fuera de la infraestructura municipal.

2. OBJETO DEL CONTRATO

El objeto del contrato es la prestación de servicio de **consultoría** para obtener la **Certificación de conformidad con el Esquema Nacional de Seguridad (en adelante, ENS) de los sistemas tecnológicos de información y soluciones tecnológicas alojados en la infraestructura municipal de BILBAOTIK S.A. por parte del Ayuntamiento de Bilbao y Entidades Municipales Adheridas al presente contrato.**

Las Entidades Municipales Adheridas al presente contrato son las siguientes:

- Bilbao Musika, O.A.L.
- Bilbao Zerbitzuak – Servicios, EPEL
- Centro Azkuna de Sociedad y Cultura Contemporánea S.A.
- Funicular de Artxanda, S.A.
- C.A.C. Teatro Arriaga, S.A.

El objetivo final del Ayuntamiento de Bilbao y entidades municipales adheridas al presente contrato es sustentar la confianza que merece el sistema en materia de seguridad, es decir, garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

3. PARTE 1: CERTIFICACIÓN EN ENS DEL AYUNTAMIENTO DE BILBAO

3.1. ALCANCE DEL CONTRATO

3.1.1. ADECUACIÓN CON EL ESQUEMA NACIONAL DE SEGURIDAD

3.1.1.1. Plan de Adecuación.

La Certificación y Conformidad con el ENS conlleva la elaboración previa de un **Plan de Adecuación** que incluya como mínimo, las **cuatro fases previas siguientes**:

- Revisión de la **Política de Seguridad**
- Determinación de la **Categoría de los sistemas**
- **Análisis de Riesgos**
- **Declaración de Aplicabilidad/Perfil de Cumplimiento.**

El Plan de Adecuación dispondrá como mínimo, de la siguiente información: el alcance de los sistemas que se van a someter al proceso de certificación en el ENS, la categoría los mismos, qué medidas del Anexo II del Esquema Nacional de Seguridad se van a implementar (Declaración de Aplicabilidad), qué riesgos se asumen, la Política de Seguridad del Ayuntamiento de Bilbao...

Para abordar de forma eficiente el Plan de Adecuación, es necesario realizar como mínimo los siguientes pasos para cada una de las fases:

FASE 0: Planificación: Identificar el alcance del sistema. Para ello se evaluarán las diferentes alternativas con el objetivo de buscar un sistema factible de certificar.

FASE 1: Revisión de la Política de Seguridad

- Revisando y aprobando los cambios necesarios en la política de seguridad del ayuntamiento
- Definición de roles y asignación de personas
- Modelo de organización de la seguridad
- Revisar la Política de Seguridad y el modelo de gobernanza de la seguridad: Comité de seguridad, Comité de Crisis, Cyberzaintza y analizar la necesidad de otros órganos de coordinación/alineamiento de seguridad de la información en el ámbito municipal.

FASE 2: Determinación de la categoría de los sistemas,

- Inventario de la Información y los Servicios, teniendo en cuenta las implicaciones en materia de protección de Datos.
- Valorar la información y los servicios de cada una de sus dimensiones (disponibilidad, autenticidad, confidencialidad, integridad y trazabilidad) según “niveles de importancia”: Bajo, Medio y Alto.
- Determinar la categoría de los sistemas

FASE 3: Análisis de Riesgos: Se deberá realizar un análisis previo y diagnóstico inicial de cumplimiento y aplicación del ENS, que incluya además la revisión de inventario de activos, comprobación de su valoración y la definición de responsabilidades. Se deberá realizar un análisis y tratamiento de los riesgos de seguridad a los que está expuesto el Ayuntamiento de Bilbao, que incluya la valoración de las medidas de seguridad existentes, así como determinar los controles de seguridad necesarios para dotarles de una protección eficaz.

- Identificación de activos y sus dependencias
- Valoración de amenazas y salvaguardas
- Analizar impacto y riesgo
- Utilización de la Herramienta de referencia municipal

FASE 4: Declaración de Aplicabilidad/Perfil de Cumplimiento: Validar la Declaración de Aplicabilidad Definitiva o evaluar la posibilidad de adherirse a un Perfil de Cumplimiento Específico.

3.1.1.2. Implantación de la Seguridad.

Una vez realizado el Plan de Adecuación, se pasa a la fase de implantación de la Seguridad. Esta fase consta de los siguientes pasos:

- Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades, que sirva de base para poner en marcha las acciones necesarias para asegurar el cumplimiento normativo. Las recomendaciones y la hoja de ruta deberán incluir todo tipo de acciones para el total cumplimiento normativo y adecuación al ENS, cuantificarlas e incluir una propuesta de calendario para las mismas, incluyendo todos los medios técnicos, materiales, funcionales y de cualquier tipo incluyendo estimación económica y temporal.
- Revisar el Marco Normativo, la Política de Seguridad, la Normativa de Seguridad que desarrolla la Política de Seguridad y la Implantación de la seguridad.
- Elaborar Procedimientos relacionados con los controles de ENS ajustados a la categoría del sistema.
- Crear instrucciones técnicas.

- Proponer, consensuar e implantar un sistema para recoger las acciones realizadas en materia de ENS.
- Aprobar el Sistema de Gestión de la Seguridad de la Información y revisión continua.

3.1.1.3. Declaración/ Certificación de Conformidad

La determinación de la conformidad de los sistemas de información del ámbito de aplicación de ENS, se determinará según dos procedimientos distintos según se trate de categoría Media, Alta o Básica:

- La conformidad de los sistemas de información del ámbito de aplicación del ENS en las categorías MEDIA o ALTA se realizará mediante una auditoría formal que verifique los requerimientos contemplados en el ENS, al menos cada dos años, o con carácter extraordinario si se producen modificaciones significativas.
- La conformidad de los sistemas de información en la categoría BÁSICA requiere de una autoevaluación que verifique su cumplimiento al menos cada dos años o, con carácter extraordinario si se producen modificaciones significativas. Este requisito para la conformidad no impide que un sistema de categoría BÁSICA se someta a una auditoría formal.

3.1.1.4. Informar sobre el estado de Seguridad. Métricas e Indicadores

Los organismos a los que se aplica el ENS están obligados a cumplimentar e informar sobre el Estado de Seguridad.

Para cumplir con este mandato, el CCN ha desarrollado el proyecto INES (Informe Nacional del Estado de Seguridad).

Informar a la Agencia Vasca de Ciberseguridad Cyberzaintza y a la Autoridad Vasca de protección de Datos, cuando proceda.

3.1.1.5. Vigilancia y Mejora Continua.

La gestión de la seguridad de la información es un proceso sujeto a cambios constantes que pueden proceder de cambios en la organización, amenazas, tecnologías y/o legislación y por ello es necesaria una mejora continua de nuestros sistemas.

Esta actualización continua conllevará entre otras acciones:

- Revisión de la Política de Seguridad de la Información
- Revisión de la Normativa de Seguridad que desarrolla la Política de Seguridad
- Revisión de la información y los servicios, y su categorización
- Actualización del análisis y gestión de riesgos, al menos anualmente
- Revisión de la Declaración de Aplicabilidad o del Perfil de Cumplimiento
- Realización de auditorías internas

- Revisión del Plan de Mejora
- Revisión de las medidas de seguridad
- Revisión y actualización de procedimientos
- Revisión de las métricas
- Revisión del Estado de Seguridad (INÉS), Agencia Vasca de Ciberseguridad (Cyberzaintza), Autoridad Vasca de Protección de Datos...
- Revisión por la Dirección

3.1.2. SERVICIOS ORIENTADOS AL CUMPLIMIENTO DEL NIS2

Se realizará un plan de convergencia para el cumplimiento de lo dispuesto en NIS2.

Los servicios de análisis de riesgos deberán de acompañarse de ejercicios de hacking ético que permitan comprobar el nivel real de seguridad a nivel de infraestructura y aplicaciones corporativas.

Respecto a la gestión de incidentes de seguridad, se establecerá procedimientos de gestión de violaciones de seguridad de los datos.

3.1.3. DESPLIEGUE DE HERRAMIENTAS ORIENTADAS A MEJORAR EL NIVEL DE PROTECCIÓN Y CUMPLIMIENTO NORMATIVO

3.1.3.1. Identificación de necesidades de seguridad

Se identificarán necesidades para mejorar el nivel de seguridad y cumplimiento normativo, con la colaboración de BilbaoTIK, la empresa tecnológica del Ayuntamiento de Bilbao.

Se verificará el cumplimiento de las guías CCN-STIC por parte de BilbaoTIK en la realización del bastionado de sistemas.

3.1.3.2. Plataforma de formación al personal

Se realizará la **formación, concienciación y sensibilización** en materia de seguridad del personal del Ayuntamiento de Bilbao como una medida fundamental de reducción del riesgo de seguridad.

Para que las acciones de concienciación sean realmente efectivas es necesario disponer de una plataforma automatizada que permita:

- Evaluar el riesgo de seguridad asociado a las personas.
- Disponer de métricas e indicadores que permitan medir tanto el nivel de riesgo como la eficacia de las acciones de concienciación y el nivel de alerta de las personas.
- Aumentar o mantener el estado de alerta en ciberseguridad de las personas.
- Elaborar planes de acción y realizar actividades de formación dirigidas a colectivos específicos en diferentes formatos.

- Lanzar campañas de ataque dirigido a colectivos específicos de las principales amenazas en ciberseguridad orientadas a las personas.

Se pondrá en marcha una plataforma software que permita evaluar el riesgo de ciberseguridad asociado a las personas y concienciar en diferentes áreas de la ciberseguridad y de las amenazas de mayor riesgo: ingeniería social, phishing, manejo de cuentas y credenciales, etc.

La plataforma debe permitir la adaptación automática de los contenidos en función tanto del desarrollo de las acciones en el tiempo y de los indicadores de alerta, como de la evolución de las amenazas.

El **idioma nativo** tanto del interfaz de usuario de la plataforma como de los contenidos de concienciación y formación en ciberseguridad debe ser el castellano y euskera.

Puesto que el objetivo fundamental de esta plataforma es la evaluación del riesgo de seguridad asociado a las personas, debe permitir la generación de paneles de métricas e indicadores que informen del estado de alerta con suficiente granularidad como para proporcionar información clasificada por colectivos. Estos paneles de indicadores deben actualizarse periódicamente y mostrar su evolución en el tiempo. Esta evaluación permitirá diseñar planes de acción en concienciación de ciberseguridad acordes a los niveles de alerta en cada momento.

