SOCIEDAD MUNICIPAL AGUAS DE BURGOS S.A.

Expediente de contratación nº 029/2024

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR LA CONTRATACIÓN DEL QUE HA DE REGIR LA CONTRATACIÓN DEL **SERVICIO DE GESTIÓN INTEGRAL Y SUMINISTROS HARDWARE VINCULADOS A LA CIBERSEGURIDAD, PARA LA SOCIEDAD MUNICIPAL AGUAS DE BURGOS S.A.**, MEDIANTE PROCEDIMIENTO ABIERTO, CON PLURALIDAD DE CRITERIOS**, FINANCIADO POR LOS FONDOS NEXT GENERATION-EU A TRAVÉS DEL PLAN DE RECUPERACIÓN TRANSFORMACIÓN Y RESILIENCIA(PRTR).**

Burgos, agosto de 2024

Contenido

1. Introducción

La Sociedad Municipal Aguas de Burgos S.A. (en adelante Aguas de Burgos), ha incluido la prestación objeto de este contrato dentro del proyecto denominado "DIGITAGUABUR", que ha sido incluido como beneficiario de financiación europea de la Orden TED/934/2022 de 23 de septiembre, por la que se aprueban las bases reguladoras de la concesión de ayudas por concurrencia competitiva para la elaboración de proyectos de mejora de la eficiencia del ciclo urbano del agua y la primera convocatoria de subvenciones (2022) en concurrencia competitiva de proyectos de mejora de la eficiencia del ciclo urbano del agua (PERTE digitalización del ciclo del agua), en el marco del Plan de Recuperación, Transformación y Resiliencia, Componente 5 "Preservación del espacio litoral y los recursos hídricos", inversión 1 (C5.I1 Materialización de las actuaciones de depuración, saneamiento, eficiencia, ahorro, reutilización y seguridad de infraestructuras (DSEAR) y Objetivo CID/OA número 76, e Inversión 3 [«Transición digital en el sector del agua ("Enforcement Digital Medioambiental")»] del Plan de Recuperación, Transformación y Resiliencia con el objetivo de obtener mejoras en el funcionamiento de las infraestructuras de tratamiento de aguas residuales así como mejorar el cumplimiento de los criterios de eficiencia energética o mejorar la eficiencia y reducir las pérdidas de agua en los sistemas de distribución de agua.

Entre las actuaciones del proyecto se encuentra las actuaciones:

- A4. PLAN DIRECTOR DE SEGURIDAD INTEGRAL (GESTIONAR E INTEGRAR LA SEGURIDAD FÍSICA, LÓGICA Y DE LAS PERSONAS)
- A12. CIBERSEGURIDAD

entre cuyos objetivos se encuentra el análisis de riegos, la reducción del riesgo de interrupción de las operaciones por ataques malintencionados o por causas accidentales, la aplicación Esquema Nacional de Seguridad (ENS) y RGPD, y la implantación de software de ciberseguridad.

Aguas de Burgos ha efectuado un diagnóstico de ciberseguridad el cual ha proporcionado un conjunto de recomendaciones de implantación (Plan de Acciones de Mejora) que se han agrupado como diferentes pasos consecutivos a llevar a cabo por Aguas de Burgos para potenciar las capacidades de resiliencia, protección y defensa de Aguas de Burgos frente al creciente número y sofisticación de las amenazas provenientes del ciberespacio a fin de:

- Conseguir que el análisis de riesgos forme parte de la cultura de Aguas de Burgos y que se considere el tratamiento de riesgos como parte del quehacer diario.
- Reducir el riesgo de interrupción de las operaciones de Aguas de Burgos por ataques malintencionados o por causas accidentales, limitar su impacto potencial y reforzar la capacidad de resiliencia y recuperación en caso de verse

afectada.

- Garantizar la autenticidad, confidencialidad, integridad, disponibilidad, auditoría y privacidad de la información, tanto aquella generada por la actividad propia, como la recibida en custodia por parte de ciudadanos, empleados y terceras partes.

- Asegurar el cumplimiento de las obligaciones legales de la compañía en materia de seguridad física, seguridad de la información y ciberseguridad.

Todas estas actuaciones se abordarán en cuatro líneas estratégicas:

1. Desarrollo y adecuación del modelo de gobierno (marco organizativo y cuerpo normativo) de Aguas de Burgos para adecuarlo a los riesgos a los que se enfrenta.

2. Refuerzo de la concienciación y potenciación de las capacidades de los empleados y colaboradores externos en materia de seguridad integral.

3. Mejora y modernización de los actuales sistemas de seguridad, para garantizar que son toman las medidas de protección adecuadas.

4. Despliegue de nuevas herramientas técnicas de prevención, protección y recuperación y/o mejora de las ya existentes.

2. Objeto y alcance

El objeto del contrato es la mejora del control y de la seguridad de la infraestructura IT/OT (*Information Technology / Operational Technology*), la implantación de una Oficina Técnica de Seguridad Integral (OTSI), la implantación de herramientas del Centro Criptológico Nacional (CCN-CERT), la implantación de un Centro de Operaciones de Seguridad (SOC), junto con el hardware y software necesario, y el posterior soporte, operación, vigilancia y gestión de incidentes a través de la OTSI y el SOC.

Para alcanzar estos objetivos es necesario que todas las actuaciones que se emprendan sean llevadas a cabo con un enfoque integrador y coordinadas por un único responsable de la ejecución de todos los trabajos, que garantice el cumplimiento de los hitos del proyecto y la calidad y coherencia de los trabajos.

El presente pliego hace referencia a las siguientes actuaciones del proyecto “DIGITAGUABUR” A07, A08, A10, A11, enmarcadas en el Componente 5 del PRTR, Inversión 1; Submedida 1.a “Actuaciones de depuración, saneamiento y reutilización del agua”; y Submedida 1.b “Actuaciones para la mejora de la eficiencia y reducción de pérdidas en el uso del agua”.

Componente	Inversión	Tipología de actuación	Código Actuación objeto de la licitación	Submedida
5	1	B2 B3 B4 C	A07 A08 A10 A11	1.a 1.b

En relación a la consecución de Hitos y Objetivos (Hyo) a través de esta contratación se deberá contribuir a la consecución del Objetivo 76, 427 y 428 del Componente 5 Inversión 1, establecidos en la Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del Plan de Recuperación Transformación y Resiliencia, PRTR, (documento CID, en sus siglas en inglés), y recogidos en el Acuerdo de la Conferencia Sectorial de Turismo de 21 de diciembre de 2021 y 29 de marzo de 2022, y lo establecido en el art. 3 de la Orden HFP/1030/2021 de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.

Será el Ministerio para la Transición Ecológica y Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente, el órgano responsable en la gestión, el seguimiento de los hitos y objetivos, la rendición de cuentas en relación con su cumplimiento y la información a proporcionar al sistema de gestión, así como el cumplimiento de todos los requerimientos establecidos que derivan de la normativa aplicable asumiendo y siguiendo el régimen jurídico que les resulta de aplicación con carácter general a los mismos, conforme a lo establecido en el artículo 13.6 del Real Decreto 690/2021, de 3 de agosto.

2.1. Necesidad a satisfacer

Ante la necesidad de evitar ataques y crisis en el suministro de agua que comprometan el funcionamiento de los servicios de Ciclo Integral del Agua, y en línea con las actuales directrices de seguridad para la gestión del riesgo, y considerando que su interacción en la cadena de suministro de entidades públicas y privadas de carácter comercial e industrial forma una parte muy importante del tejido empresarial de la provincia de Burgos y, por ende, de la Comunidad Autónoma de Castilla y León, desde Aguas de Burgos se plantea el desarrollo de conjunto de actuaciones que permitan potenciar las capacidades de resiliencia, protección y defensa de Aguas de Burgos frente al creciente número y sofisticación de las amenazas provenientes del ciberespacio.

Por lo tanto, es necesario disponer como proveedor de servicio con una empresa especialista en Seguridad de la Información y en Seguridad Gestionada, que posea un

SOC adherido a la Red Nacional de SOC del CCN-CERT, y un equipo de personas especializadas y con capacidad suficiente para afrontar tanto los dominios que componen la seguridad de la información como el amplio abanico de las tareas de ciberseguridad industrial que los forman, tanto a nivel operativo y jurídico como técnico, por lo que deberá tener una visión global que permita la prestación de un servicio de seguridad integral a Aguas de Burgos.

2.2. Infraestructura IT/OT

La información de detalle sobre las infraestructuras de las redes IT y OT se considera confidencial por razones de seguridad. Los licitadores podrán solicitar a Aguas de Burgos dicha información bajo el siguiente procedimiento.

- El licitador que vaya a presentarse al concurso y requiera la información, la solicitará a Aguas de Burgos por medio del canal establecido para las dudas, antes de los 6 días anteriores para la finalización del plazo de presentación de ofertas.
- Aguas de Burgos le envía el acuerdo de confidencialidad por correo electrónico.
- El licitador que desea la información adicional devuelve firmado el acuerdo digitalmente con un certificado válido.
- Aguas de Burgos suministra la información solicitada. Esta información podrá ser suministrada por escrito o citando a los representantes de las empresas en las oficinas de Aguas de Burgos, donde se les darán las explicaciones necesarias.

Siendo la herramienta GLORIA del CCN-CERT la base sobre la que pivotarán gran parte de las actuaciones del pliego, y siendo la certificación en dicha herramienta un requisito de solvencia de obligatorio cumplimiento según se establece en el PCA, la información adicional solo se suministrará a aquellas empresas que aparezcan como certificadas en GLORIA en el portal oficial del CCN-CERT.

No obstante, con el objetivo de que los ofertantes puedan hacer una estimación de la infraestructura IT/OT, se proporcionan los siguientes datos orientativos:

- 40 estaciones de trabajo.
- 20 ordenadores portátiles.
- 60 dispositivos móviles (móviles y tabletas).
- Infraestructura IT. Activos y sistemas información on-premise y cloud.
- Infraestructura OT. Activos y sistemas de control industrial en ETAP, EDAR, depósitos, redes de abastecimiento y saneamiento.

- Redes de comunicaciones propias.

3. Códigos CPV

A los efectos de la nomenclatura del Vocabulario Común de Contratos (CPV) de la Comisión Europea la codificación correspondiente es:

- 30200000-1 Equipo y material informático
- 48730000-4 Paquetes de software de seguridad
- 72000000-5 Servicios IT: consultoría, desarrollo de software, Internet y apoyo.
- 72514000-1 Servicios de gestión de instalaciones informáticas

4. Normativa de aplicación

A los productos y servicios objeto de este pliego les será de aplicación la normativa que esté en vigor en cada momento, que con carácter no exhaustivo ni excluyente se relaciona a continuación:

- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.
- Plan Nacional de Protección de Infraestructuras Críticas (PNPIC), aprobado mediante Instrucción núm. 1/2016, de la Secretaría de Estado de Seguridad.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril del 2016 (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección

de Datos Personales y Garantía de los Derechos Digitales.

- Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.
- Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2), 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).
- Cyber Resilience Act. Propuesta de Reglamento del 15 de septiembre de 2022 de la Comisión Europea sobre los requisitos de ciberseguridad de los productos con elementos digitales, conocida como la Ley de Ciberresiliencia, refuerza las normas de ciberseguridad para garantizar unos productos de hardware y software más seguros.
- Normativa IEC 62443. Marco integral para la seguridad de los sistemas de automatización y control industrial.

Por otro lado, se seguirá lo establecido en la siguiente normativa, y de conformidad con lo previsto en el artículo 6 de la Ley 38/2003, de 17 de noviembre:

- Ley 38/2003, de 17 de noviembre, General de Subvenciones, y el Real Decreto 887/2006, de 21 de julio, por el que se aprueba el Reglamento que la desarrolla.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, en caso de que en la ejecución de las subvenciones se celebren contratos que deban someterse a esta ley.
- Real Decreto-ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia.
- Reglamento (UE) 2020/852 del Parlamento Europeo y del Consejo, de 18 de junio de 2020, relativo al establecimiento de un marco para facilitar las inversiones sostenibles, en cuanto que todas las actuaciones que se ejecuten dentro del Plan Nacional de Recuperación, Transformación y Resiliencia (PRTR)

deben cumplir el principio de no causar un perjuicio significativo a los objetivos medioambientales recogidos en el artículo 17 del citado Reglamento, y por el que se modifica el Reglamento (UE) 2019/2088..

- Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia.
- Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del Plan de Recuperación, Transformación y Resiliencia, PRTR.
- Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.
- Orden HFP/1031/2021, de 29 de septiembre, por la que se establece el procedimiento y formato de la información a proporcionar por las Entidades del Sector Público Estatal, Autonómico y Local para el seguimiento del cumplimiento de hitos y objetivos y de ejecución presupuestaria y contable de las medidas de los componentes del Plan de Recuperación, Transformación y Resiliencia.
- Orden TED/423/2022, de 10 de mayo, sobre delegación de competencias en la ejecución de los fondos del Plan de Recuperación, Transformación y Resiliencia transferidos al Fondo de Restauración Ecológica y Resiliencia.
- Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia.
- La Adenda al Plan de Recuperación, Transformación y Resiliencia (PRTR), aprobada por el Consejo de Asuntos Económicos y Financieros (ECOFIN) el 17 de octubre de 2023.
- Como documentación de referencia, se tendrá en cuenta, además, el Componente 5: Preservación del litoral y recursos hídricos, del Plan de Recuperación, Transformación y Resiliencia.

5. Descripción de los trabajos a realizar

5.1. Oficina Técnica de Seguridad Integral (OTSI)

Considerando el continuo aumento y complejidad de las amenazas, ataques e incidentes en materia de seguridad física y de calidad del agua, seguridad de la información y ciberseguridad, así como la entrada en vigor de nuevas obligaciones legales relativas a la necesidad de la monitorización continua y comunicación de los incidentes de seguridad, se hace necesario crear la **Oficina Técnica de Seguridad Integral (OTSI)** de Aguas de Burgos que proporcionará servicios de GRC (Gobierno,

Riesgo y Cumplimiento) a fin de agilizar el cumplimiento y adecuación a la normativa vigente (RGPD, ENS, NIS2) como objetivos inmediatos de Aguas de Burgos.

En el caso de la norma NIS2, su entrada en vigor fue el 16 de enero de 2023, y todos los Estados miembros deben adoptar las medidas necesarias para garantizar el cumplimiento de esta directiva antes del 17 de octubre de 2024. La norma NIS2 se encuentra actualmente en fase de trasposición a la regulación española. La trasposición de dicha norma, y dado que Aguas de Burgos pertenece al concepto de entidades esenciales, puede significar que el nivel del ENS que deba adoptar Aguas de Burgos sea el nivel ALTO.

A semejanza de otras infraestructuras críticas del sector de aguas, Aguas de Burgos apuesta por la creación de la Oficina Técnica de Seguridad Integral (OTSI) complementando su actividad con la creación de un Centro de Operaciones de Seguridad (SOC) que asegurará la monitorización 24x7 de sus instalaciones y de las personas, la detección de incidentes de seguridad y el despliegue de una respuesta inmediata en la lucha contra los riesgos especiales, los riesgos tecnológicos y los derivados de actividades de delincuencia común y comportamientos antisociales minimizando sus efectos gracias a la contratación de recursos especializados.

5.1.1 Plan de adecuación al ENS

5.1.1.1 Situación de partida

La situación actual en las siguientes dimensiones del Esquema Nacional de Seguridad (ENS) es la siguiente:

- **Marco organizativo**: El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad. La OTSI será la responsable de definir desde cero la Política de Seguridad de la Información en la que se establecen la organización de la seguridad, las funciones y las responsabilidades, así como procedimientos de respuesta ante incidentes. Desarrollará y elaborará toda la normativa de seguridad, los procedimientos operativos de seguridad y la formalización del proceso de autorización.

- **Marco operacional**: El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin. El nivel de madurez en cuanto a la planificación de la seguridad del análisis de riesgos es INICIAL y no está extendido a todos los sistemas de información de una manera homogénea. El establecimiento del marco operacional incluye:

    - La realización y redefinición de la categorización de sistemas de información, la declaración de aplicabilidad, determinación del nivel de madurez de las medidas y el análisis de riesgos para todos los sistemas.

    - La formalización de una arquitectura de seguridad asociada a los

sistemas de información.

- La formalización de las actividades de continuidad de servicios a través de un Plan de emergencia y continuidad de negocio.
- El establecimiento de un sistema de métricas definido y claro que permita la evaluación periódica de los controles implantados y tener un nivel claro de la seguridad de la organización. La gestión diaria es realizada a través de un servicio de seguridad de la información que realiza tanto el seguimiento de indicadores y de los sistemas de monitorización y reporte ante alertas como centro de respuesta ante incidentes de seguridad.

- **Marco de medidas de protección**: Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad. El nivel de madurez en cuanto a la planificación de la seguridad del análisis de riesgos es INICIAL y no está extendido a todos los sistemas de información de una manera homogénea. El establecimiento del marco operacional incluye:
  - Protección de las Instalaciones e Infraestructuras.
  - Gestión del Personal.
  - Protección de los Equipos.
  - Protección de las Comunicaciones.
  - Protección de los Soportes de Información.
  - Protección de las Aplicaciones Informáticas.
  - Protección de la Información.
  - Protección de los Servicios.

5.1.1.2 Adecuación al ENS

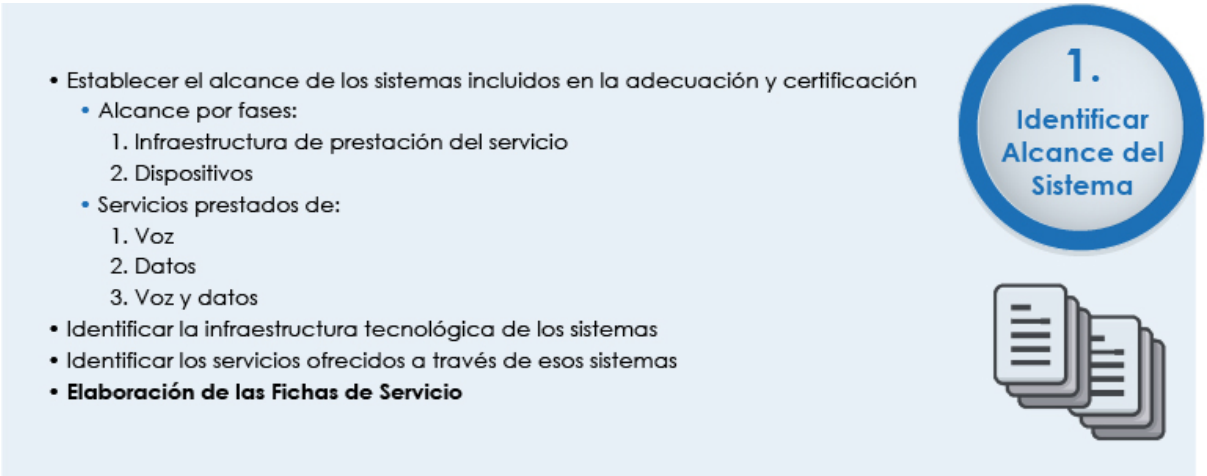
Se considera que el enfoque metodológico más adecuado para llevar a cabo el **Plan de Adecuación al Esquema Nacional de Seguridad** (ENS) es el desarrollado por el Centro Criptológico Nacional (CCN) que define el Plan de Adecuación al ENS como:

"*El Plan de Adecuación es un documento que contendrá 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 se van a implementar (Declaración de Aplicabilidad), qué riesgos se asumen, la Política de Seguridad del Organismo con su organización de la seguridad...*"

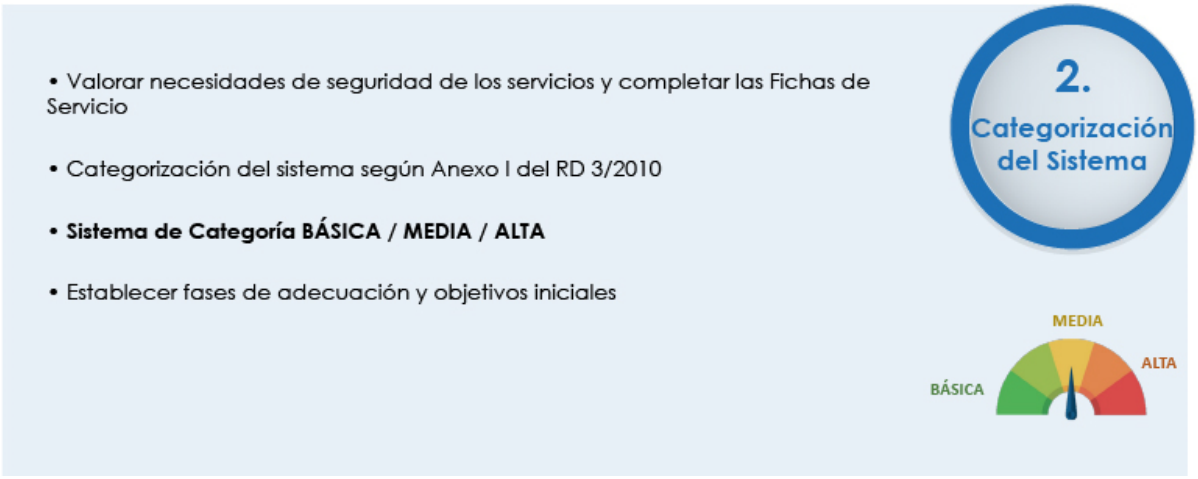
La OTSI será la responsable de la ejecución de todas las tareas necesarias para la

ejecución del Plan de Adecuación de los Sistemas de Información de Aguas de Burgos al ENS, de acuerdo con los pasos definidos por el CCN:

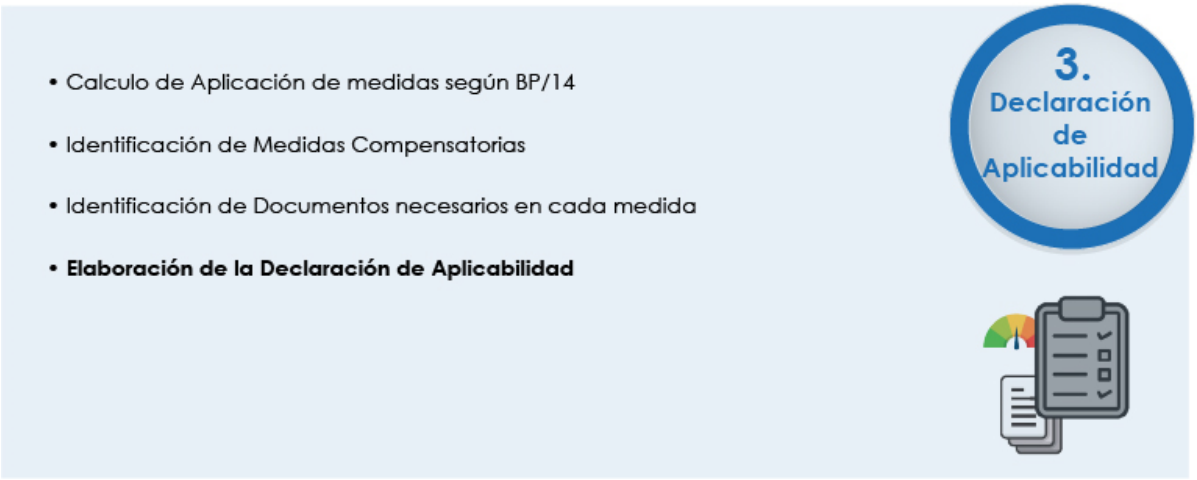
La determinación del Alcance requiere la identificación de los servicios prestados por Aguas de Burgos, así como los sistemas en los que se alojan. Este paso plantea como entregable principal las Fichas de Servicio de Aguas de Burgos.



La Categorización del Sistema se lleva a cabo atendiendo a la valoración de las dimensiones de seguridad de los servicios prestados y de la información que manejan (teniendo en cuenta si incluyen datos de carácter personal). Este paso plantea como entregable principal Sistema de Categoría BÁSICA/MEDIA/ALTA.