La granularidad mencionada es necesaria también para el desarrollo de **itinerarios de concienciación personalizados**, con el objetivo de aumentar la eficacia de estas acciones, aumentar el estado de alerta en ciberseguridad e informar a cada persona de sus resultados y evolución.

Además de las capacidades de formación (e-learning), debe incluir la realización de campañas de simulación y entrenamiento ante las principales amenazas de ciberseguridad para las personas, de manera que pueda adaptarse al perfil de cada una (colectivo y nivel de alerta). Para ello debe incorporar herramientas y algoritmos que permitan incorporar los aspectos psicológicos asociados en la realización de ataques dirigidos a los colectivos de mayor riesgo.

Otro aspecto fundamental de la herramienta debe ser su eficiencia, es decir debe maximizar el rendimiento al tiempo dedicado por cada persona a la concienciación en ciberseguridad.

El proveedor debe ofrecer el uso de la plataforma de evaluación del riesgo en ciberseguridad asociado a las personas en la modalidad SaaS (Software as a Service). La herramienta deberá formar parte del catálogo CPSTIC 105 del CCN.

También se impartirá formación presencial en formato de seminarios, píldoras formativas a toda la plantilla que serán grabados y cuyos videos se colgarán en un espacio accesible para toda la plantilla. Se generarán manuales de seguridad, documentos y videos formativos accesibles para toda la plantilla. Como mínimo, se realizarán al menos 9 jornadas de formación, sensibilización

y gestión del cambio, cuyos contenidos serán propuestos en la oferta y que incluirá como mínimo 3 tipos de formaciones en función del perfil del personal:

- Perfil Comité de Seguridad: incluirá como mínimo:
 - Aspectos generales de ENS
 - Justificación normativa sobre los aspectos incluidos en la política de seguridad, en la normativa de seguridad y en el plan de mejora de seguridad.
 - Recomendaciones y responsabilidades de la alta dirección.
- Perfil personal técnico en sistema de información y administración electrónica: incluirá como mínimo:
 - Política de seguridad y normativa de seguridad y ENS
 - Procedimientos de mejora del sistema de gestión de seguridad.
 - Metodologías para la actualización de documentación.
 - Recomendaciones y responsabilidades de los responsables de seguridad, de los administradores y del comité de seguridad de la información.
- Perfil personas usuarias: incluirá como mínimo:
 - Control de accesos y auditorías
 - Documento de seguridad: aspectos relacionados con los usuarios.
 - Recomendaciones y responsabilidades de los usuarios.

3.1.4. AUDITORÍA INTERNA

Se realizará la Auditoría Interna previa a la auditoría externa, así como la resolución de desviaciones.

La Auditoría Interna, se realizará por un Auditor independiente, acometiendo como mínimo las siguientes actuaciones:

- Desarrollo del Plan de Auditoría (alcance, frecuencia, metodología).
- Revisar la conformidad del sistema de seguridad.
- Revisión documental.
- Revisar el nivel de implementación.
- Revisar la efectividad y adecuación del sistema para cumplir la política y objetivos de seguridad.
- Recopilación de evidencias y registros de cumplimiento.
- Identificar vulnerabilidades y debilidades.
- Proveer la oportunidad de mejorar el SGSI.
- Elaboración del Informe de Auditoría.
- Desarrollo del Plan de Acciones Correctivas (PAC).

3.1.5. ACOMPAÑAMIENTO EN LA AUDITORÍA EXTERNA DE CERTIFICACIÓN

Se dará soporte durante la Auditoría Externa de Certificación de ENS, mediante el acompañamiento presencial durante todo el proceso de auditoría.

Como mínimo se realizarán las siguientes actuaciones:

- Preparación previa a la auditoría, revisando el alcance, criterios y requisitos aplicables y verificando la disponibilidad y adecuación de la documentación y evidencias requeridas.
- Soporte en la organización de la auditoría: planificación de agenda e identificación de interlocutores a entrevistar.
- Revisión y validación de evidencias, asegurando que la información y los registros presentados son coherentes, trazables y alineados con los requisitos normativos o del estándar de referencia.
- Acompañamiento durante la auditoría externa, proporcionando soporte técnico a los responsables municipales, aclarando dudas y ayudando a resolver solicitudes de información planteadas por el Auditor Externo.
- Soporte para la definición, seguimiento y cierre del Plan de Acciones Correctivas (PAC).
- Acompañamiento técnico en la implantación de las acciones correctivas, resolviendo dudas y validando las evidencias generadas.
- Revisión de la adecuación y suficiencia de las evidencias aportadas para el cierre de las acciones.

Seguimiento del grado de avance del PAC y verificación del cierre efectivo de las acciones cuando proceda.

3.2. ENTREGABLES

La empresa adjudicataria deberá presentar los siguientes entregables mínimos:

- Revisión de la Política de Seguridad Municipal y revisión de la Normativa de Seguridad que desarrolla la Política de Seguridad.
- Informe de la situación actual de seguridad "Análisis diferencial o Gap Analysis": estado inicial del Ayuntamiento de Bilbao en relación con la seguridad y grado de cumplimiento de normativas y procedimientos de seguridad existentes que recoja las conclusiones del análisis inicial.
- Informe del resultado del análisis de riesgos.
- Declaración de aplicabilidad: que incluya la relación de medidas de seguridad seleccionadas.
- Plan de Adecuación al ENS.
- Hoja de Ruta de Implantación de la Seguridad.

- Plan de mejora de la seguridad conforme a lo establecido en el Real Decreto 311/2022 que detallará las acciones que es necesario emprender para implementar las medidas de seguridad necesarias para adecuar el sistema al ENS y mitigar los riesgos identificados del análisis. Incluir las medidas de seguridad necesarias para el cumplimiento del NIS2.
- Informe de Auditoría Interna.

3.3. EQUIPO HUMANO: DIRECCIÓN Y EQUIPO TÉCNICO DEL TRABAJO

El equipo de personas asignado al proyecto deberá ajustarse a las necesidades del servicio, asignando los recursos adecuados para la realización de cada tarea, designando personas de los siguientes 3 perfiles:

- Consultor/a director/a del proyecto, que dirigirá el equipo y actuará como interlocutor principal con la persona designada por el Ayuntamiento de Bilbao.
- Consultor/es experto/as en adecuación, implantación del Esquema Nacional de Seguridad, seguridad TIC y ciberseguridad (al menos 2 personas).
- Auditor Independiente en el Esquema Nacional de Seguridad

Se requiere como mínimo que los 3 perfiles cumplan los siguientes requerimientos:

Responsabilidad en el contrato (funciones)	Experiencia profesional (1) y formación exigidas (2)
Consultor/a Director/a del Proyecto	(1) 4 años de experiencia profesional en dirección y coordinación de proyectos de adecuación, implantación y certificación en Esquema Nacional de Seguridad (ENS) (2) Titulación Universitaria Superior o Grado Universitario (Nivel 2 del MECES) o Diplomatura/Ingeniería Técnica
Consultor/a experto/a en adecuación, implantación del Esquema Nacional de Seguridad.	(1) 4 años de experiencia profesional como consultor/a experto/a en adecuación, implantación y certificación en Esquema Nacional de Seguridad (ENS) (2) Titulación Universitaria Superior o Grado Universitario (Nivel 2 del MECES) o Diplomatura/Ingeniería Técnica
Auditor/a Independiente	(1) 4 años de experiencia profesional en auditoría de certificación en Esquema Nacional de Seguridad (ENS) (2) Titulación Universitaria Superior o Grado Universitario (Nivel 2 del MECES) o Diplomatura/Ingeniería Técnica

Deben proponer una figura que realice labores de coordinación con la persona responsable del contrato. Las labores de coordinación consistirán en recibir instrucciones generales por parte

del responsable, coordinar la realización de los proyectos, verificar su nivel de calidad, asumir la responsabilidad de los proyectos y se encargará de la planificación, seguimiento y control de los trabajos a realizar.

Se coordinarán con la DPO municipal, todas las tareas que impacten en el cumplimiento en materia de protección de datos. Anualmente, se facilitará a la DPO una memoria con las actividades realizadas en el ámbito del Esquema Nacional de Seguridad.

El equipo asignado deberá mantenerse durante todo el periodo de ejecución del contrato:

- La discrepancia entre el nivel de conocimientos técnicos del personal ofertado según valores especificados en la oferta, y los conocimientos reales demostrados en la ejecución de los trabajos, dará lugar al requerimiento a la adjudicataria de adopción de medidas para su corrección.
- Si la valoración de la calidad de los trabajos del equipo se considera inadecuada, se podrá solicitar la sustitución de parte del equipo por parte del Ayuntamiento de Bilbao, con un preaviso de 15 días si existen razones justificadas que así lo aconsejen.
- Si la empresa adjudicataria propusiera el cambio de una persona del equipo designada en la oferta lo comunicará por escrito con 15 días de antelación exponiendo los cambios realizados y adjuntará datos de perfil equivalente que adscribirá para sustitución. Se deberá planificar un tiempo de transferencia de conocimiento suficiente que garantice que la sustitución de la persona no va a producir ninguna dilación ni a perjudicar la ejecución de los trabajos. Esta curva de aprendizaje del proyecto será responsabilidad exclusiva de la empresa adjudicataria.
- La adjudicataria habrá de prever la sustitución en caso de enfermedad, accidente o cualquier otra circunstancia imprevista.
- La empresa adjudicataria se responsabilizará de la transmisión interna de conocimiento del proyecto de tal manera que cualquier situación (sustitución, vacaciones, enfermedad, accidente, o cualquier otra circunstancia) no conlleve demora o paralización del proyecto. Esta transmisión de conocimiento del proyecto será responsabilidad exclusiva de la empresa adjudicataria.

Los medios humanos aportados por la adjudicataria para la ejecución del contrato estarán sometidos al poder de dirección y organización de la adjudicataria en todo ámbito y orden legalmente establecido; será por tanto la adjudicataria el único responsable de dicho personal, no teniendo por tanto, vinculación jurídico-laboral alguna con el Ayuntamiento de Bilbao. Todo ello con independencia del control de la ejecución del contrato que corresponda.