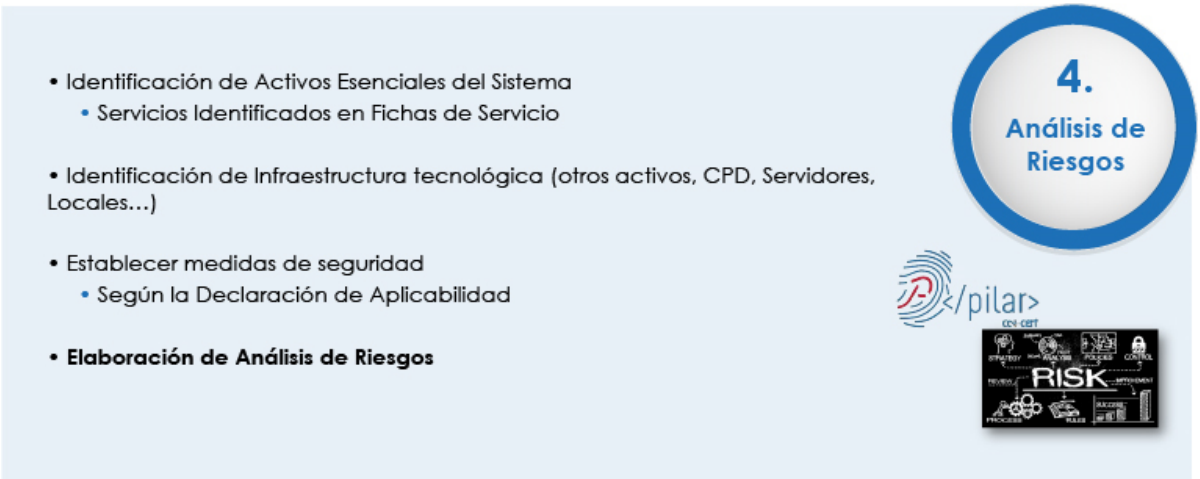


La obtención de la Declaración de Aplicabilidad provisional permite tener una primera versión de la Declaración de Aplicabilidad. Este paso plantea como entregable principal la Declaración de Aplicabilidad de Aguas de Burgos.

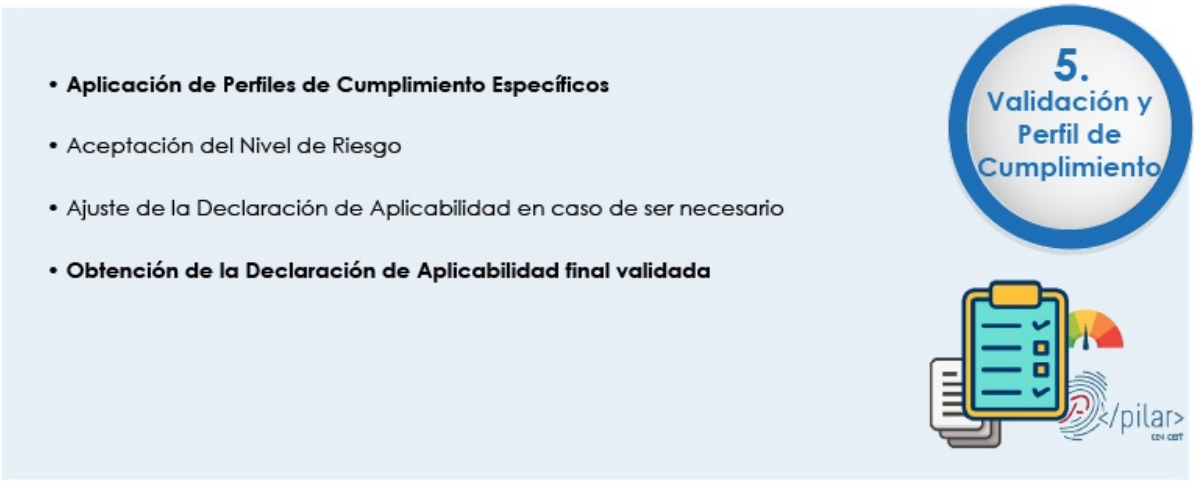


La realización del Análisis de Riesgos debe incluir la valoración de las medidas de seguridad definidas en la Declaración de Aplicabilidad. Este paso plantea como entregable principal el Análisis de Riesgos de Aguas de Burgos.

El Análisis de Riesgos se llevará a cabo mediante la herramienta PILAR.

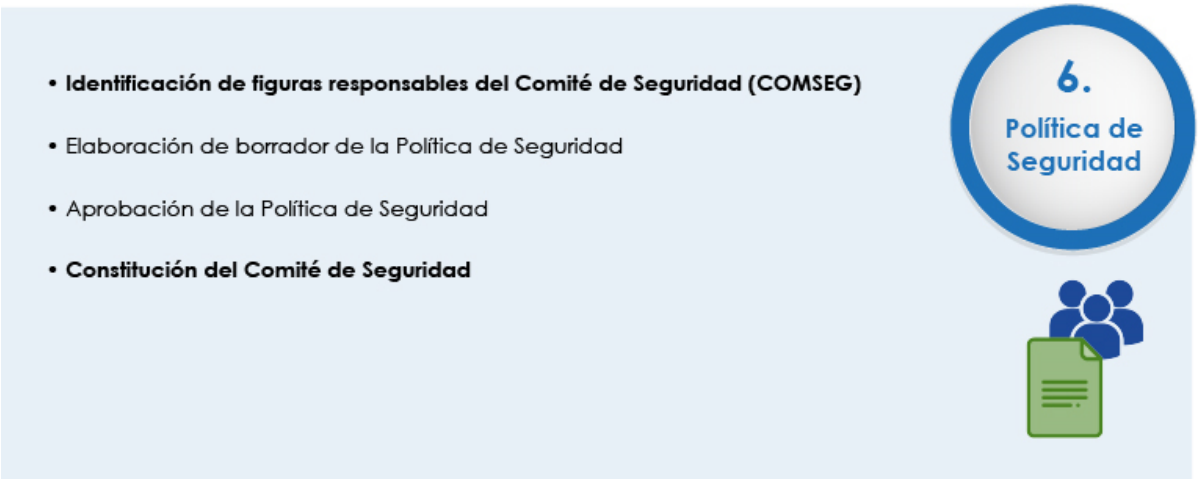


La validación de la Declaración de Aplicabilidad definitiva o Perfil de Cumplimiento específico se apoya en la aceptación del Riesgo residual. Este paso plantea como entregable principal la Declaración de Aplicación final validada de Aguas de Burgos.



La preparación y aprobación de la Política de Seguridad (en este caso revisión) incluye la definición de roles, la asignación de responsabilidades y la creación del Comité de Seguridad. Este paso plantea como entregables principales la Política de Seguridad de Aguas de Burgos revisada por la Dirección y el Acta de Constitución del Comité de Seguridad.

Es importante recalcar que la Política de Seguridad de la Información debe recoger los nombramientos de los roles de los diferentes responsables, y de sus funciones, así como de las funciones y miembros de los diferentes Comité necesarios, requeridos por el Marco Organizativo del ENS.



De acuerdo con las indicaciones del CCN-CERT se usarán las siguientes guías CCN-STIC (Guías de Seguridad de las TIC) en cada uno de los seis pasos descritos.

5.1.2 Gestión de la seguridad

5.1.2.1 Seguridad proactiva

Tendrá como objetivo la implantación y mejora continua del proceso de gestión de la seguridad alineado con las buenas prácticas internacionales de seguridad y la legislación aplicable a Aguas de Burgos.

La OTSI realizará actividades vinculadas a la seguridad proactiva, en concreto:

- Implantación y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) de Aguas de Burgos, realizando al menos las siguientes tareas:
    - Elaboración del análisis de riesgos, incluido el inventariado de activos IT/OT, la definición y elaboración del modelo de dependencias, el diseño, obtención y análisis de resultados de encuestas para valoración de activos, la identificación y valoración de las amenazas, la identificación y valoración de salvaguardas, la estimación del riesgo, la proyección del riesgo etc. Para ello hará uso de la herramienta de análisis y gestión de riesgos PILAR, desarrollada por el Centro Criptológico Nacional (CCN) y cuantas herramientas del CCN-CERT se consideren necesarias.
    - El análisis de riesgos incluirá tanto los riesgos IT como los riesgos de las redes OT, siendo un análisis especializado para el sector del agua.
    - Elaboración o revisión de normas, procedimientos, protocolos, instrucciones técnicas y guías de seguridad de la información (técnicas y no técnicas).
    - Desarrollo y seguimiento del cuadro de mando de indicadores.

  El marco de trabajo de referencia será el Esquema Nacional de Seguridad (ENS), la directiva NIS2, la norma ISO 27001 y subsiguientes, o equivalentes, así como otras metodologías en el ámbito de la seguridad de la información ampliamente reconocidas (Leet, ENS, NIST, SANS, COBIT, etc.).
- Asesoramiento experto en materia regulatoria en el ámbito de la seguridad de la información y la ciberseguridad, en particular en las leyes vigentes en los siguientes ámbitos:
    - Esquema Nacional de Seguridad (ENS).
    - Directiva NIS2.
    - Esquema Nacional de Interoperabilidad (ENI).
    - Protección de Infraestructuras Críticas y Servicios Esenciales.
    - Protección de Datos de Carácter Personal (RGPD).
    - Firma electrónica.
    - Otras normas asociadas del sector de carácter nacional y/o internacional.
- Integración de la OTSI en todos aquellos proyectos que requieran de asesoría en materia de seguridad, para la identificación, definición y propuesta de requisitos de seguridad en el desarrollo y/o implantación, tanto de nuevos

sistemas de información como en la evolución de los existentes (correctivos, evolutivos y perfectivos).

- Definición de requerimientos de seguridad a incluir en los pliegos de contratación según las normas y los requisitos legales existentes que sean de aplicación, así como las políticas, normas y procedimientos aprobados por Aguas de Burgos o que se consideren necesarios.
- Definición de requisitos técnicos y estimaciones económicas que sirvan de apoyo a Aguas de Burgos en la redacción de los pliegos de prescripciones técnicas de:
    - Seguridad física de las instalaciones y de las activos IT/OT.
    - Redacción de proyectos de mejoras y adaptación del CPD de Aguas de Burgos en cumplimiento del estándar ANSI/TIA-942.
    - Licencias comerciales según lo indicado en el apartado “5.3.9 Software”.
    - Suministros de productos y servicios de ciberseguridad identificados por la OTSI.
    - Suministros de productos y servicios que garanticen la seguridad y optimización de las comunicaciones internas y externas, y de las redes IT/OT.
    - Test de penetración y vulnerabilidades.
- Gestión de herramientas del CCN-CERT para el aseguramiento de la correcta implantación de la seguridad, adecuación al ENS, cumplimiento normativo y acceso a la información indicadores entre otros:
    - ANA Central
    - AMPARO
    - CLARA
    - INES
    - IRIS
    - PILAR

La actividad de la OTSI contempla la resolución de consultas, la elaboración de informes, la preparación de propuestas para adaptación y mejora, preparación de declaración de aplicabilidad y planes de adecuación, elaboración de encuestas para valoración y seguimiento del cumplimiento de la normativa vigente (RGPD, ENS, NIS2), así como cualquier otra actividad relacionada con el objetivo de esta actividad.

- Apoyo a la continuidad del negocio, realizando al menos las siguientes tareas:
    - Elaboración del Análisis de Impacto en el Negocio (BIA).
    - Elaboración y revisión, en su caso, de los Planes de Recuperación ante Desastres y pruebas asociadas, para la detección de deficiencias y elaboración de propuestas de mejora e identificación de oportunidades.
    - Definición de pruebas de controles sobre los sistemas corporativos de gestión y control de la información financiera (SCIIF).
- Consultoría y asesoramiento especializado en cualquier aspecto relacionado con la seguridad de la información y la ciberseguridad incluido en el cumplimiento del de la normativa vigente (RGPD, ENS, NIS2), entre otros y sin que se trate de una relación exhaustiva, los siguientes:
    - Gestión y de identidades y control de acceso a los sistemas de información.
    - Gestión de certificados digitales y firma electrónica.
    - Gestión de vulnerabilidades.
    - Seguridad Perimetral (WAF, NGF, IDS/IPS, etc.).
    - Control de acceso a la red (NAC).
    - Seguridad en el puesto de trabajo (*endpoint*).
    - Seguridad en dispositivos móviles.
    - Arquitecturas de seguridad y segmentación de redes.
    - Seguridad en los protocolos de comunicación.
    - Bastionado y *hardening* de sistemas, servidores y servicios.
    - Seguridad en la nube (SaaS, PaaS, IaaS, etc.).
    - Gestión de logs y correlación de eventos de seguridad.
    - Código malicioso (*malware*).
    - Mecanismos de autorización, acceso y autenticación.
    - Desarrollo seguro de software.
    - Acreditación de sistemas.
    - Definición de cómo llevarse a cabo la Detección, prevención, análisis (tácticas y técnicas) y respuesta ante Amenazas Avanzadas Persistentes

(APTs).