El cumplimiento de lo previsto en esta cláusula **así como de los compromisos contenidos en su oferta respecto al equipo humano** se considera **obligación contractual esencial** de forma que su incumplimiento por parte del contratista podrá ser causa de resolución del contrato.

3.4. PLANIFICACIÓN Y GESTIÓN DEL PROYECTO

3.4.1. COMITÉ PARA COORDINACIÓN/ DIRECCIÓN DEL CONTRATO/ PROYECTO

Se formará un **Comité para la coordinación y dirección del contrato/proyecto**, que estará compuesto por las personas responsables del Ayuntamiento de Bilbao, BILBAOTIK S.A., una persona de la adjudicataria y cuantas otras personas designen las partes. Las tareas del Comité para la coordinación y dirección del contrato/proyecto, son entre otras:

- Seguimiento y coordinación del proyecto.
- Control y gestión de riesgos.

3.4.2. IDENTIFICACIÓN Y GESTIÓN DE ACCIONES CORRECTORAS FRENTE A RIESGOS IDENTIFICADOS

- Control y gestión de cambios en el alcance o en la planificación.
- Gestión de recursos.
- Gestión del cambio.
- Gestión de la documentación.
- Adecuada transferencia del conocimiento.

Asimismo, el Ayuntamiento de Bilbao designará la persona/s que desempeñará/n la **Dirección del Proyecto** que se encargará de la planificación, seguimiento y control de los trabajos a realizar y **una Subdirección del Proyecto** que apoyará en la realización de dichas funciones. Asimismo, por parte de BILBAOTIK S.A. se designará una **Subdirección Técnica del Proyecto** (integrada como mínimo por dos personas) que realizará el seguimiento, control y validación de los trabajos tecnológicos.

3.4.3. PLANIFICACIÓN

La empresa adjudicataria deberán describir los aspectos de **planificación del proyecto**, incluyendo de la forma más detallada posible el **calendario** previsto para el desarrollo de éste, los plazos parciales y totales comprometidos, así como los de la ejecución para cada uno de los conjuntos de trabajos en los que el mismo se descomponga. Cumpliendo la planificación del proyecto e hitos definidos en el presente documento y desarrollado en este punto, la empresa adjudicataria tiene que entregar el plan de proyecto estableciendo los hitos principales del proyecto, definiendo y concretando cualquier aspecto del alcance del mismo. En él se identificarán:

- Descripción de los trabajos y tareas a realizar, sus dependencias, sus hitos, indicadores y entregables resultantes

- Interlocutores necesarios para cada tarea, así como la identificación de la información y/o documentación a recopilar, elaborar y/o revisar.
- Asignación de las personas responsables de la ejecución.
- Metodologías a aplicar.
- Detalle de jornadas.
- Etc...

Dentro de la planificación, para un periodo máximo de DOS AÑOS desde la formalización del contrato, se han de cumplir los siguientes hitos más relevantes:

- Revisar el Marco Normativo y la Implantación de la seguridad.
- Aprobar el Sistema de Gestión de Seguridad de la información y revisión continua.
- Cumplimiento del Esquema Nacional de Seguridad (ENS) y al NIS2.
- Definir indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad y actualización mensual de los mismos.
- Despliegue de herramientas para mejorar cumplimiento normativo.
- Plan de Gestión del cambio.
- Elaborar Plan de Adecuación al ENS.
- Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.
- Sensibilización, Concienciación y Formación de toda la Plantilla Municipal.
- Definir Métricas e Indicadores del Estado de la Seguridad y reportar a las autoridades pertinentes
- Auditoría Interna en ENS.
- Revisión continua del Sistema de Gestión de Seguridad.
- Elaboración del Plan de convergencia para el cumplimiento de lo dispuesto en NIS2.
- Realización de ejercicios de hacking ético.
- Coordinación con la DPO municipal.
- Vigilancia y Mejora continua
- Hacking ético.
- Modelo de seguimiento y evaluación a realizar durante el proyecto.
- Acompañamiento presencial durante todo el proceso de auditoría externa de certificación en ENS.
- Acompañamiento y asesoramiento durante todo el proceso hasta obtener la certificación en el Esquema Nacional de Seguridad

La planificación trimestral del cumplimiento de estos hitos anteriores, serán los siguientes:

1.- Hitos que se ejecutarán de forma Continua:

- Actualización mensual de los indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad.
- Revisar el Marco Normativo y la Implantación de la seguridad.

- Revisión continua del Sistema de Gestión de Seguridad de la información
- Sensibilización, Concienciación y Formación Continua de toda la Plantilla Municipal (el foco principal ha de ser en el tercer y cuarto trimestre).
- Reportar a las autoridades pertinentes cuando proceda, la información asociada a las Métricas e Indicadores del Estado de la Seguridad.
- Coordinación con la DPO municipal.
- Seguimiento y evaluación a realizar durante el proyecto según el modelo definido.
- Acompañamiento y asesoramiento durante todo el proceso hasta obtener la certificación en el Esquema Nacional de Seguridad.

2.-Hitos a ejecutar en cada Trimestre:

Primer Trimestre:

- Revisión de la Política de Seguridad Municipal y revisión de la Normativa de Seguridad que desarrolla la Política de Seguridad.
- Elaborar un informe de la situación actual de seguridad “análisis diferencial o gap análisis”: estado inicial del Ayuntamiento de Bilbao en relación con la seguridad y grado de cumplimiento de normativas y procedimientos de seguridad existentes que recoja las conclusiones del análisis inicial.
- Informe del resultado del Análisis de Riesgos.
- Declaración de aplicabilidad que incluya la relación de medidas de seguridad seleccionadas.
- Elaborar Plan de Adecuación al Esquema Nacional de Seguridad.
- Elaboración del Plan de convergencia para el cumplimiento de lo dispuesto en NIS2.
- Plan de Mejora de la Seguridad conforme a lo establecido en el RD 311/2022 que detallará las acciones que es necesario emprender para implementar las medidas de seguridad necesarias para adecuar el sistema del ENS y mitigar los riesgos identificados del análisis. Incluir las medidas de seguridad necesarias para el cumplimiento del NIS2.
- Definir indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad y actualización mensual de los mismos.
- Aprobar el Sistema de Gestión de Seguridad de la información y revisión continua.
- Definir Métricas e Indicadores del Estado de la Seguridad y reportar a las autoridades pertinentes.
- Modelo de seguimiento y evaluación a realizar durante el proyecto.

Segundo Trimestre:

- Despliegue de herramientas para mejorar cumplimiento normativo.
- 50% Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.

Tercer Trimestre:

- 50% Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.
- Plan de Gestión del cambio.
- 50% Sensibilización, Concienciación y Formación de toda la Plantilla Municipal.

Cuarto Trimestre:

- 50% Sensibilización, Concienciación y Formación de toda la Plantilla Municipal.
- Realización de ejercicios de hacking ético.

Quinto Trimestre:

- Auditoría Interna en ENS.
- Informe de Auditoría Interna de ENS.

Sexto Trimestre

- Acompañamiento presencial durante todo el proceso de auditoría externa de certificación en ENS.
- Definición del PAC Plan de Actuaciones Correctivas.

Séptimo y Octavo trimestre

- Obtención de la Certificación del ENS por parte del Ayuntamiento de Bilbao en el alcance que se defina en el presente contrato

Una vez formalizado el contrato, y en el plazo máximo de siete (7) días naturales, se revisará el plan propuesto y el/la Responsable del proyecto, con la colaboración de los demás miembros del equipo de proyecto, validará el plan de trabajo definitivo, que se registrará en el Acta de Inicio del contrato. Este plan de trabajo deberá mantenerse actualizado y consensado entre el Ayuntamiento de Bilbao, BILBAOTIK S.A. y la empresa adjudicataria.

3.4.4. CALIDAD, SEGUIMIENTO Y CONTROL DE LOS TRABAJOS

La empresa adjudicataria debe establecer todos aquellos procedimientos de control que permita verificar de forma continuada el cumplimiento de los objetivos especificados, tanto en los plazos como en la calidad final.

Durante la ejecución del trabajo, se presentará un informe de las horas (unidades y %) imputadas a cada perfil profesional que se ejecuten cada mes.

La empresa adjudicataria deberá nombrar un/a Director/a del proyecto que será el responsable de los trabajos en todos sus aspectos. Esta persona será la encargada de convocar las reuniones

de seguimiento, realizar informes de seguimiento para la adecuada evaluación y mejora continua y cuantas reuniones estime oportuno para el correcto desarrollo de los trabajos.

Como mínimo, se realizarán las siguientes actividades de seguimiento y control de los trabajos:

- Se realizará una primera reunión de lanzamiento, al inicio del proyecto; en ella intervendrán los interlocutores que designe el Ayuntamiento de Bilbao, BILBAOTIK S.A. así como las personas designadas por parte de la empresa adjudicataria. Su objetivo es establecer las principales líneas del proyecto.
- Semanalmente, se realizará una reunión de seguimiento. Por cada reunión de seguimiento, la empresa adjudicataria hará un resumen de los trabajos realizados desde la última reunión de seguimiento y elaborará su correspondiente acta, que deberá ser visada por los asistentes a la misma. Previamente al visado del acta, el Ayuntamiento de Bilbao, BILBAOTIK S.A. revisarán los trabajos ya realizados y comprobarán si se corresponden con las tareas planificadas en su momento. Todas aquellas tareas que estime interesantes la empresa adjudicataria y que pretenda llevar a cabo durante esa semana, serán propuestas al Ayuntamiento de Bilbao, BILBAOTIK S.A. para su aceptación o rechazo.
- Para el seguimiento de los trabajos será necesario entregar un informe con la evolución de los trabajos. Tras la revisión, el/la Responsable del Contrato o el/la Director del Proyecto nombrado por el Ayuntamiento de Bilbao, comunicará a la empresa adjudicataria su aprobación o en su caso, el rechazo total o parcial, en su caso, de los trabajos realizados, en la medida que no respondan a lo acordado, o no superen los controles de calidad.

Inicialmente se estima un informe cada mes.

En caso de detectarse desviaciones entre la planificación y la situación real del trabajo desarrollado, la empresa adjudicataria deberá emprender las acciones correctivas apropiadas, tras ser consensuadas con el Ayuntamiento de Bilbao, BILBAOTIK S.A.

- A petición de cualquiera de las partes, se celebrarán reuniones extraordinarias, con el objetivo de subsanar cualquier incidencia grave que requiera una respuesta inmediata y no pueda esperar a la reunión de seguimiento.
- En la reunión de cierre, que es la última reunión del proyecto, para dar por finalizado el contrato, deberá validarse por el Ayuntamiento de Bilbao, el Acta de Recepción o Cierre tras la validación técnica de BILBAOTIK S.A., por el que se dará el Vº Bº a los trabajos realizados.
- El Ayuntamiento de Bilbao no tendrán responsabilidad directa, solidaria, ni subsidiaria respecto al cumplimiento de las obligaciones laborales de la empresa adjudicataria, así como tampoco de las que se puedan derivar, en su caso, de la extinción de los contratos de trabajo, tanto durante la vigencia del presente contrato, como con posterioridad a su terminación, asumiendo la empresa adjudicataria la totalidad de las consecuencias jurídico laborales derivadas de los mismos.
- El Ayuntamiento de Bilbao y/o BILBAOTIK S.A. no tendrán ninguna facultad organizativa ni de dirección respecto a las personas que presten sus servicios para la empresa

adjudicataria, ni existirá relación jurídico laboral, civil o administrativa alguna con las mismas.

3.4.5. DOCUMENTACIÓN A ENTREGAR

La documentación generada durante la ejecución del contrato será propiedad exclusiva de del Ayuntamiento de Bilbao sin que la adjudicataria pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización del Ayuntamiento de Bilbao, que la facilitaría, en su caso, previa petición formal de la adjudicataria con expresión del fin.

La documentación se entregará en soporte electrónico de forma que el Ayuntamiento de Bilbao pueda efectuar el mantenimiento de la misma posteriormente.

La adjudicataria será responsable de mantener actualizada la documentación del contrato a lo largo del mismo. Asimismo, deberá mantener un registro histórico de los cambios producidos en la documentación con una breve explicación de la causa que originó los mismos.

3.5. CONTEXTO DEL ENTORNO TECNOLÓGICO E INFRAESTRUCTURA TECNOLÓGICA MUNICIPAL

A aquellas empresas que tengan interés en la presentación de la Oferta, previa petición identificándose la empresa, se les facilitará información sobre el contexto de la Infraestructura Tecnológica Municipal actualmente existente en el entorno municipal. Dicha petición se ha de dirigir al correo modernizazioa@bilbao.eus

3.6 PRECIO

El importe total del contrato, se realizarán **pagos trimestrales** asociados al cumplimiento de los Hitos Planificados según el Calendario de Planificación del Proyecto, previa validación por parte del Ayuntamiento de Bilbao y BilbaoTIK; así pues se abonarán los siguientes porcentajes sobre el precio de adjudicación de la parte 1: “Certificación en ENS del Ayuntamiento de Bilbao” asociados al cumplimiento de los hitos:

- 2,81% +IVA/trimestre se abonarán por la ejecución de los hitos que se ejecutarán de forma continua
- 25% + IVA se abonarán en el primer trimestre por la ejecución de los hitos planificados para el primer trimestre
- 12,5% + IVA se abonarán en el segundo trimestre por la ejecución de los hitos planificados para el segundo trimestre.
- 12,5% + IVA se abonarán en el tercer trimestre por la ejecución de los hitos planificados para el tercer trimestre.

- 12,5% + IVA se abonarán en el cuarto trimestre por la ejecución de los hitos planificados para el cuarto trimestre
- 3,75% + IVA se abonarán en el quinto trimestre por la ejecución de los hitos planificados para el quinto trimestre.
- 1,27% + IVA se abonarán en el sexto trimestre por la ejecución de los hitos planificados para el sexto trimestre.
- 10% + IVA se abonarán en el momento que se haya obtenido la Certificación del Esquema de Seguridad Nacional por parte del Ayuntamiento de Bilbao

Por cada trimestre, se abonará el % de los hitos planificados ejecutados definidos anteriormente sobre el precio de adjudicación del contrato de la parte 1: “Certificación en ENS del Ayuntamiento de Bilbao”, abonándose el sumatorio de los hitos ejecutados, en función del % designado a cada hito:

1.- Importe de pago de Hitos a ejecutar de forma Continua:

- 20%: Actualización mensual de los indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad.
- 10%: Revisar el Marco Normativo y la Implantación de la seguridad.
- 10%: Revisión continua del Sistema de Gestión de Seguridad de la información
- 10%: Sensibilización, Concienciación y Formación Continua de toda la Plantilla Municipal (el foco principal ha de ser en el tercer y cuarto trimestre).
- 4%: Reportar a las autoridades pertinentes cuando proceda, la información asociada a las Métricas e Indicadores del Estado de la Seguridad.
- 6%: Coordinación con la DPO municipal.
- 20%: Seguimiento y evaluación a realizar durante el proyecto según el modelo definido.
- 20%: Acompañamiento y asesoramiento durante todo el proceso hasta obtener la certificación en el Esquema Nacional de Seguridad.

2.-Importe de pago de Hitos a ejecutar en cada Trimestre:

Primer Trimestre:

- 10%: Revisión de la Política de Seguridad Municipal y revisión de la Normativa de Seguridad que desarrolla la Política de Seguridad.
- 15%: Elaborar un informe de la situación actual de seguridad “análisis diferencial o gap análisis”: estado inicial del Ayuntamiento de Bilbao en relación con la seguridad y grado de cumplimiento de normativas y procedimientos de seguridad existentes que recoja las conclusiones del análisis inicial.
- 10%: Informe del resultado del Análisis de Riesgos.
- 4%: Declaración de aplicabilidad que incluya la relación de medidas de seguridad seleccionadas.
- 25%: Elaborar Plan de Adecuación al Esquema Nacional de Seguridad.

- 10%: Elaboración del Plan de convergencia para el cumplimiento de lo dispuesto en NIS2.
- 10%: Plan de Mejora de la Seguridad conforme a lo establecido en el RD 311/2022 que detallará las acciones que es necesario emprender para implementar las medidas de seguridad necesarias para adecuar el sistema del ENS y mitigar los riesgos identificados del análisis. Incluir las medidas de seguridad necesarias para el cumplimiento del NIS2.
- 4%: Definir indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad y actualización mensual de los mismos.
- 3%: Aprobar el Sistema de Gestión de Seguridad de la información y revisión continua.
- 4%: Definir Métricas e Indicadores del Estado de la Seguridad y reportar a las autoridades pertinentes.
- 5%: Modelo de seguimiento y evaluación a realizar durante el proyecto.

Segundo Trimestre:

- 30%: Despliegue de herramientas para mejorar cumplimiento normativo.
- 70%: 50% Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.

Tercer Trimestre:

- 60%: 50% Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.
- 10%: Plan de Gestión del cambio.
- 30%: 50% Sensibilización, Concienciación y Formación de toda la Plantilla Municipal.

Cuarto Trimestre:

- 70%: 50% Sensibilización, Concienciación y Formación de toda la Plantilla Municipal.
- 30%: Realización de ejercicios de hacking ético.

Quinto Trimestre:

- 50%: Auditoría Interna en ENS.
- 50%: Informe de Auditoría Interna de ENS.

Sexto Trimestre

- 50%: acompañamiento presencial durante todo el proceso de auditoría externa de certificación en ENS.
- 50%: Definición del PAC Plan de Actuaciones Correctivas.

Séptimo y Octavo trimestre

- 100%: Obtención de la Certificación del ENS por parte del Ayuntamiento de Bilbao en el alcance que se defina en el presente contrato.

3.7. PROTECCIÓN DE DATOS

Los datos recibidos deberán cumplir con los requisitos legales actualmente establecidos para la protección de datos personales según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3.8 SEGURIDAD DE LA INFORMACIÓN

Se requiere que la empresa adjudicataria disponga del Certificado de conformidad con el Esquema Nacional de Seguridad categoría alta: Las medidas de seguridad a aplicar en los servicios objeto de este contrato y en los posibles sistemas de información desarrollados/desplegados/mantenidos serán las que correspondan del Anexo II del ENS, para la categoría ALTA .

Se requiere que la empresa adjudicataria disponga del certificado ISO 27.001, norma internacional para la gestión de la seguridad de la información.

4. PARTE 2: CERTIFICACIÓN EN ENS DE LAS ENTIDADES MUNICIPALES ADHERIDAS

Las Entidades Municipales Adheridas al presente contrato son las siguientes:

- Bilbao Musika, O.A.L.
- Bilbao Zerbitzuak – Servicios, EPEL
- Centro Azkuna de Sociedad y Cultura Contemporánea S.A.
- Funicular de Artxanda, S.A.
- C.A.C. Teatro Arriaga, S.A.

4.1. ALCANCE DEL CONTRATO

El objeto del contrato es la prestación de servicio de **consultoría** para obtener la **Certificación de conformidad con el Esquema Nacional de Seguridad (en adelante, ENS) de los sistemas**

tecnológicos de información y soluciones tecnológicas alojados en la infraestructura municipal de BILBAOTIK S.A. de cada Entidad Municipal Adherida al presente contrato:

- Bilbao Musika, O.A.L.
- Bilbao Zerbitzuak – Servicios, EPEL
- Centro Azkuna de Sociedad y Cultura Contemporánea S.A.
- Funicular de Artxanda, S.A.
- C.A.C. Teatro Arriaga, S.A.

4.1.1. ADECUACIÓN CON EL ESQUEMA NACIONAL DE SEGURIDAD

4.1.1.1. Plan de Adecuación.

La Certificación y Conformidad con el ENS de cada entidad municipal adherida al presente contrato, conlleva la elaboración previa de un **Plan de Adecuación** que incluya como mínimo, las **cuatro fases previas siguientes**:

- Revisión de la **Política de Seguridad**
- Determinación de la **Categoría de los sistemas**
- **Análisis de Riesgos**
- **Declaración de Aplicabilidad/Perfil de Cumplimiento.**

El Plan de Adecuación dispondrá como mínimo, por cada una de las entidades municipales adheridas al presente contrato, de la siguiente información: el alcance de los sistemas que se van a someter al proceso de certificación en el ENS, la categoría los mismos, qué medidas del Anexo II del Esquema Nacional de Seguridad se van a implementar (Declaración de Aplicabilidad), qué riesgos se asumen, la Política de Seguridad del Ayuntamiento de Bilbao y entidades municipales adheridas al presente contrato con su organización de la seguridad...