- Definición de los planes de implantación de las herramientas del CCN-CERT seleccionadas para la ejecución de las diferentes actividades de seguridad integral.
- Elaboración y programación de informes estadísticos y de detalle sobre las herramientas de seguridad disponibles por Aguas de Burgos (antivirus, antispam, gestor de navegación segura, etc.).
- Soporte a las actividades de divulgación y concienciación en materia de seguridad de la información y ciberseguridad industrial, realizando al menos las siguientes tareas:
    - Elaboración de propuestas formativas (módulos formativos, *newsletters*, guías, píldoras, etc.).
    - Generación de contenidos divulgativos relacionados con la prevención y respuesta a incidentes de seguridad.
    - Impartición de seminarios y formación relacionada con la seguridad TIC y la ciberseguridad industrial al personal de Aguas de Burgos.

5.1.2.2 Seguridad preventiva

Tendrá como objetivo incorporar los mecanismos necesarios de vigilancia que permitan anticipar la posible ocurrencia de incidentes de seguridad, aplicando para ello las medidas correctoras más adecuadas para la infraestructura IT/OT de Aguas de Burgos.

La OTSI coordinará actividades vinculadas a la definición de procedimientos y protocolos de seguridad preventiva, así como la ampliación de la selección de las herramientas de CCN-CERT más adecuadas en concreto:

- Ciberinteligencia:
    - Vigilancia digital: búsqueda en Internet de información relacionada con Aguas de Burgos, su marca, imagen y servicios, con el objeto de detectar posibles fugas de información, campañas contra su seguridad y/o imagen, fraude, phishing, etc. Los ámbitos de búsqueda incluyen, al menos, foros, blogs, redes sociales y redes profesionales, bases de datos de ofertas y demandas de empleo, sitios corporativos de terceros y sites personales, metadatos, webs externas a Aguas de Burgos, canales y foros *underground*, redes alternativas, redes P2P, criptodivisas (Bitcoin, Litecoin, etc.), etc.
    - Ciberinvestigación para el análisis de datos relevantes.

- Inteligencia de amenazas.

- Enumeración de los diferentes recursos expuestos hacia Internet y que, por tanto, están en riesgo al ser susceptibles de recibir ataques relacionados con su plataforma tecnológica, aplicaciones, arquitectura, implantación y/o desarrollo.
- Análisis de visibilidad (pasiva y activa), enumeración, identificación y revisión de los dispositivos inalámbricos dentro del área de radiofrecuencia WiFi en las ubicaciones físicas que determine Aguas de Burgos.
- Revisión del diseño de los actuales escenarios de uso WiFi y de la evolución prevista de los mismos.
- Verificación de la eficacia de las medidas de seguridad establecidas a través de los distintos sistemas de seguridad implantados.
- Análisis del nivel de exposición y riesgo de los sistemas de información que soportan las distintas aplicaciones y servicios existentes.
- Análisis en profundidad de los mecanismos que gestionan las sesiones de usuario en aplicativos y servicios web, incluyendo la autenticación y autorización de los mismos.
- Identificación y verificación de las vulnerabilidades y amenazas asociadas a los sistemas de Información, aplicaciones y servicios existentes, y análisis de los actuales mecanismos de seguridad desplegados para el control de dichas vulnerabilidades y amenazas.
- Análisis de resultados de los test de penetración y vulnerabilidades que Aguas de Burgos encargue a proveedores externos. El resultado de este análisis servirá para actualizar la documentación generada por la OTSI.
- Propuesta de una metodología de desarrollo seguro, así como el desarrollo del marco normativo necesario y relacionado con las distintas tecnologías de programación utilizadas en Aguas de Burgos.
- Buenas prácticas, recomendaciones y propuestas de mejora, securización, bastionado y *hardening* de sistemas, aplicaciones y servicios en base a las arquitecturas y escenarios actuales y previstos, y los distintos problemas detectados. Priorización por esfuerzo (temporal y económico) y beneficios obtenidos (*quick wins*).
- Soporte al seguimiento y control de las medidas correctoras y planes de acción identificados en los resultados de auditorías de seguridad realizadas por terceros.

5.1.2.3 Seguridad reactiva

Tendrá como objetivos, entre otros, la mejora del control y del nivel de seguridad de los sistemas informáticos corporativos y de los sistemas de control industrial, la mejora en los plazos de detección, evaluación y respuesta a los posibles incidentes de seguridad que se produzcan, disminuir el riesgo ante las amenazas actuales (phishing, fraude, virus y malware en general, denegación de servicio, intrusión, robo o filtración de información, pérdida de datos, etc.), el acceso a mejores mecanismos y herramientas de seguridad, la monitorización de la seguridad a través de la integración de los eventos de los distintos sistemas de seguridad, así como definir las capacidades de un futuro equipo especializado para la actuación ante posibles incidentes de seguridad que afecten a la seguridad de la información, seguridad física, ciberseguridad industrial y seguridad de las personas.

La OTSI coordinará actividades vinculadas a la definición de procedimientos y protocolos de seguridad reactiva, así como la ampliación de la selección de las herramientas de CCN-CERT más adecuadas en concreto:

- Servicio de monitorización de la seguridad.
- Gestión de incidentes de seguridad.
- Servicio de respuesta ante incidentes.
- Análisis de malware.
- Investigación forense.
- Uso de indicadores de compromiso en la respuesta a incidentes de seguridad y en la investigación forense.

5.1.3 Gestión del proyecto

5.1.3.1 Coordinación de tareas

La OTSI actuará como responsable e interlocutor con Aguas de Burgos de la ejecución de todas las tareas a realizar dentro del alcance de este pliego durante de la fase adecuación. Para ello, designará un Jefe de Proyecto (Responsable de la OTSI) encargado de dicha gestión.

La OTSI coordinará por tanto la realización de los trabajos que le son propios, así como los de la implantación de las herramientas del CCN-CERT, la implantación del hardware y software, las tareas de adecuación de la infraestructura IT/OT y la puesta en marcha del SOC, junto con todas las interrelaciones y dependencias entre dichos trabajos.

5.1.3.2 Priorización de tareas

La OTSI elaborará un plan de proyecto detallado, con el desglose de actividades y

tareas, recursos, hitos y entregables de la fase de adecuación e implantación desde la fecha de firma del contrato. Este plan reflejará el porcentaje que representa cada una de las tareas, respecto al total del proyecto. Este plan, deberá ser validado por Aguas de Burgos al inicio del proyecto. En caso de desacuerdo, en las actividades, recursos, hitos o entregables, Aguas de Burgos establecerá el plan de proyecto conforme a los requisitos de este pliego.

Periódicamente, se revisará, priorizará y completará el programa de tareas asignadas a la OTSI, según las necesidades de Aguas de Burgos. La programación se realizará por el Jefe de Proyecto (Responsable de la OTSI) según la priorización de las necesidades de Aguas de Burgos.

Por su parte, el Jefe del Proyecto del adjudicatario deberá presentar una propuesta justificada con la duración prevista para cada tarea asignada, que será tenida en cuenta para la planificación. Para esta propuesta se partirá de la premisa básica de que los consultores cuentan con la formación, experiencia, capacidad, habilidad y conocimientos expertos en las diferentes áreas y recursos necesarios para abordar los trabajos de forma diligente. No se admitirán demoras injustificadas, en particular aquellas que denoten falta de formación o conocimientos por parte de los técnicos adscritos a la OTSI.

El retraso en la ejecución de las tareas programadas será un indicador clave en los Acuerdos de Nivel de Servicio (ANS).

5.1.3.3 Transferencia

Todos los trabajos que realice la OTSI deben realizarse en coordinación con Aguas de Burgos, y especialmente con el Responsable de Seguridad de Aguas de Burgos, otros empleados de Aguas de Burgos o un tercero designado por Aguas de Burgos, quienes deberán recibir la capacitación, documentación e informaciones necesarias para poder dar continuidad a los trabajos realizados al alcanzarse la fecha de finalización del contrato.

5.2. Implantación de herramientas del CCN-CERT

Atendiendo a lo establecido por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y en concreto por el artículo 157 relativo a la Reutilización de sistemas y aplicaciones de propiedad de la Administración, Aguas de Burgos opta por el uso de las herramientas y tecnologías que el Centro Criptológico Nacional (CCN) pone a disposición de sector público.

Las herramientas proporcionadas por el CCN-CERT proporcionan funcionalidades de Detección, Análisis, Auditoría e Intercambio de información. La OTSI coordinará los planes de implantación de las herramientas del CCN-CERT para asegurar la más idónea implantación en Aguas de Burgos.

Entre estas soluciones del CCN-CERT se encuentran las siguientes:

- Auditoría e implantación de Seguridad y Cumplimiento del ENS:
    - ANA (Automatización y normalización de auditorías).
    - PILAR (Análisis y Gestión de Riesgos).
    - CLARA (Auditoría de Cumplimiento ENS/STIC en Sistemas Windows y Linux).
    - INES (Informe de Estado de Seguridad en el ENS). Conviene reseñar que el siguiente paso sería la implantación de medidas de seguridad, a través de la solución AMPARO.
    - AMPARO (Implantación de seguridad y conformidad del ENS).
    - MARGA (permite la elaboración de la Documentación de Seguridad necesaria para la solicitud de la Acreditación de Seguridad de los sistemas que manejan información clasificada).
    - IRIS (Estado de Ciberseguridad).
    - REYES (Intercambio de Información de Ciberamenazas).
- Tratamiento de incidentes:
    - ADA (Plataforma avanzada de análisis de malware).
    - CARMEN (Defensa de ataques avanzados/APT).
    - LUCIA (Sistema de Gestión Federada de Tickets).
- Herramientas para la defensa de equipos y activos de la organización:
    - CLAUDIA (Herramienta para la detección de amenazas complejas en el puesto de usuario).
    - MicroCLAUDIA (Centro de vacunación).
    - ROCIO (Inspección de Operación. Auditoría de configuraciones de dispositivos de red).
- Herramientas para la defensa de las conexiones y la red:
    - ELSA (Exposición Local y Superficie de Ataque).
    - EMMA (Visibilidad y control sobre la red).
    - SAT (Sistema de Alerta Temprana). Se distingue entre SAT-ICS, SAT-INET y SAT-SARA y SAT-Distribuido / GLORIA.

- Herramientas de protección de la información:
    - CARLA (Protección y trazabilidad del dato).
- SIEMs, monitorización y alerta de eventos:
    - GLORIA (Gestor de logs para responder ante incidentes y amenazas).

El adjudicatario realizará la implantación y configuración de las herramientas del CCN-CERT que se detallan en los siguientes subapartados, junto con todas las integraciones entre dichas herramientas. La implantación de herramientas se realizará preferentemente en modo on-premise sobre la infraestructura hardware y software que el adjudicatario implante para dar cumplimiento a los requisitos del apartado “5.3 Suministros de ciberseguridad”. Dicha infraestructura deberá estar suficientemente dimensionada para permitir la correcta operación de los sistemas ya implantados durante los próximos 5 años, los cuales están descritos en el apartado “2 Objeto y alcance”, así como de las herramientas del CCN-CERT a ser implantadas.

Se podrán utilizar herramientas del CCN-CERT en la nube (modo cloud), siempre y cuando no estén disponibles en modo on-premise, o cuando el adjudicatario justifique y recomiende la utilización de herramientas en la nube y Aguas de Burgos así lo apruebe.