Para abordar de forma eficiente el **Plan de Adecuación de cada Entidad Municipal Adherida al presente contrato**, es necesario realizar como mínimo los siguientes pasos para cada una de las fases:

FASE 0: Planificación: Identificar el alcance del sistema. Para ello se evaluarán las diferentes alternativas con el objetivo de buscar un sistema factible de certificar.

FASE 1: Revisión de la Política de Seguridad

- Revisando y aprobando los cambios necesarios en la política de seguridad del ayuntamiento y de la entidad municipal adherida al presente contrato.
- Definición de roles y asignación de personas
- Modelo de organización de la seguridad

- Revisar la Política de Seguridad y el modelo de gobernanza de la seguridad: Comité de seguridad, Comité de Crisis, Cyberzaintza y analizar la necesidad de otros órganos de coordinación/alineamiento de seguridad de la información en el ámbito municipal.

FASE 2: Determinación de la categoría de los sistemas,

- Inventario de la Información y los Servicios, teniendo en cuenta las implicaciones en materia de protección de Datos.
- Valorar la información y los servicios de cada una de sus dimensiones (disponibilidad, autenticidad, confidencialidad, integridad y trazabilidad) según “niveles de importancia”: Bajo, Medio y Alto.
- Determinar la categoría de los sistemas

FASE 3: Análisis de Riesgos: Se deberá realizar un análisis previo y diagnóstico inicial de cumplimiento y aplicación del ENS, que incluya además la revisión de inventario de activos, comprobación de su valoración y la definición de responsabilidades. Se deberá realizar un análisis y tratamiento de los riesgos de seguridad a los que están expuestas las entidades municipales adheridas al presente contrato, que incluya la valoración de las medidas de seguridad existentes, así como determinar los controles de seguridad necesarios para dotarles de una protección eficaz.

- Identificación de activos y sus dependencias
- Valoración de amenazas y salvaguardas
- Analizar impacto y riesgo
- Utilización de la Herramienta de referencia municipal

FASE 4: Declaración de Aplicabilidad/Perfil de Cumplimiento: Validar la Declaración de Aplicabilidad Definitiva o evaluar la posibilidad de adherirse a un Perfil de Cumplimiento Específico.

4.1.1.2. Implantación de la Seguridad.

Una vez realizado el Plan de Adecuación de cada entidad municipal adherida al presente contrato, se pasa a la fase de implantación de la Seguridad. Esta fase consta de los siguientes pasos:

- Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades, que sirva de base para poner en marcha las acciones necesarias para asegurar el cumplimiento normativo. Las recomendaciones y la hoja de ruta deberán incluir todo tipo de acciones para el total cumplimiento normativo y adecuación al ENS, cuantificarlas e incluir una propuesta de calendario para las mismas, incluyendo todos los medios técnicos, materiales, funcionales y de cualquier tipo incluyendo estimación económica y temporal.

- Revisar el Marco Normativo, la Política de Seguridad, la Normativa de Seguridad que desarrolla la Política de Seguridad y la Implantación de la seguridad.
- Elaborar Procedimientos relacionados con los controles de ENS ajustados a la categoría del sistema.
- Crear instrucciones técnicas.
- Proponer, consensuar e implantar un sistema para recoger las acciones realizadas en materia de ENS.
- Aprobar el Sistema de Gestión de la Seguridad de la Información y revisión continua.

4.1.1.3. Declaración/ Certificación de Conformidad

La determinación de la conformidad de los sistemas de información del ámbito de aplicación de ENS de cada entidad municipal adherida al presente contrato, se determinará según dos procedimientos distintos según se trate de categoría Media, Alta o Básica:

- La conformidad de los sistemas de información del ámbito de aplicación del ENS en las categorías MEDIA o ALTA se realizará mediante una auditoría formal que verifique los requerimientos contemplados en el ENS, al menos cada dos años, o con carácter extraordinario si se producen modificaciones significativas.
- La conformidad de los sistemas de información en la categoría BÁSICA requiere de una autoevaluación que verifique su cumplimiento al menos cada dos años o, con carácter extraordinario si se producen modificaciones significativas. Este requisito para la conformidad no impide que un sistema de categoría BÁSICA se someta a una auditoría formal.

4.1.1.4. Informar sobre el estado de Seguridad. Métricas e Indicadores

Los organismos a los que se aplica el ENS están obligados a cumplimentar e informar sobre el Estado de Seguridad.

Para cumplir con este mandato, el CCN ha desarrollado el proyecto INES (Informe Nacional del Estado de Seguridad).

Informar a la Agencia Vasca de Ciberseguridad Cyberzaintza y a la Autoridad Vasca de protección de Datos, cuando proceda.

4.1.1.5. Vigilancia y Mejora Continua.

La gestión de la seguridad de la información de cada entidad municipal adherida al presente contrato, es un proceso sujeto a cambios constantes que pueden proceder de cambios en la organización, amenazas, tecnologías y/o legislación y por ello es necesaria una mejora continua de nuestros sistemas.

Esta actualización continua por parte de cada entidad municipal adherida al presente contrato, conllevará entre otras acciones:

- Revisión de la Política de Seguridad de la Información
- Revisión de la Normativa de Seguridad que desarrolla la Política de Seguridad
- Revisión de la información y los servicios, y su categorización
- Actualización del análisis y gestión de riesgos, al menos anualmente
- Revisión de la Declaración de Aplicabilidad o del Perfil de Cumplimiento
- Realización de auditorías internas
- Revisión del Plan de Mejora
- Revisión de las medidas de seguridad
- Revisión y actualización de procedimientos
- Revisión de las métricas
- Revisión del Estado de Seguridad (INÉS), Agencia Vasca de Ciberseguridad (Cyberzaintza), Autoridad Vasca de Protección de Datos...
- Revisión por la Dirección

4.1.2. SERVICIOS ORIENTADOS AL CUMPLIMIENTO DEL NIS2

Por cada entidad municipal adherida al presente contrato, se realizará un plan de convergencia para el cumplimiento de lo dispuesto en NIS2.

Los servicios de análisis de riesgos deberán de acompañarse de ejercicios de hacking ético que permitan comprobar el nivel real de seguridad a nivel de infraestructura y aplicaciones corporativas.

Respecto a la gestión de incidentes de seguridad, se establecerá procedimientos de gestión de violaciones de seguridad de los datos.

4.1.3. DESPLIEGUE DE HERRAMIENTAS ORIENTADAS A MEJORAR EL NIVEL DE PROTECCIÓN Y CUMPLIMIENTO NORMATIVO

4.1.3.1. Identificación de necesidades de seguridad

En cada entidad municipal adherida al presente contrato, se identificarán necesidades para mejorar el nivel de seguridad y cumplimiento normativo, con la colaboración de BilbaoTIK, la empresa tecnológica del Ayuntamiento de Bilbao.

Se verificará el cumplimiento de las guías CCN-STIC por parte de BilbaoTIK en la realización del bastionado de sistemas.

4.1.3.2. Plataforma de formación al personal

Se realizará la **formación, concienciación y sensibilización** en materia de seguridad del personal de cada entidad municipal adherida al presente contrato, como una medida fundamental de reducción del riesgo de seguridad.

Para que las acciones de concienciación sean realmente efectivas es necesario disponer de una plataforma automatizada que permita:

- Evaluar el riesgo de seguridad asociado a las personas.
- Disponer de métricas e indicadores que permitan medir tanto el nivel de riesgo como la eficacia de las acciones de concienciación y el nivel de alerta de las personas.
- Aumentar o mantener el estado de alerta en ciberseguridad de las personas.
- Elaborar planes de acción y realizar actividades de formación dirigidas a colectivos específicos en diferentes formatos.
- Lanzar campañas de ataque dirigido a colectivos específicos de las principales amenazas en ciberseguridad orientadas a las personas.

Se pondrá en marcha una plataforma software que permita evaluar el riesgo de ciberseguridad asociado a las personas y concienciar en diferentes áreas de la ciberseguridad y de las amenazas de mayor riesgo: ingeniería social, phishing, manejo de cuentas y credenciales, etc.

La plataforma debe permitir la adaptación automática de los contenidos en función tanto del desarrollo de las acciones en el tiempo y de los indicadores de alerta, como de la evolución de las amenazas.

El **idioma nativo** tanto del interfaz de usuario de la plataforma como de los contenidos de concienciación y formación en ciberseguridad debe ser el castellano y euskera.

Puesto que el objetivo fundamental de esta plataforma es la evaluación del riesgo de seguridad asociado a las personas, debe permitir la generación de paneles de métricas e indicadores que informen del estado de alerta con suficiente granularidad como para proporcionar información clasificada por colectivos. Estos paneles de indicadores deben actualizarse periódicamente y mostrar su evolución en el tiempo. Esta evaluación permitirá diseñar planes de acción en concienciación de ciberseguridad acordes a los niveles de alerta en cada momento.

La granularidad mencionada es necesaria también para el desarrollo de **itinerarios de concienciación personalizados**, con el objetivo de aumentar la eficacia de estas acciones, aumentar el estado de alerta en ciberseguridad e informar a cada persona de sus resultados y evolución.

Además de las capacidades de formación (e-learning), debe incluir la realización de campañas de simulación y entrenamiento ante las principales amenazas de ciberseguridad para las personas, de manera que pueda adaptarse al perfil de cada una (colectivo y nivel de alerta). Para ello debe incorporar herramientas y algoritmos que permitan incorporar los aspectos psicológicos asociados en la realización de ataques dirigidos a los colectivos de mayor riesgo.

Otro aspecto fundamental de la herramienta debe ser su eficiencia, es decir debe maximizar el rendimiento al tiempo dedicado por cada persona a la concienciación en ciberseguridad.

El proveedor debe ofrecer el uso de la plataforma de evaluación del riesgo en ciberseguridad asociado a las personas en la modalidad SaaS (Software as a Service). La herramienta deberá formar parte del catálogo CPSTIC 105 del CCN.

También se impartirá formación presencial en formato de seminarios, píldoras formativas a toda la plantilla de cada entidad municipal adherida al presente contrato que serán grabados y cuyos videos se colgarán en un espacio accesible para toda la plantilla. Se generarán manuales de seguridad, documentos y videos formativos accesibles para toda la plantilla. Como mínimo, se realizarán al menos 9 jornadas de formación, sensibilización y gestión del cambio, cuyos contenidos serán propuestos en la oferta y que incluirá como mínimo 3 tipos de formaciones en función del perfil del personal:

- Perfil Comité de Seguridad: incluirá como mínimo:
 - Aspectos generales de ENS
 - Justificación normativa sobre los aspectos incluidos en la política de seguridad, en la normativa de seguridad y en el plan de mejora de seguridad.
 - Recomendaciones y responsabilidades de la alta dirección.
- Perfil personal técnico en sistema de información y administración electrónica: incluirá como mínimo:
 - Política de seguridad y normativa de seguridad y ENS
 - Procedimientos de mejora del sistema de gestión de seguridad.
 - Metodologías para la actualización de documentación.
 - Recomendaciones y responsabilidades de los responsables de seguridad, de los administradores y del comité de seguridad de la información.
- Perfil personas usuarias: incluirá como mínimo:
 - Control de accesos y auditorías
 - Documento de seguridad: aspectos relacionados con los usuarios.
 - Recomendaciones y responsabilidades de los usuarios.

4.1.4. AUDITORÍA INTERNA

Se realizará la Auditoría Interna previa a la auditoría externa en cada una de las entidades municipales adheridas al presente contrato, así como la resolución de desviaciones.

La Auditoría Interna, se realizará por un Auditor independiente, acometiendo como mínimo las siguientes actuaciones:

- Desarrollo del Plan de Auditoría (alcance, frecuencia, metodología).
- Revisar la conformidad del sistema de seguridad.
- Revisión documental.
- Revisar el nivel de implementación.

- Revisar la efectividad y adecuación del sistema para cumplir la política y objetivos de seguridad.
- Recopilación de evidencias y registros de cumplimiento.
- Identificar vulnerabilidades y debilidades.
- Proveer la oportunidad de mejorar el SGSI.
- Elaboración del Informe de Auditoría.
- Desarrollo del Plan de Acciones Correctivas (PAC).

4.1.5. ACOMPAÑAMIENTO EN LA AUDITORÍA EXTERNA DE CERTIFICACIÓN

Se dará soporte durante la Auditoría Externa de Certificación de ENS en cada una de las entidades municipales adheridas al presente contrato, mediante el acompañamiento presencial durante todo el proceso de auditoría.

Como mínimo se realizarán las siguientes actuaciones:

- Preparación previa a la auditoría, revisando el alcance, criterios y requisitos aplicables y verificando la disponibilidad y adecuación de la documentación y evidencias requeridas.
- Soporte en la organización de la auditoría: planificación de agenda e identificación de interlocutores a entrevistar.
- Revisión y validación de evidencias, asegurando que la información y los registros presentados son coherentes, trazables y alineados con los requisitos normativos o del estándar de referencia.
- Acompañamiento durante la auditoría externa, proporcionando soporte técnico a los responsables de las entidades municipales, aclarando dudas y ayudando a resolver solicitudes de información planteadas por el Auditor Externo.
- Soporte para la definición, seguimiento y cierre del Plan de Acciones Correctivas (PAC).
- Acompañamiento técnico en la implantación de las acciones correctivas, resolviendo dudas y validando las evidencias generadas.
- Revisión de la adecuación y suficiencia de las evidencias aportadas para el cierre de las acciones.

Seguimiento del grado de avance del PAC y verificación del cierre efectivo de las acciones cuando proceda.

4.2. ENTREGABLES

La empresa adjudicataria deberá presentar los siguientes entregables mínimos por cada entidad municipal adherida al presente contrato:

- Revisión de la Política de Seguridad Municipal y de las entidades municipales adheridas y revisión de la Normativa de Seguridad que desarrolla la Política de Seguridad.

- Informe de la situación actual de seguridad: "Análisis diferencial o Gap Analysis": estado inicial de cada entidad municipal adherida al presente contrato, en relación con la seguridad y grado de cumplimiento de normativas y procedimientos de seguridad existentes que recoja las conclusiones del análisis inicial.
- Informe del resultado del análisis de riesgos.
- Declaración de aplicabilidad: que incluya la relación de medidas de seguridad seleccionadas.
- Plan de Adecuación al ENS.
- Hoja de Ruta de Implantación de la Seguridad.
- Plan de mejora de la seguridad conforme a lo establecido en el Real Decreto 311/2022 que detallará las acciones que es necesario emprender para implementar las medidas de seguridad necesarias para adecuar el sistema al ENS y mitigar los riesgos identificados del análisis. Incluir las medidas de seguridad necesarias para el cumplimiento del NIS2.
- Informe de Auditoría Interna.

4.3. EQUIPO HUMANO: DIRECCIÓN Y EQUIPO TÉCNICO DEL TRABAJO

El equipo de personas asignado al proyecto de cada entidad municipal adherida al presente contrato, deberá ajustarse a las necesidades del servicio, asignando los recursos adecuados para la realización de cada tarea, designando personas de los siguientes 3 perfiles:

- Consultor/a director del proyecto, que dirigirá el equipo y actuará como interlocutor principal con la persona designada por el Ayuntamiento de Bilbao.
- Consultor/es experto/as en adecuación, implantación del Esquema Nacional de Seguridad, seguridad TIC y ciberseguridad (al menos 2 personas).
- Auditor Independiente en el Esquema Nacional de Seguridad

Se requiere como mínimo que los 3 perfiles cumplan los siguientes requerimientos:

Responsabilidad en el contrato (funciones)	Experiencia profesional (1) y formación exigidas (2)
Consultor/a Director/a del Proyecto	(1) 4 años de experiencia profesional en dirección y coordinación de proyectos de adecuación, implantación y certificación en Esquema Nacional de Seguridad (ENS)
	(2) Titulación Universitaria Superior o Grado Universitario (Nivel 2 del MECES) o Diplomatura/Ingeniería Técnica
Consultor/a experto/a en adecuación, implantación del Esquema	(1) 4 años de experiencia profesional como consultor/a experto/a en adecuación, implantación y certificación en Esquema Nacional de Seguridad (ENS)
	(2) Titulación Universitaria Superior o Grado Universitario (Nivel 2 del MECES) o Diplomatura/Ingeniería Técnica

Nacional de Seguridad.	
Auditor/a Independiente	(1) 4 años de experiencia profesional en auditoría de certificación en Esquema Nacional de Seguridad (ENS)
	(2) Titulación Universitaria Superior o Grado Universitario (Nivel 2 del MECES) o Diplomatura/Ingeniería Técnica

Deben proponer una figura que realice labores de coordinación con la persona responsable del contrato por parte de cada entidad municipal adherida al presente contrato. Las labores de coordinación consistirán en recibir instrucciones generales por parte del responsable, coordinar la realización de los proyectos, verificar su nivel de calidad, asumir la responsabilidad de los proyectos y se encargará de la planificación, seguimiento y control de los trabajos a realizar.

Se coordinarán con la DPO municipal, todas las tareas que impacten en el cumplimiento en materia de protección de datos. Anualmente, se facilitará a la DPO una memoria con las actividades realizadas en el ámbito del Esquema Nacional de Seguridad.

El equipo asignado deberá mantenerse durante todo el periodo de ejecución del contrato:

- La discrepancia entre el nivel de conocimientos técnicos del personal ofertado según valores especificados en la oferta, y los conocimientos reales demostrados en la ejecución de los trabajos, dará lugar al requerimiento a la adjudicataria de adopción de medidas para su corrección.
- Si la valoración de la calidad de los trabajos del equipo se considera inadecuada, se podrá solicitar la sustitución de parte del equipo de la entidad municipal adherida al presente contrato, con un preaviso de 15 días si existen razones justificadas que así lo aconsejen.
- Si la empresa adjudicataria propusiera el cambio de una persona del equipo designada en la oferta lo comunicará por escrito con 15 días de antelación exponiendo los cambios realizados y adjuntará datos de perfil equivalente que adscribirá para sustitución. Se deberá planificar un tiempo de transferencia de conocimiento suficiente que garantice que la sustitución de la persona no va a producir ninguna dilación ni a perjudicar la ejecución de los trabajos. Esta curva de aprendizaje del proyecto será responsabilidad exclusiva de la empresa adjudicataria.
- La adjudicataria habrá de prever la sustitución en caso de enfermedad, accidente o cualquier otra circunstancia imprevista.
- La empresa adjudicataria se responsabilizará de la transmisión interna de conocimiento del proyecto de tal manera que cualquier situación (sustitución, vacaciones, enfermedad, accidente, o cualquier otra circunstancia) no conlleve demora o paralización del proyecto. Esta transmisión de conocimiento del proyecto será responsabilidad exclusiva de la empresa adjudicataria.

Los medios humanos aportados por la adjudicataria para la ejecución del contrato estarán sometidos al poder de dirección y organización de la adjudicataria en todo ámbito y orden legalmente establecido; será por tanto la adjudicataria el único responsable de dicho personal,

no teniendo por tanto, vinculación jurídico-laboral alguna con el Ayuntamiento de Bilbao ni con las entidades municipales adheridas al presente contrato. Todo ello con independencia del control de la ejecución del contrato que corresponda.

El cumplimiento de lo previsto en esta cláusula **así como de los compromisos contenidos en su oferta respecto al equipo humano** se considera **obligación contractual esencial** de forma que su incumplimiento por parte del contratista podrá ser causa de resolución del contrato.

4.4. PLANIFICACIÓN Y GESTIÓN DEL PROYECTO

4.4.1. COMITÉ PARA COORDINACIÓN/ DIRECCIÓN DEL CONTRATO/ PROYECTO

Se formará un **Comité para la coordinación y dirección del contrato/proyecto por cada entidad municipal adherida**, que estará compuesto por las personas responsables de la entidad municipal adherida al presente contrato, Ayuntamiento de Bilbao, BILBAOTIK S.A., una persona de la adjudicataria y cuantas otras personas designen las partes. Las tareas del Comité para la coordinación y dirección del contrato/proyecto, son entre otras:

- Seguimiento y coordinación del proyecto.
- Control y gestión de riesgos.