Cualquier otro equipamiento hardware, software o licencias necesarias será por cuenta del adjudicatario, debiendo detallarse todas y cada una de las necesarias, siendo obligatorio, en todo caso, incluir de todo ello garantía del fabricante que incluya actualizaciones del software y firmware durante al menos los cinco primeros años.

Todas las gestiones necesarias para la implantación, configuración y utilización de las herramientas del CCN-CERT serán realizadas por la OTSI.

En el caso las herramientas CARLA, EMMA y CARMEN que requieren de una certificación para su instalación, operación y soporte en el sector público, libre de costes de licencias como soluciones desarrollada por el CCN-CERT, será requisito obligatorio disponer de las certificaciones necesarias para la instalación y operación con garantías de cada una de dichas herramientas, o deberán ser objeto de subcontratación a una empresa certificada, los trabajos para la instalación y operación con garantías de cada una de dichas herramientas, conforme al artículo 140.4 de la Ley 9/2017 (LCSP), y según Anexo XII del PCAP. Aguas de Burgos, dispondrá de acceso a todos los niveles de soporte de todas las herramientas del CCN-CERT de este pliego.

Al finalizar la implantación de las herramientas del CCN-CERT, el adjudicatario proporcionará al personal de Aguas de Burgos el acceso, con el perfil que determine Aguas de Burgos, a todas las consolas, aplicaciones, portales, cuadros de mando, etc., de las que dispongan las herramientas del CCN-CERT.

5.2.1 PILAR

PILAR (Análisis y Gestión de Riesgos). El adjudicatario realizará un análisis de riesgos con la herramienta PILAR del CCN-CERT (no se usará microPILAR, ni PILAR Basic) que implementa la metodología MAGERIT. Se usará la última versión de esta herramienta. Este análisis de riesgos se repetirá anualmente durante la vigencia del contrato, de forma que no transcurran más de 12 meses desde el análisis anterior.

PILAR cuenta con un módulo de cumplimiento con el ENS que ayuda a la adecuación del mismo, que será utilizado por el adjudicatario.

El adjudicatario se coordinará con el Delegado de Protección de Datos de Aguas de Burgos para incorporar al análisis de riesgos la parte relativa al cumplimiento del RGPD. La función del Delegado de Protección de Datos (DPD) está ejercida en el marco de un contrato de servicios suscrito con un proveedor externo.

En la realización del análisis de riesgos se reflejará el estado de cumplimiento de las medidas de seguridad, indicando el nivel de madurez de las medidas de la declaración de aplicabilidad.

5.2.2 LUCIA

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) es una herramienta desarrollada por el CCN-CERT para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora.

LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.

El adjudicatario deberá realizar todas las tareas de configuración y administración de la herramienta LUCIA, junto con la elaboración de la documentación necesaria para la operación, vigilancia y gestión de incidentes por parte del SOC. Las tareas a realizar permitirán:

- Dotar a Aguas de Burgos de una herramienta interna para la gestión de sus incidentes propios.
- Comunicar y sincronizar incidentes de seguridad entre el CCN-CERT y su comunidad mejorando el intercambio y coordinación con aquellos adscritos al Sistema de Alerta Temprana (SAT-INET / SAT-ICS)
- Reportar al CCN-CERT la información de metadatos de todos los incidentes de seguridad identificados en Aguas de Burgos.

- Reportar incidentes que afecten a la RGPD (AGPD) y LPIC (CNPIC).
- Integración con el resto de herramientas del CCN-CERT de este pliego.

5.2.3 REYES

REYES (Intercambio de Información de Ciberamenazas) es una solución desarrollada por el CCN-CERT para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas.

A través de este portal centralizado de información se puede realizar cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes. Una información contextualizada y correlacionada con las principales fuentes de información, tanto públicas como privadas.

El núcleo de información de REYES está basado en la tecnología MISP (Malware Information Sharing Platform), que es enriquecida con fuentes externas de información que permiten agilizar la prevención y la respuesta a incidentes.

El adjudicatario deberá realizar todas las tareas de configuración y administración de la herramienta REYES, junto con la elaboración de la documentación necesaria para la operación, vigilancia y gestión de incidentes por parte del SOC. Las tareas a realizar permitirán:

- Dotar a Aguas de Burgos de un repositorio de ciberinteligencia, empleado para el análisis y detección de ciberamenazas.
- Descargar paquetes de reglas de detección de ciberamenazas, muestras e indicadores para responder a posibles ciberincidentes.
- Configuración de alertas y descarga automática de listas negras generadas por el CCN-CERT para la detección y bloqueo de ciberamenazas, que incluyen información sobre direcciones IP, dominios, URL sospechosas, etc.
- Reportar incidentes que afecten a la RGPD (AGPD) y LPIC (CNPIC).
- Integración con el resto de herramientas del CCN-CERT de este pliego.

5.2.4 GLORIA

GLORIA (Gestor de Logs para Respuesta ante Incidentes y Amenazas) es una solución que, va más allá del SIEM para la operación integral de un Centro de Operaciones de Seguridad (CSIRT/CERT o SOC).

GLORIA es la adoptada por el CCN-CERT para la operación de sus servicios, entre ellos SAT-INET y SAT-ICS y está a disposición de la Administración Pública española, sin

coste de licencias, como parte de la familia de soluciones del CCN-CERT.

GLORIA es la herramienta principal de monitorización a instalar en este proyecto, y sobre la que girarán otras herramientas del CCN-CERT.

GLORIA tiene capacidades de monitorización y recolección de eventos de seguridad tanto del mundo IT (Information Technology) como del mundo OT (Operational Technology), de centralización, normalización y análisis de eventos (logs), así como de inteligencia avanzada mediante técnicas de correlación compleja de eventos o análisis de patrones para la detección de amenazas y la identificación de anomalías.

En definitiva, el uso de GLORIA aumenta la eficiencia de los equipos de analistas de los Centros de Operaciones de Seguridad (SOC) mediante la aplicación de técnicas de automatización y orquestación de las tareas de detección y respuesta (análisis de eventos, identificación de incidentes, recolección de información de contexto, confirmación y notificación de incidentes).

El adjudicatario deberá realizar todas las tareas de instalación, implantación y administración de la herramienta GLORIA, junto con la elaboración de la documentación necesaria para la operación, vigilancia y gestión de incidentes por parte del SOC. Entre dichas tareas, y sin que suponga una lista limitante, deberán realizarse al menos las siguientes:

- Diseño de la arquitectura, análisis y solución definitiva.
- Definición de los requerimientos técnicos (servidores y software necesario) sobre los que se instalará la solución GLORIA y las diferentes sondas.
- Preparación, documentación y despliegue del nodo principal de GLORIA en formato virtual dentro del CPD principal de Aguas de Burgos, y de nodos secundarios y/o de alta disponibilidad en el CPD complementario. El despliegue abarca la implantación y configuración de todos los módulos de GLORIA, así como de la definición, preparación y configuración de los backups y mantenimiento necesario de los mismos.
- Instalación y preparación de sondas (HIDS, NIDS, redirector logs FG) remotas en los CPDs que dispone Aguas de Burgos
- Configuración y parametrización de las funcionalidades base (HIDS, NIDS) de la plataforma GLORIA
- Parametrización de reglas de correlación.
- Integración de las fuentes orígenes de datos en la plataforma GLORIA:
    - Logs de los dispositivos de seguridad perimetral como firewall, antivirus, proxys, etc.

- Logs de los servidores y de las aplicaciones.
- Logs de switches/Routers
- Logs de dispositivos de redes OT
- Equipos personales.
- Integración con otras herramientas del CCN-CERT de este pliego.

El listado final de los activos (servidores, dispositivos de redes IT/OT, de bases de datos, aplicaciones, etc.) a monitorizar será definido de mutuo acuerdo con el adjudicatario durante la fase de consultoría inicial.

- Integración con el SAT distribuido GLORIA Central.
- Definición de cuadro de mandos de las fuentes de información integradas.

El listado de los activos (servidores, dispositivos de redes IT/OT, de bases de datos, aplicaciones, etc.) a monitorizar se obtendrá a partir del análisis de riesgos y del inventariado de activos IT/OT realizado por la OTSI.

Todo el hardware necesario para el funcionamiento de GLORIA, su correcto dimensionamiento, suministro, instalación y configuración será por cuenta del adjudicatario.

5.2.5 EMMA

Con EMMA (Visibilidad y control sobre la red), el CCN-CERT pretende facilitar a las organizaciones visibilidad y control completo de la capa de acceso a la red (routers, switches, puntos de acceso, controladores, etc.), un punto crucial para verificar quién o qué está conectado en una red. En el contexto actual, los modelos de seguridad requieren de una verificación de identidad estricta para cada persona y dispositivo (estén dentro o fuera del perímetro) y es más difícil controlar el crecimiento exponencial de los activos (distintos lugares físicos, data-centers, proveedores, distintos tipos (dispositivos de usuario, IoT, dispositivos de electrónica (switches APs etc.)).

EMMA es una solución modular, lo que permite a las organizaciones adoptar solo los módulos necesarios en su situación actual y en una aproximación de menos a más. Esta aproximación permite reducir el riesgo e impacto operacional al acotar el alcance funcional de la implementación a las necesidades actuales.

Aguas de Burgos requiere la implantación del sistema de Control de Acceso a la Red (NAC) basado en la solución del CCN-CERT EMMA, que cubre las necesidades anteriormente expuestas y que está integrado con otras soluciones del CCN-CERT como ROCÍO. Esta solución ofrece funcionalidades de:

- Visibilidad. Control de Acceso Universal. Autenticación.

- Segmentos de red mínimos: Red Corporativa, VoIP, Invitados, Impresión, Gestión, IoT, Microsegmentación y Wifi.
- Aplicar segmentación dinámicamente para reducir la superficie de ataque, aislar dispositivos críticos y responder ante ataques de manera centralizada.
- Comprobación del compliance/cumplimiento de políticas por parte de la configuración de la electrónica de red mediante la integración con ROCIO y securización de redes.
- Registros de actividad (logs) e informes.
- Agregación de datos sobre activos, dispositivos, usuarios, eventos, accesos etc. Informes de trazabilidad e integración con ROCÍO.
- Bastionado de los servidores instalados, según guías CCN-CERT.
- CMDB.

El adjudicatario deberá realizar todas las tareas de instalación, implantación y administración de la herramienta EMMA, junto con la elaboración de la documentación necesaria para la operación, vigilancia y gestión de incidentes por parte del SOC. Entre dichas tareas, y sin que suponga una lista limitante, deberán realizarse al menos las siguientes:

- Diseño de la arquitectura, análisis y solución definitiva.
- Definición de los requerimientos técnicos (servidores y software necesario) sobre los que se instalará la solución EMMA y las diferentes sondas.
- Preparación, documentación y despliegue del nodo principal de EMMA en formato virtual dentro del CPD principal de Aguas de Burgos, y de nodos secundarios y/o de alta disponibilidad en el CPD complementario.
- El despliegue incluirá la implantación y configuración de todos los módulos de EMMA, así como de la definición, preparación y configuración de los backups y mantenimiento necesario de los mismos.
- Integración de la plataforma EMMA con el resto de herramientas del CCN-CERT de este pliego.
- Definición de cuadro de mandos.

5.2.6 ROCIO

ROCIO (Inspección de Operación. Auditoría de configuraciones de dispositivos de red) es una solución para la automatización de las tareas básicas realizadas por un auditor

de seguridad sobre equipos de comunicaciones: enrutadores, conmutadores y cortafuegos. Así, ha sido desarrollada por el CCN-CERT para verificar el nivel de seguridad de dichos equipos. La solución ROCIO complementa EMMA, ya que comprueba la configuración de los dispositivos con las guías STIC que tiene ROCIO.

Para usar la solución, el usuario debe cargar el fichero de configuración del equipo a auditar. Adicionalmente, puede cargar también el resultado de la ejecución de algunos comandos que muestren información del sistema. Por ejemplo, tablas de encaminamiento, direcciones o estado de enlaces, entre otras.