4.4.2. IDENTIFICACIÓN Y GESTIÓN DE ACCIONES CORRECTORAS FRENTE A RIESGOS IDENTIFICADOS

- Control y gestión de cambios en el alcance o en la planificación.
- Gestión de recursos.
- Gestión del cambio.
- Gestión de la documentación.
- Adecuada transferencia del conocimiento.

Asimismo, cada entidad municipal adherida al presente contrato, designará la persona/s que desempeñará/n la **Dirección del Proyecto** que se encargará de la planificación, seguimiento y control de los trabajos a realizar y una **Subdirección del Proyecto** que apoyará en la realización de dichas funciones. Asimismo, por parte de BILBAOTIK S.A. se designará una **Subdirección Técnica del Proyecto** (integrada como mínimo por dos personas) que realizará el seguimiento, control y validación de los trabajos tecnológicos.

4.4.3. PLANIFICACIÓN

La empresa adjudicataria deberán describir los aspectos de **planificación del proyecto por cada una de las entidades municipales adheridas al presente contrato**, incluyendo de la forma más detallada posible el **calendario** previsto para el desarrollo de éste, los plazos parciales y totales comprometidos, así como los de la ejecución para cada uno de los conjuntos de trabajos en los que el mismo se descomponga. Cumpliendo la planificación del proyecto e hitos definidos en el presente documento y desarrollado en este punto, la empresa adjudicataria tiene que entregar el plan de proyecto estableciendo los hitos principales del proyecto, definiendo y concretando cualquier aspecto del alcance del mismo. En él se identificarán:

- Descripción de los trabajos y tareas a realizar, sus dependencias, sus hitos, indicadores y entregables resultantes
- Interlocutores necesarios para cada tarea, así como la identificación de la información y/o documentación a recopilar, elaborar y/o revisar.
- Asignación de las personas responsables de la ejecución.
- Metodologías a aplicar.
- Detalle de jornadas.
- Etc...

Dentro de la planificación, para un periodo máximo de DOS AÑOS desde la formalización del contrato, se han de cumplir los siguientes hitos más relevantes, en cada una de las entidades municipales adheridas al presente contrato:

- Revisar el Marco Normativo y la Implantación de la seguridad.
- Aprobar el Sistema de Gestión de Seguridad de la información y revisión continua.
- Cumplimiento del Esquema Nacional de Seguridad (ENS) y al NIS2.
- Definir indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad y actualización mensual de los mismos.
- Despliegue de herramientas para mejorar cumplimiento normativo.
- Plan de Gestión del cambio.
- Elaborar Plan de Adecuación al ENS.
- Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.
- Sensibilización, Concienciación y Formación de toda la Plantilla Municipal.
- Definir Métricas e Indicadores del Estado de la Seguridad y reportar a las autoridades pertinentes
- Auditoría Interna en ENS.
- Revisión continua del Sistema de Gestión de Seguridad.
- Elaboración del Plan de convergencia para el cumplimiento de lo dispuesto en NIS2.
- Realización de ejercicios de hacking ético.
- Coordinación con la DPO municipal.
- Vigilancia y Mejora continua
- Hacking ético.

- Modelo de seguimiento y evaluación a realizar durante el proyecto.
- Acompañamiento presencial durante todo el proceso de auditoría externa de certificación en ENS.
- Acompañamiento y asesoramiento durante todo el proceso hasta obtener la certificación en el Esquema Nacional de Seguridad.

La planificación trimestral del cumplimiento de estos hitos anteriores en cada entidad municipal adherida en el presente contrato, serán los siguientes:

1.- Hitos que se ejecutarán de forma Continua:

- Actualización mensual de los indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad.
- Revisar el Marco Normativo y la Implantación de la seguridad.
- Revisión continua del Sistema de Gestión de Seguridad de la información
- Sensibilización, Concienciación y Formación Continua de toda la Plantilla de cada entidad municipal adherida en el presente contrato.
- Reportar a las autoridades pertinentes cuando proceda, la información asociada a las Métricas e Indicadores del Estado de la Seguridad.
- Coordinación con la DPO municipal.
- Seguimiento y evaluación a realizar durante el proyecto según el modelo definido.
- Acompañamiento y asesoramiento durante todo el proceso hasta obtener la certificación en el Esquema Nacional de Seguridad.

2.-Hitos a ejecutar en cada Trimestre:

Primer Trimestre:

- Revisión de la Política de Seguridad Municipal y revisión de la Normativa de Seguridad que desarrolla la Política de Seguridad.
- Elaborar un informe de la situación actual de seguridad “análisis diferencial o gap análisis”: estado inicial de cada una de las entidades municipales adheridas al presente contrato, en relación con la seguridad y grado de cumplimiento de normativas y procedimientos de seguridad existentes que recoja las conclusiones del análisis inicial.
- Informe del resultado del Análisis de Riesgos.
- Declaración de aplicabilidad que incluya la relación de medidas de seguridad seleccionadas.
- Elaborar Plan de Adecuación al Esquema Nacional de Seguridad.
- Elaboración del Plan de convergencia para el cumplimiento de lo dispuesto en NIS2.
- Plan de Mejora de la Seguridad conforme a lo establecido en el RD 311/2022 que detallará las acciones que es necesario emprender para implementar las medidas de

seguridad necesarias para adecuar el sistema del ENS y mitigar los riesgos identificados del análisis. Incluir las medidas de seguridad necesarias para el cumplimiento del NIS2.

- Definir indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad y actualización mensual de los mismos.
- Aprobar el Sistema de Gestión de Seguridad de la información y revisión continua.
- Definir Métricas e Indicadores del Estado de la Seguridad y reportar a las autoridades pertinentes.
- Modelo de seguimiento y evaluación a realizar durante el proyecto.

Segundo Trimestre:

- Despliegue de herramientas para mejorar cumplimiento normativo.
- 50% Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.

Tercer Trimestre:

- 50% Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.
- Plan de Gestión del cambio.
- Sensibilización, Concienciación y Formación de toda la Plantilla Municipal.

Cuarto Trimestre:

- Realización de ejercicios de hacking ético.
- Auditoría Interna en ENS.
- Informe de Auditoría Interna de ENS.

Quinto y Sexto Trimestre

- Acompañamiento presencial durante todo el proceso de auditoría externa de certificación en ENS.
- Definición del PAC Plan de Actuaciones Correctivas.

Séptimo y Octavo trimestre

- Obtención de la Certificación del ENS por parte del Ayuntamiento de Bilbao en el alcance que se defina en el presente contrato

Una vez formalizado el contrato, y en el plazo máximo de siete (7) días naturales, se revisará el plan propuesto y el/la Responsable del proyecto de cada entidad municipal adherida al presente contrato, con la colaboración de los demás miembros del equipo de proyecto, validará el plan de trabajo definitivo, que se registrará en el Acta de Inicio del contrato. Este plan de trabajo

deberá mantenerse actualizado y consensado entre cada una de las entidades municipales adheridas al contrato, Ayuntamiento de Bilbao, BILBAOTIK S.A. y la empresa adjudicataria.

4.4.4. CALIDAD, SEGUIMIENTO Y CONTROL DE LOS TRABAJOS

La empresa adjudicataria debe establecer todos aquellos procedimientos de control que permita verificar de forma continuada el cumplimiento de los objetivos especificados, tanto en los plazos como en la calidad final en cada una de las entidades municipales adheridas al presente contrato.

Durante la ejecución del trabajo, se presentará un informe de las horas (unidades y %) imputadas a cada perfil profesional que se ejecuten cada mes, por cada una de las entidades municipales adheridas al presente contrato.

La empresa adjudicataria deberá nombrar un/a Director/a del proyecto en cada entidad municipal adherida al presente contrato que será el responsable de los trabajos en todos sus aspectos. Esta persona será la encargada de convocar las reuniones de seguimiento, realizar informes de seguimiento para la adecuada evaluación y mejora continua y cuantas reuniones estime oportuno para el correcto desarrollo de los trabajos.

Como mínimo, se realizarán las siguientes actividades de seguimiento y control de los trabajos:

- Se realizará una primera reunión de lanzamiento en cada una de las entidades municipales adheridas al presente contrato, al inicio del proyecto; en ella intervendrán los interlocutores que designe cada entidad municipal adherida al presente contrato, Ayuntamiento de Bilbao, BILBAOTIK S.A. así como las personas designadas por parte de la empresa adjudicataria. Su objetivo es establecer las principales líneas del proyecto.
- Semanalmente, se realizará una reunión de seguimiento en cada entidad municipal adherida al presente contrato. Por cada reunión de seguimiento, la empresa adjudicataria hará un resumen de los trabajos realizados desde la última reunión de seguimiento y elaborará su correspondiente acta, que deberá ser visada por los asistentes a la misma. Previamente al visado del acta, cada entidad municipal adherida, Ayuntamiento de Bilbao, BILBAOTIK S.A. revisarán los trabajos ya realizados y comprobarán si se corresponden con las tareas planificadas en su momento. Todas aquellas tareas que estime interesantes la empresa adjudicataria y que pretenda llevar a cabo durante esa semana, serán propuestas a cada entidad municipal adherida, Ayuntamiento de Bilbao, BILBAOTIK S.A. para su aceptación o rechazo.
- Para el seguimiento de los trabajos será necesario entregar un informe con la evolución de los trabajos. Tras la revisión, el/la Responsable del Contrato o el/la Director del Proyecto nombrado por cada una de las entidades municipales adheridas, comunicará a la empresa adjudicataria su aprobación o en su caso, el rechazo total o parcial, en su caso, de los trabajos realizados, en la medida que no respondan a lo acordado, o no superen los controles de calidad.

Inicialmente se estima un informe cada mes.

En caso de detectarse desviaciones entre la planificación y la situación real del trabajo desarrollado, la empresa adjudicataria deberá emprender las acciones correctivas apropiadas, tras ser consensuadas con cada entidad municipal adherida, Ayuntamiento de Bilbao y BILBAOTIK S.A.

- A petición de cualquiera de las partes, se celebrarán reuniones extraordinarias, con el objetivo de subsanar cualquier incidencia grave que requiera una respuesta inmediata y no pueda esperar a la reunión de seguimiento.
- En la reunión de cierre, que es la última reunión del proyecto, para dar por finalizado el contrato, deberá validarse por cada entidad municipal adherida, Ayuntamiento de Bilbao, el Acta de Recepción o Cierre tras la validación técnica de BILBAOTIK S.A., por el que se dará el Vº Bº a los trabajos realizados.
- Ni las entidades municipales adheridas ni el Ayuntamiento de Bilbao, tendrán responsabilidad directa, solidaria, ni subsidiaria respecto al cumplimiento de las obligaciones laborales de la empresa adjudicataria, así como tampoco de las que se puedan derivar, en su caso, de la extinción de los contratos de trabajo, tanto durante la vigencia del presente contrato, como con posterioridad a su terminación, asumiendo la empresa adjudicataria la totalidad de las consecuencias jurídico laborales derivadas de los mismos.
- Las entidades municipales adheridas, el Ayuntamiento de Bilbao y/o BILBAOTIK S.A. no tendrán ninguna facultad organizativa ni de dirección respecto a las personas que presten sus servicios para la empresa adjudicataria, ni existirá relación jurídico laboral, civil o administrativa alguna con las mismas.

4.4.5. DOCUMENTACIÓN A ENTREGAR

La documentación generada durante la ejecución del contrato será propiedad exclusiva de cada entidad municipal adherida, sin que la adjudicataria pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de cada entidad municipal adherida, que la facilitaría, en su caso, previa petición formal de la adjudicataria con expresión del fin.

La documentación se entregará en soporte electrónico de forma que cada entidad municipal adherida, pueda efectuar el mantenimiento de la misma posteriormente.

La adjudicataria será responsable de mantener actualizada la documentación del contrato a lo largo del mismo. Asimismo, deberá mantener un registro histórico de los cambios producidos en la documentación con una breve explicación de la causa que originó los mismos.

4.5. CONTEXTO DEL ENTORNO TECNOLÓGICO E INFRAESTRUCTURA TECNOLÓGICA MUNICIPAL

A aquellas empresas que tengan interés en la presentación de la Oferta, previa petición identificándose la empresa, se les facilitará información sobre el contexto de la Infraestructura

Tecnológica Municipal actualmente existente en el entorno municipal. Dicha petición se ha de dirigir al correo modernizazioa@bilbao.eus

4.6. PRESUPUESTO

El presupuesto de las entidades municipales adheridas al presente contrato de la parte 2: “Certificación ENS de las entidades municipales adheridas”, está definido en la Carátula de Cláusulas Administrativas de este Pliego es un presupuesto máximo asociado a los servicios contratados.

Las entidades municipales adheridas al presente contrato dispondrán de un presupuesto individualizado máximo plurianual para cada entidad municipal, para DOS AÑOS:

- Bilbao Musika, O.A.L.: 14.400 euros + IVA
- Bilbao Zerbitzuak – Servicios, EPEL
- Centro Azkuna de Sociedad y Cultura Contemporánea S.A.: 14.400 euros + IVA
- Funicular de Artxanda, S.A.: 10.800 euros + IVA
- C.A.C. Teatro Arriaga, S.A.: 10.800 euros + IVA

El importe total del contrato de la parte 2: “Certificación ENS de las entidades municipales adheridas” de cada una de las entidades municipales adheridas, se realizarán **pagos trimestrales** asociados al cumplimiento de los Hitos Planificados según el Calendario de Planificación del Proyecto por cada entidad municipal adherida, previa validación por parte de cada entidad municipal adherida, Ayuntamiento de Bilbao y BilbaoTIK; así pues se abonarán los siguientes porcentajes sobre el precio de adjudicación de la parte 2: “Certificación en ENS de las entidades municipales adheridas” asociados al cumplimiento de los hitos:

- 2,81% +IVA/trimestre se abonarán por la ejecución de los hitos que se ejecutarán de forma continua
- 25% + IVA se abonarán en el primer trimestre por la ejecución de los hitos planificados para el primer trimestre
- 12,5% + IVA se abonarán en el segundo trimestre por la ejecución de los hitos planificados para el segundo trimestre.
- 12,5% + IVA se abonarán en el tercer trimestre por la ejecución de los hitos planificados para el tercer trimestre.
- 14,5% + IVA se abonarán en el cuarto trimestre por la ejecución de los hitos planificados para el cuarto trimestre
- 3,02% + IVA se abonarán en el quinto y sexto trimestre por la ejecución de los hitos planificados para el quinto y sexto trimestre.
- 10% + IVA se abonarán en el momento que se haya obtenido la Certificación del Esquema de Seguridad Nacional por parte de cada una de las entidades municipales adheridas.

Por cada trimestre, se abonará el % de los hitos planificados ejecutados definidos anteriormente sobre el precio de adjudicación del contrato de la parte 2: “Certificación en ENS de las entidades municipales adheridas”, abonándose el sumatorio de los hitos ejecutados, en función del % designado a cada hito:

1.- Importe de pago de Hitos a ejecutar de forma continua:

- 20%: Actualización mensual de los indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad.
- 10%: Revisar el Marco Normativo y la Implantación de la seguridad.
- 10%: Revisión continua del Sistema de Gestión de Seguridad de la información
- 10%: Sensibilización, Concienciación y Formación Continua de toda la Plantilla Municipal (el foco principal ha de ser en el tercer y cuarto trimestre).
- 4%: Reportar a las autoridades pertinentes cuando proceda, la información asociada a las Métricas e Indicadores del Estado de la Seguridad.
- 6%: Coordinación con la DPO municipal.
- 20%: Seguimiento y evaluación a realizar durante el proyecto según el modelo definido.
- 20%: Acompañamiento y asesoramiento durante todo el proceso hasta obtener la certificación en el Esquema Nacional de Seguridad.

2.-Importe de pago de Hitos a ejecutar en cada trimestre:

Primer Trimestre:

- 10%: Revisión de la Política de Seguridad Municipal y revisión de la Normativa de Seguridad que desarrolla la Política de Seguridad.
- 15%: Elaborar un informe de la situación actual de seguridad “análisis diferencial o gap análisis”: estado inicial de cada entidad municipal adherida en relación con la seguridad y grado de cumplimiento de normativas y procedimientos de seguridad existentes que recoja las conclusiones del análisis inicial.
- 10%: Informe del resultado del Análisis de Riesgos.
- 4%: Declaración de aplicabilidad que incluya la relación de medidas de seguridad seleccionadas.
- 25%: Elaborar Plan de Adecuación al Esquema Nacional de Seguridad.
- 10%: Elaboración del Plan de convergencia para el cumplimiento de lo dispuesto en NIS2.
- 10%: Plan de Mejora de la Seguridad conforme a lo establecido en el RD 311/2022 que detallará las acciones que es necesario emprender para implementar las medidas de seguridad necesarias para adecuar el sistema del ENS y mitigar los riesgos identificados del análisis. Incluir las medidas de seguridad necesarias para el cumplimiento del NIS2.
- 4%: Definir indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad y actualización mensual de los mismos.
- 3%: Aprobar el Sistema de Gestión de Seguridad de la información y revisión continua.
- 4%: Definir Métricas e Indicadores del Estado de la Seguridad y reportar a las autoridades pertinentes.

- 5%: Modelo de seguimiento y evaluación a realizar durante el proyecto.

Segundo Trimestre:

- 30%: Despliegue de herramientas para mejorar cumplimiento normativo.
- 70%: 50% Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.

Tercer Trimestre:

- 60%: 50% Implantación de la Seguridad: Definir Hoja de ruta: documentos a elaborar, medidas técnicas a implementar y definir las prioridades.
- 10%: Plan de Gestión del cambio.
- 30%: Sensibilización, Concienciación y Formación de toda la Plantilla Municipal.

Cuarto Trimestre:

- 30%: Realización de ejercicios de hacking ético.
- 30%: Auditoría Interna en ENS.
- 40%: Informe de Auditoría Interna de ENS.

Quinto y Sexto Trimestre:

- 50%: acompañamiento presencial durante todo el proceso de auditoría externa de certificación en ENS.
- 50%: Definición del PAC Plan de Actuaciones Correctivas.

Séptimo y Octavo trimestre

- 100%: Obtención de la Certificación del ENS por parte de cada una de las entidades municipales adheridas.

4.7. PROTECCIÓN DE DATOS

Los datos recibidos deberán cumplir con los requisitos legales actualmente establecidos para la protección de datos personales según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4.8. SEGURIDAD DE LA INFORMACIÓN

Se requiere que la empresa adjudicataria disponga del Certificado de conformidad con el Esquema Nacional de Seguridad categoría alta: Las medidas de seguridad a aplicar en los servicios objeto de este contrato y en los posibles sistemas de información desarrollados/desplegados/mantenidos serán las que correspondan del Anexo II del ENS, para la categoría ALTA .

Se requiere que la empresa adjudicataria disponga del certificado ISO 27.001, norma internacional para la gestión de la seguridad de la información.

Ayuntamiento de Bilbao / Área de Cultura y Gobernanza	BILBAOTIK S.A.
ANE MIREN IBAÑEZ ZUGAZAGA - 14259729M Firmado digitalmente por ANE MIREN IBAÑEZ ZUGAZAGA - 14259729M Fecha: 2026.08.07 10:47:54 +02'00' Firmado digitalmente por ROSA ANA YURREBASO SESTAFE - 30596010F Nombre de reconocimiento (DN): c=ES, o=Ayuntamiento de Bilbao - Bilboko Udala, ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO, cn=ROSA ANA YURREBASO SESTAFE - 30596010F, givenName=ROSA ANA, sn=YURREBASO SESTAFE, serialNumber=IDCES-30596010F Fecha: 2026.08.10 08:10:15 +02'00'	Firmado digitalmente por ENRIQUE PASCUAL ANCHIA - 30601196H Fecha: 2026.08.07 11:22:21 +02'00' JOSE MANUEL MATO FERNANDEZ - 72396594T 2026.08.07 11:57:40 +02'00' Firmado digitalmente por MANUEL ROIBAL PRIETO - 22738555L Fecha: 2026.08.07 12:09:16 +02'00' AITOR LETE FANO - 14598192T Firmado digitalmente por AITOR LETE FANO - 14598192T Fecha: 2026.08.07 12:12:42 +02'00'

Dirección de Modernización/ Subdirección de Servicios Generales de Alcaldía	Dirección General / Subdirección de Transformación Digital, Subdirector de Smart Data y Servicios Corporativos y Dirección de Infraestructuras y Ciberseguridad