Una vez cargada la información, el usuario solicita la realización de la auditoría de seguridad; que consiste en la comprobación de un conjunto de reglas predefinidas que analizan aspectos de seguridad del equipo, como el cifrado de las contraseñas, la utilización de protocolos de cifrado para el acceso a la gestión o la existencia de listas de acceso.

El adjudicatario deberá utilizar la herramienta ROCIO para la adecuación al ENS de los dispositivos de red forma previa a la operación por parte del SOC.

5.2.7 CLARA

CLARA (Auditoría de Cumplimiento ENS/STIC en Sistemas Windows y Linux), Herramienta para analizar las características de seguridad técnicas por el Esquema Nacional de Seguridad.

La aplicación se compone de CLARA ENS (versión 32 y 64 bits), para análisis independiente en entornos Microsoft Windows y CLARA ENS LINUX para entornos Linux.

La herramienta para el análisis de cumplimiento es funcional exclusivamente en sistemas Windows y Linux, tanto en sus versiones cliente como servidor, miembros de un dominio o independientes al mismo.

El adjudicatario deberá utilizar la herramienta CLARA para la adecuación al ENS de los dispositivos de red forma previa a la operación por parte del SOC.

5.2.8 ANA CENTRAL

ANA (Automatización y Normalización de Auditorías) es un sistema de auditoría continúa desarrollado por el CCN-CERT que tiene por objetivo incrementar la capacidad de vigilancia y conocer la superficie de exposición. Con esta herramienta se pretende reducir los tiempos en la gestión de la seguridad, mediante una gestión eficiente de la detección de vulnerabilidades y de la notificación de alertas, así como ofreciendo recomendaciones para un tratamiento oportuno de las mismas.

Entre las características más destacadas de esta herramienta se encuentran:

- Evolución: utiliza las tecnologías más vanguardistas.
- Fluidez: permite aunar en ella múltiples funciones.
- Centralización: posibilita la integración con otras herramientas, como LUCIA, PILAR y CLARA.
- Versatilidad: favorece la visualización multiplataforma.

El adjudicatario deberá realizar todas las tareas de configuración y administración de la herramienta ANA CENTRAL, junto con la elaboración de la documentación necesaria para la operación, vigilancia y gestión de incidentes por parte del SOC. Las tareas a realizar permitirán:

- Gestionar grupos de usuarios y sus roles. Integración con Directorio Activo.
- Crear cuadros de mando sobre dispositivos por riesgo.
- Cuantificar y visualizar dispositivos afectados.
- Crear cuadros de mando para planes de acción (remediación). Generación de tickets a través de LUCIA.
- Alerta temprana mediante interacción directa y detallada de los problemas encontrados permitiendo una notificación oportuna sin dilación indebida
- Definir las auditorías que se realizarán, para gestionar que información se recogerá de cada activo y evitar duplicados en la recogida de información:
    - Integrar ANA con EMMA y CLARA, quienes poseen un inventariado de activos externos (direcciones IPs, dominios y subdominios) por parte de ANA, de servidores y puestos de trabajo Windows/Linux gracias a CLARA y añadiendo a su inventariado los dispositivos de red de EMMA.
    - Integración con herramientas de escaneo compatibles, como Nessus de Tenable u otras de libre distribución.
- Integración con el resto de herramientas del CCN-CERT de este pliego.

El adjudicatario deberá utilizar la herramienta ANA CENTRAL para la adecuación al ENS de los dispositivos de red tanto de forma previa como posterior a la operación por parte del SOC.

5.2.9 CARMEN

CARMEN (Centro de Análisis de Registros y Minería de EveNtos) es una solución software del CCN-CERT de adquisición, procesamiento y análisis de información para soportar el proceso de identificación de Amenazas Persistentes Avanzadas (APT) a

partir del tráfico de red interno y saliente de una forma eficiente, apoyando la toma de decisiones a partir de la información generada y procesada. Se compone de agentes que recopilan los flujos de tráfico, un motor de almacenamiento en el que se inserta la información, un sistema de detección de anomalías que se encarga de procesar la información almacenada y una aplicación web que permite la representación y consulta tanto de la información obtenida como de la procesada.

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

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

En relación a los movimientos laterales de la amenaza, CARMEN es capaz de adquirir información de los mecanismos más habituales para el mantenimiento de persistencia y el intercambio de información entre sistemas (psexec, rdp, named pipes, etc.).

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

El adjudicatario deberá realizar todas las tareas de instalación, implantación y administración de la herramienta CARMEN en Aguas de Burgos e integrará:

- La adquisición, el procesamiento y el análisis de la información recogida. por CARMEN, junto al resto de soluciones de detección (SAT-INET y SAT-ICS) y de análisis (GLORIA, ADA), CARMEN se encarga de detectar anomalías y movimientos laterales y externos dentro de la red. Además, esta solución del CCN-CERT gubernamental analiza código dañino mediante sandboxing avanzado.

- GLORIA con la solución CARMEN, para la gestión de amenazas persistentes avanzadas. CARMEN realiza el análisis automático, semiautomático y manual del tráfico de red de la organización para la detección de usos indebidos y para la detección de anomalías significativas en este tráfico, aportando también capacidades para la detección de la amenaza en la etapa de intrusión, así como despliegue e integración de capacidades de sandboxing, para la detección de estafas por correo como el spear phishing.

- El resto de herramientas del CCN-CERT expuestas en este pliego.

La instalación, implantación y administración de la herramienta CARMEN incluirá:

- Diseño de la arquitectura, análisis y solución definitiva.
- Definición de los requerimientos técnicos (servidores y software necesario) sobre los que se instalará la solución CARMEN y las diferentes sondas.
- Preparación, documentación y despliegue del nodo principal de CARMEN en formato virtual dentro del CPD principal de Aguas de Burgos, y de nodos secundarios y/o de alta disponibilidad en el CPD complementario.
- El despliegue incluirá la implantación y configuración de todos los módulos de CARMEN, así como de la definición, preparación y configuración de los backups y mantenimiento necesario de los mismos.
- Integración de la plataforma CARMEN con el resto de herramientas del CCN-CERT de este pliego.
- Definición de cuadro de mandos.
- Conexión con CARMEN CENTRAL.

5.2.10 CLAUDIA y microCLAUDIA

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

CLAUDIA (Herramienta detección de amenazas en el puesto de usuario) ofrece la posibilidad de ejecutar varios sensores que permitirán obtener más información de las máquinas de la red:

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

MicroCLAUDIA (Centro de vacunación) es una herramienta del CCN-CERT gratuita para administraciones públicas basada en CLAUDIA, que proporciona protección contra malware del tipo ransomware a los equipos de trabajo, es un agente para sistemas Microsoft Windows, que se encarga del despliegue y ejecución de vacunas contra ataques de ransomware.

La conexión del agente al servicio central de microCLAUDIA, ubicado en la nube del CCN-CERT, permite descargar y ejecutar las vacunas que se hayan configurado para sus equipos. Una vez descargadas, el agente no requiere de conectividad a la nube para su ejecución ni de un servicio central o servidor instalado en Aguas de Burgos.

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

Por otro lado, el CCN-CERT administra el servicio central en su nube y se encarga de la generación de nuevas vacunas, permitiendo un acceso a este servicio para su administración y supervisión.

El adjudicatario deberá establecer un plan para la implantación masiva de los agentes de CLAUDIA y microCLAUDIA en todos los equipos de la red de Aguas de Burgos. Una vez hecho esto, toda la información recogida por dichos agentes deberá estar integrada tanto con las herramientas del CCN-CERT expuestas en este pliego con las propias de monitorización y Sistemas de Información de Aguas de Burgos. Se enmarcan las siguientes actividades:

- Diseño de la arquitectura de las herramientas CLAUDIA/microCLAUDIA a instalar definitivamente, incluyendo requisitos hardware en base a las necesidades de los agentes.
- Definición de los requerimientos técnicos sobre los que se instalarán las herramientas CLAUDIA/microCLAUDIA.
- Preparación, documentación y despliegue de las herramientas en formato físico dentro del CPD principal y secundarios.
- Integración con el resto de herramientas del CCN-CERT (CARMEN, GLORIA), a través de APIs provistas por las propias herramientas de CLAUDIA y microCLAUDIA. Integración con el resto de herramientas de monitorización de Aguas de Burgos para generar cuadros de mando.
- Aplicación de inteligencia mediante casos de uso, personalización y desarrollo de nuevos casos de uso.

El adjudicatario deberá proporcionar al personal del equipo técnico de Aguas de Burgos y al SOC acceso a la consola de gestión de CLAUDIA/microCLAUDIA y la formación necesaria sobre las herramientas de trabajo.

5.2.11 Sondas SAT-ICS, SAT-INET y SAT-Distribuido / GLORIA

Implantación del sistema de alerta temprana, que permite descubrir de forma rápida y sencilla las vulnerabilidades que afectan a sus sistemas. El sistema notifica y proporciona el remedio por la solución de vulnerabilidad.

Cada sonda es un servidor de alto rendimiento y dedicado, que incorpora varias herramientas de detección y monitorización open source y comerciales (NIDS, arpwatch, ntop, etc…) y que cuenta con dos interfaces de red diferenciados:

- Interfaz de análisis: recibe todo el tráfico a analizar. Este interfaz sólo lee el

tráfico, sin modificarlo en ningún momento, y sólo aquel que es necesario para su función (no datos que puedan considerarse sensibles-payload).

- Interfaz de gestión: conecta a través de internet de forma segura con el sistema de monitorización/correlación, haciendo uso de la infraestructura de Aguas de Burgos.

El adjudicatario deberá:

- Implantar las sondas necesarias en la arquitectura de red de Aguas de Burgos.
- Establecer los requisitos de hardware para el correcto funcionamiento de las mismas, así como definir el número de equipos necesarios en caso de necesitar redundancia o alta disponibilidad en la solución desplegada.
- Proveer del material hardware necesario para la realización de todas las conexiones de equipos con las sondas. Las capacidades de procesador, memoria, almacenamiento, red, soporte óptico y sistema operativo deberán ser las suficientes y necesarias para que permitan la instalación tanto del sistema operativo como de las aplicaciones necesarias y que aseguren el almacenamiento de eventos generados por la sonda durante un periodo de tiempo razonable para el correcto funcionamiento del sistema, incluyendo requisitos hardware para las sondas necesarias a implementar de tipo:
    - **SAT-ICS**
        - Dada la especificidad del servicio a prestar por parte del adjudicatario, exigida por el Centro Criptológico Nacional y en virtud del ENS, el adjudicatario deberá disponer de personal con experiencia y capacidad técnica necesaria para realizar el despliegue e implantación de sondas SAT-ICS.
        - Será necesario suministrar aquellos accesorios necesarios para el funcionamiento del equipo (Taps, cables RX con conectores industriales, etc.).
    - **SAT-INET**
        - Instalación de las sonda y configuraciones necesarias en la electrónica de red para enviar hacia la sonda el tráfico a analizar.
    - **SAT-DISTRIBUIDO GLORIA**
        - Mantenimiento actualizado del producto y el sistema operativo de los módulos desplegados a través de GLORIA CENTRAL.
        - Posibilidad actualización automática de reglas y de los componentes de GLORIA mediante un agente en cada instancia

que se encarga de comprobar si hay nueva configuración disponible en el nodo central.

- La comunicación se produce desde la instancia al nodo central para la descarga y aplicación de la actualización.
- Definición de los requerimientos técnicos sobre los que se instalará el sistema de alerta temprana.
- Preparación, documentación y despliegue del sistema de alerta temprana en formato físico dentro del CPD principal y secundarios.

- Garantizar el funcionamiento de la solución SAT-INET/SAT-ICS en caso de que hubiera alguna incidencia a causa del mal funcionamiento de los servidores instalados por el adjudicatario.
- El plan de backups, así como su definición, configuración e implementación deberán ser provistos por el adjudicatario, haciendo hincapié en los requisitos necesarios tanto de capacidad de disco como de máquina.
- Presentar, con una periodicidad negociada, un informe detallando las actuaciones ejecutadas en la plataforma de Aguas de Burgos
- Deberá realizar los trámites y gestiones necesarias para integrar el GLORIA de Aguas de Burgos con el GLORIA CENTRAL del CCN-CERT (SAT-Distribuido).
- Deberá integrar las sondas con el resto de equipamiento de Aguas de Burgos, incluyendo las herramientas del CCN-CERT de este pliego como el resto de Sistemas de la Información de Aguas de Burgos.

5.2.12 INES

INES (Informe de Estado de Seguridad en el ENS) es una solución desarrollada por el CCN-CERT para la gobernanza de la ciberseguridad, que permite evaluar regularmente el estado de la seguridad de los sistemas TIC de las entidades, organismos y organizaciones, además de su adecuación e implantación al Esquema Nacional de Seguridad (ENS) adaptándose a otros estándares o normas reguladoras en caso necesario.

Existen dos (2) modalidades de INES:

- Entidad matriz: entidad con entidades vinculadas o dependientes de ella.
- Entidad individual: una única entidad sin entidades vinculadas o dependientes.

El adjudicatario realizará las gestiones necesarias para implantar la plataforma INES, la

cual permitirá la recogida de información organizada, delegada y supervisada de forma continua a lo largo de todo el año. De tal manera, que Aguas de Burgos y el SOC puedan acceder, completar o consultar sus datos, en cualquier momento y ver su evolución.

Conviene reseñar que el siguiente paso sería la implantación de medidas de seguridad, a través de la solución AMPARO, así como completar la información en la herramienta ANA. El adjudicatario deberá asegurar la integración de estas herramientas, además de integrarlas con el resto de herramientas del CCN-CERT expuestas en este pliego y con el resto de Sistemas de Información de Aguas de Burgos.

5.2.13 AMPARO

AMPARO (Implantación de Seguridad y conformidad del ENS) es una solución desarrollada por el CCN-CERT para la gobernanza de la ciberseguridad de uso exclusivo para las Entidades de Certificación (EC) y Órganos de Auditoría Técnica (OAT). Incorpora diversas funcionalidades para facilitar los procesos de auditoría de conformidad, evaluando automáticamente la conformidad del sistema y facilitando la gestión de la Certificación de Conformidad.

AMPARO facilita la auditoría del ENS de los sistemas de información a través de un asistente que guía al auditor por todas las fases de la auditoría:

- Crear un Plan de Auditoría del sistema.
- Recorrer todas las medidas de seguridad recibiendo ayudas, evidencias propuestas, requisitos a comprobar y espacios para anotar observaciones.
- Incluir desviaciones en la implantación de las medidas en forma de No Conformidades.
- Crear un Informe de Auditoría a partir de las notas incluidas durante la auditoría.
- Notificar y gestionar los Certificados de Conformidad del ENS de la entidad.
- Gestionar las auditorías asociadas a la entidad y los expedientes de estas.

El adjudicatario realizará todas las tareas para la obtención de los certificados de conformidad del ENS de los sistemas de información de categoría BAJA.

Conviene reseñar que los pasos previos a la auditoría de Certificación de Conformidad se pueden llevar a cabo a través de la solución INES, así como completar la información en la herramienta ANA. El adjudicatario deberá asegurar la integración de estas herramientas, además de integrarlas con el resto de herramientas del CCN-CERT expuestas en este pliego y con el resto de Sistemas de Información de Aguas de Burgos.

5.2.14 ADA

ADA es una plataforma de análisis avanzado de malware, capaz de conseguir un análisis en profundidad similar al resultante de un proceso de investigación en detalle. Evolución natural de las capacidades de análisis dinámico (MARTA) y las capacidades de análisis estático (MARÍA), incluye capacidades adicionales orientadas al enriquecimiento de los resultados obtenidos. De esta forma, la solución permite controlar, gestionar y acceder a los resultados de todas las tecnologías de análisis que integra desde un solo interfaz unificado.

ADA analiza todo tipo de archivos (.zip, .pdf, documentos de office) y URLs para detectar ciberamenazas de tipo malware y comportamientos anómalos en los ficheros examinados.

Esta nueva plataforma integra las capacidades de las soluciones MARTA y MARÍA del CCN-CERT para realizar análisis avanzado de código dañino.

Dado que MARTA estaba integrado con GLORIA, el adjudicatario realizar las gestiones necesarias para la implantación de ADA en los sistemas de Aguas de Burgos. Deberá asegurar la integración de ADA y GLORIA, además de integrarlas con el resto de herramientas del CCN-CERT expuestas en este pliego y con el resto de Sistemas de Información de Aguas de Burgos.

5.2.15 ELSA

ELSA (Exposición Local y Superficie de Ataque) combina en una única solución de gestión de superficie de ataque (Attack Surface Management, ASM) la visibilidad extendida y capacidades de monitorización, corrección y supervisión continua, integrada con la última inteligencia de amenazas, de las vulnerabilidades y potenciales vectores de ataque que componen la superficie de ataque de una organización.

A diferencia de otras soluciones, se basa en la perspectiva de un atacante, en lugar de la de un defensor, identificando objetivos y evaluando riesgos en función de las oportunidades que se presenten para un atacante, y gracias a sus algoritmos de aprendizaje, es capaz de funcionar sin un inventario inicial por parte de la organización.

Ofrece un inventario completo, preciso y actualizado de todos los activos conectados a Internet, permitiendo detectar, evaluar y mitigar los riesgos de la superficie de ataque, incluyendo el riesgo asociado a los proveedores la seguridad de terceros, proporcionando:

- Fuente de información fidedigna: tener una visión completa permitirá detectar activos y exposiciones desconocidos, ayudando a reducir la superficie de ataque.
- Inventario autónomo alimentado por IA, mediante técnicas de ML: la mayoría de las organizaciones desconoce su superficie expuesta. ELSA es capaz de

solucionar este problema ya que no necesita ser alimentada por un inventario inicial que podría generar una falta de visibilidad de partes críticas. Gracias a sus algoritmos de aprendizaje y grafos de asociación es capaz, de forma autónoma y sin interacción alguna, de obtener todos los activos expuestos de un organismo.

- Descubrimiento y supervisión continua: las superficies de ataque cambian constantemente. ELSA analiza todo el espacio IPv4 hasta varias veces al día para descubrir todos sus activos conectados a Internet y realizar un seguimiento de los cambios que podrían suponer un riesgo.

- Clasificación, análisis y priorización: mitigar las amenazas requiere saber quién es responsable de un activo vulnerable. Con ELSA, incluso los activos previamente desconocidos se pueden rastrear para ayudar a una rápida corrección.

- Seguridad en tiempo real: una organización normal encuentra, de media, dos problemas de seguridad por día, mientras que los atacantes encuentran uno cada hora. ELSA mantiene actualizado su inventario de activos para que pueda mantenerse a la vanguardia.

El adjudicatario solicitará junto con Aguas de Burgos la participación en los escaneos por parte de ELSA, identificándolos desde los Sistemas de Información de Aguas de Burgos, junto con su integración con el resto de herramientas del CCN-CERT.

Aguas de Burgos podrá solicitar la participación en los escaneos por parte de ELSA. Los resultados de los escaneos serán analizados por la OTSI y/o el SOC, de forma que se implementen las medidas correctoras que sean necesarias en base a los resultados obtenidos.

5.2.16 IRIS

IRIS (Indicadores Relacionados para Informar de la Situación) es la herramienta de situational awareness, para el análisis del estado de la ciberseguridad. Permite conocer a tiempo real el estado de la ciberseguridad, tanto del sector público como el privado, ofreciendo una visión completa de la situación de la ciberamenaza a nivel nacional.

Gracias a la información que recoge unificando las herramientas comunes y compartidas, y plasmándolas de una forma visual y sencilla, IRIS permite una mayor rapidez en la detección de amenazas. Esto nos permite aumentar la ciberseguridad de las empresas reforzando sus capacidades de defensa y respuesta ante distintas amenazas e incidentes de ciberseguridad.

A través de sus diferentes paneles y mediante mapas interactivos, IRIS nos muestra toda la información a tiempo real. En los distintos puntos del mapa podemos encontrar alertas inmediatas de ciberataques, vulnerabilidades y riesgos en las AAPP, indicando

tipologías y peligrosidad.

Mediante su panel derecho, la herramienta de ciberseguridad IRIS nos permite visualizar los distintos tipos de organización que recoge, los sectores a los que pertenecen y el nivel de madurez de ciberseguridad de estas.

De esta forma, facilita la toma de decisiones en la gestión de incidentes sobre amenazas, centralizando y unificando la información del SAT y las herramientas LUCIA, CARMEN, GLORIA, MONICA, INES y PILAR del Centro Criptológico Nacional.

El adjudicatario deberá implementar la herramienta IRIS y asegurar su integración con el resto de herramientas del CCN-CERT expuestas en este pliego y con el resto de Sistemas de Información de Aguas de Burgos.

5.2.17 CARLA

CARLA es una solución validada y prescrita por el CCN-CERT de protección centrada en los datos, que permite que la información corporativa viaje protegida y bajo control en todo momento, minimizando la posibilidad de fugas de datos y aumentando el control de la organización sobre los mismos más allá de las defensas de protección perimetrales.

Incorpora una funcionalidad de cifrado de nivel alto para protección de información según lo indicado en la guía STIC-807, basado en el uso de un cifrado simétrico con AES 128 junto con técnicas de cifrado asimétrico con claves RSA-2048 bits para la protección de las claves AES.

Entre las funcionalidades de la solución CARLA del CCN-CERT se encuentra la protección constante mediante el cifrado de datos, la total trazabilidad y visibilidad de los accesos, la revocación de accesos en tiempo real, la compatibilidad con múltiples servicios y herramientas, así como la auditoría de accesos a la documentación compartida.

El adjudicatario deberá implementar la herramienta CARLA y asegurar su integración con el resto de herramientas del CCN-CERT expuestas en este pliego y con el resto de Sistemas de Información de Aguas de Burgos, con el fin de obtener los siguientes beneficios de esta solución:

- Evitar fugas de datos derivados de acciones inapropiadas.
- Facilitar la colaboración segura, pudiendo revocar accesos en tiempo real.
- Incrementar la seguridad en la nube aplicando cifrado de datos.
- Proteger frente a brechas de seguridad en la red que puedan suponer una posible exfiltración de datos.

- Facilitar el trabajo remoto seguro a través de un enfoque de seguridad centrada en los datos.
- Ayudar al cumplimiento de regulaciones ya que la información permanece cifrada y los accesos auditados.

El adjudicatario deberá realizar todas las tareas de instalación, implantación y administración de la herramienta CARLA en Aguas de Burgos, teniendo en cuenta que:

- Deberá realizar un estudio sobre qué modalidad de CARLA implementará, CARLA o CARLA GLOBAL. Será Aguas de Burgos quien apruebe la modalidad de implementación final a partir de dicho estudio.
- Deberá realizar un estudio de qué despliegue de CARLA realizará, on-premise o SaaS, y será Aguas de Burgos quien apruebe el despliegue final a partir de dicho estudio.
- Definición y ejecución de un plan de instalación, desinstalación y actualización de Carla Viewer/Desktop en los equipos de la infraestructura de red.
- Integración con las herramientas de Office 365, PDF y resto de herramientas del CCN-CERT.

5.3. Suministros de ciberseguridad

El detalle del equipamiento hardware actual de Aguas de Burgos se considera confidencial por razones de seguridad. Los licitadores podrán solicitar a Aguas de Burgos dicha información bajo el procedimiento indicado en el apartado “2.2 Infraestructura IT/OT” de este pliego.

Aguas de Burgos necesita actualizar y aumentar el equipamiento hardware existente ya que el actual se ha quedado insuficiente para soportar la implantación de todos los sistemas de información del proyecto DIGITAGUABUR y de las herramientas de ciberseguridad necesarias de este proyecto.

El adjudicatario durante el primer mes del proyecto, elaborará un plan de adecuación y mejoras de la infraestructura IT/OT. Este plan contendrá un análisis de la infraestructura actual y de la arquitectura de red en los CPD y otras ubicaciones, a partir del cual elaborará un plan de adecuación, optimización y mejoras necesarias a realizar en paralelo a la implantación del nuevo hardware, junto con su estimación económica.

En dicho plan, el adjudicatario deberá asegurar que todo el equipamiento que suministre garantice una total integración, por lo que todo el equipamiento será en la medida de lo posible del mismo fabricante (salvo recomendación en contra por cuestiones de seguridad) y la administración de todo ese equipamiento deberá poder realizarse en una

plataforma única, de forma que los dispositivos deberán disponer de una consola de configuración homogénea para la infraestructura IT y OT.

Este plan deberá estar enfocado en la optimización de la infraestructura IT y OT, cumpliendo con las necesidades de las normativas de seguridad (ENS, NIS2, etc.) complementando y mejorando las prescripciones técnicas del hardware identificado en este apartado. Como resultado de este plan, podrán surgir prescripciones técnicas que sean incorporadas en contrataciones y pliegos a licitar por Aguas de Burgos.

Todo el material suministrado debe ser nuevo, de primer uso y no descatalogado. El hardware debe estar catalogado expresamente por el fabricante como destinado al ámbito de EMPRESA o PROFESIONAL. Todos los equipos a suministrar deberán demostrar una fecha de fin de vida posterior a los años de garantía solicitados en este pliego.

No serán facturables los dispositivos físicos que se recogen en este apartado, y que, conforme a las conclusiones del análisis y plan de adecuación realizado por el adjudicatario, no se suministren e implanten, debido a una reducción del número de unidades, la virtualización total o parcial de los dispositivos, o cualquier otra circunstancia que lo aconseje. Para las conexiones entre switches SAN o LAN y el resto de los componentes, el adjudicatario utilizará cables de conexión tipo DAC para la conexión con cada componente dentro de cada CPD y transceptores para la conexión entre CPDs y edificios. Se incluye un número mínimo aproximado de transceptores que podría ser incrementado en caso de que las configuraciones de comunicación entre dispositivos así lo requirieran.

El adjudicatario deberá tener en cuenta que toda la infraestructura hardware a implantar en Aguas de Burgos se diseña a una velocidad de 10/25 GbE, por lo que todos los componentes hardware y software de la red de comunicaciones deberán ir acorde a este requisito de velocidad, evitando los cuellos de botella en la red. Todo el hardware ofrecido constituirá un mismo sistema que dará servicio de conectividad a los dispositivos de la organización, para maximizar las prestaciones de baja latencia, máximo rendimiento y facilitar la gestión de estos, todo el hardware ofrecido deberá garantizar una completa integración. Todo el material, conectores, transceptores de fibra monomodo y adaptadores necesarios incluidos, debe ser nuevo y original del fabricante.

Las herramientas de gestión de red, proxies, firewalls deben cumplir con los requisitos del Esquema Nacional de Seguridad mediante su inclusión con categoría ALTA en la última guía de CCN-STIC- 105 o demostrar haber comenzado formalmente el proceso de certificación con el CCN a la publicación por parte del adjudicatario.

5.3.1 Servidores y almacenamiento

El adjudicatario deberá suministrar, instalar y configurar en las instalaciones de Aguas de Burgos, como máximo y teniendo en cuenta las conclusiones del plan de adecuación y mejoras de la infraestructura IT/OT, los siguientes elementos hardware.

NÚMERO DE ELEMENTOS HARDWARE		
CANTIDAD MÁXIMA	**UBICACIÓN**	**ELEMENTO**
10	5 en CPD Principal y 5 en CPD Secundario	Servidores físicos (hosts)
2	1 en CPD Principal y 1 en CPD Secundario	Sistemas almacenamiento SAN
4	2 en CPD Principal y 2 en CPD Secundario	Switches SAN
2	1 en CPD Principal y 1 en CPD Secundario	Servidores almacenamiento NAS

Los requerimientos mínimos de los elementos anteriores, pudiendo ser superiores, son los que se incluyen a continuación. Cada una de las siguientes tablas, recoge los requisitos de cada unidad de los elementos a suministrar.

Durante el primer mes de ejecución del contrato, el adjudicatario revisará la infraestructura de los racks, para elegir modelo/s compatibles con las dimensiones de cada uno de los racks, y la compatibilidad entre los mismos de cara a proveer por parte del adjudicatario, de forma justificada y consensuada con Aguas de Burgos, cableado y transceptores para conexiones a la más alta velocidad.

TABLA DE REQUERIMIENTOS	
SERVIDORES FÍSICOS (HOSTS)	
Formato	Bastidor 2U
Procesamiento	2 CPU Intel Xeon Gold 5418Y o superior 24 cores. 2 GHz de frecuencia básica del procesador. 45 MB de caché. 24 núcleos.
Memoria	Memoria RAM instalada mínima de 1 TB. DDR5-4800, máxima velocidad permitida por el procesador. 32 ranuras de memoria. No se admitirán módulos de memoria de menos de 64 GB.
Almacenamiento interno	Controladora RAID. 8 canales discos SAS y SATA.
Discos duros arranque	2 discos 480 GB M.2 NVMe SSDs en RAID1
Adaptador de red	2 adaptadores de 2 puertos compatibles en los dos extremos para su conexión con switches (misma marca que el dispositivo). El adjudicatario utilizará cables de conexión tipo DAC para la conexión con cada switch SAN.
Seguridad	TPM 2.0 o superior. Kit de bisel con cierre y detección de intrusión.

Alimentación	Doble fuente de alimentación, redundantes e intercambiables en caliente, con conectividad a PDU del RACK.
Ventilación	4 ventiladores
Gestión de infraestructura	Gestión de red avanzada remota fuera de línea: iLO/iDRAC/IPMI con acceso remoto licenciado completo.
Cableado	Cableado y transceptores para conexiones a la más alta velocidad.
Garantía	Conforme a lo indicado en el apartado 5.3.10

Para el sistema de almacenamiento SAN (MSA), éste deberá ir acompañado de una licencia que al menos como característica principal le permita realizar 512 Snapshots y replicas remotas con una licencia de tipo advanced.

TABLA DE REQUERIMIENTOS	
SISTEMAS ALMACENAMIENTO SAN	
Formato	Bastidor 2U
Protocolo host	iSCSI (25 GbE)
Almacenamiento	Doble controladora, redundantes e intercambiables en caliente. 4 puertos host por controladora, 8 puertos host por array.
Adaptador de red	El adjudicatario utilizará cables de conexión tipo DAC para la conexión con cada switch SAN en vez de transceptores.
Discos duros	18 discos 3,84 TB SAS 12G SFF (2,5'') intercambiables en caliente. Ampliable a 24 discos SFF
RAID	MSA-DP+ o equivalente
Alimentación	Doble fuente de alimentación, redundantes e intercambiables en caliente, con conectividad a PDU del RACK.
Cableado	Cableado para conexiones a la más alta velocidad.
Garantía	Conforme a lo indicado en el apartado 5.3.10

TABLA DE REQUERIMIENTOS	
SWITCHES SAN	
Formato	Bastidor 1U – Anchura media (2 switches por U)
Protocolo	iSCSI (25 GbE)

Puertos	18 puertos SFP28 4 puertos QSFP28
Adaptadores de red	El adjudicatario utilizará cables de conexión tipo DAC para la conexión con cada switch SAN 15 conexiones (5 para conexión a cada host, 4 para conexión a almacenamiento SAN, 1 servidor copias primario, 1 sistema backup en cinta, 1 entre switches, 3 de replicación, repuesto y otros usos). Misma marca que el dispositivo.
Velocidad de puerto	25 GbE para conexiones con SAN y hosts
Gestión de infraestructura	Gestión interna y externa. Gestión centralizada que permita la administración de todos los switches de este contrato.
Cableado	Cableado para conexiones a la más alta velocidad.
Alimentación	Adaptada para SAI y Corriente eléctrica, cableado necesario para ambas, con conectividad a PDU del RACK.
Configuración	Configuración redundante entre hosts y almacenamiento SAN.
Garantía	Conforme a lo indicado en el apartado 5.3.10

TABLA DE REQUERIMIENTOS	
ALMACENAMIENTO NAS	
Formato	Bastidor 2U
Sistema operativo	Microsoft Windows Server IoT 2022 for Storage Standard Edition preinstalado
Procesamiento	Intel® Xeon-Bronze 3408U (4.ª generación)
Memoria	16Gb DDR5
Almacenamiento	32 TB de capacidad. 8 HDD 4 TB SAS 12G 7200 rpm LFF estándar (3,5 pulgadas). 4 bahías disponibles para ampliación.
Replicación	Replicación del sistema de archivos distribuido (DFS-R) de Microsoft para conjuntos de datos de hasta 100 TB
Adaptador de red	2 adaptadores de 2 puertos 25GbE SFP28 con los SFPs compatibles en los dos extremos para su conexión con switches (misma marca que el dispositivo). El adjudicatario utilizará cables de conexión tipo DAC para la conexión con cada switch SAN
Alimentación	Doble fuente de alimentación, redundantes e intercambiables en caliente, con conectividad a PDU del RACK.
Ventilación	Doble ventilación
Gestión de infraestructura	Consola de gestión preinstalada.

Cableado	Cableado y transceptores para conexiones a la más alta velocidad.
Garantía	Conforme a lo indicado en el apartado 5.3.10

Ejemplos de dispositivos con los anteriores requerimientos técnicos:

- Servidores físicos (hosts): HPE Proliant DL380 Gen11 5418Y
- Sistemas almacenamiento SAN: HPE MSA 2062
- Switches SAN: HPE SN2010M 25 GbE
- Servidores almacenamiento NAS: HPE StoreEasy 1670 32 TB SAS

5.3.2 Sistemas de alimentación ininterrumpida

El adjudicatario deberá suministrar, instalar y configurar en las instalaciones de Aguas de Burgos, como máximo y teniendo en cuenta las conclusiones del plan de adecuación y mejoras de la infraestructura IT/OT, los siguientes elementos hardware.

NÚMERO DE ELEMENTOS HARDWARE		
CANTIDAD MÁXIMA	**UBICACIÓN**	**ELEMENTO**
2	1 en CPD Principal y 1 en CPD Secundario (rack servidores)	Sistema de alimentación ininterrumpida con módulo de baterías adicionales
6	Diversas ubicaciones (racks comunicaciones)	Sistema de alimentación ininterrumpida
4	2 en CPD Principal y 2 en CPD Secundario (rack servidores)	2 PDU (Unidad de Distribución de Energía) , cada uno para SAI y corriente eléctrica.

Los requerimientos mínimos de los elementos anteriores, pudiendo ser superiores, son los que se incluyen a continuación. Cada una de las siguientes tablas, recoge los requisitos de cada unidad de los elementos a suministrar.

Durante el primer mes de ejecución del contrato, el adjudicatario revisará la infraestructura de los racks, para elegir modelo/s compatibles con las dimensiones de cada uno de los racks, y la compatibilidad entre los mismos de cara a proveer por parte del adjudicatario, de forma justificada y consensuada con Aguas de Burgos. El adjudicatario deberá asegurar la tolerancia particular para la compatibilidad con otros equipos conectados a estos Sistemas de Alimentación Ininterrumpida.

TABLA DE REQUERIMIENTOS		
SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA		
Formato	Bastidor 2U del SAI + Bastidor 2U MODULO ADICIONAL DE BATERIAS	
Dimensiones	Compatible con Armario de tipo Rack HPE 19” 42u 600X1075 mm de fondo.	
Entrada eléctrica	Rango de Tensión	100V nominal = 80V – 128V 120V nominal = 89V – 159V 208V nominal = 160V – 163V 230V nominal = 160V – 294V
	Frecuencia	50/60 Hz
	Eficiencia en línea	94%
Salida eléctrica	En batería regulación	±5% de voltaje nominal
	Regulación en línea	-10% a +6% de voltaje nominal
	Forma de onda de tensión	Onda sinusoidal
	Protección de salida	Detección y control de sobrecarga por firmware
Batería (voltaje)	R/T2200 = 48V R/T3000 = 72V	
Licencia Software	Incluida	
Conectividad de red	Incluida	
Software de monitorización	Software para Windows, Linux y Mac / APP para iOS y Android / Portal WEB	
Garantía	Conforme a lo indicado en el apartado 5.3.10	

TABLA DE REQUERIMIENTOS		
SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA (PARA RACKS DE COMUNICACIONES)		
Formato	Bastidor 2U del SAI	
Dimensiones	Compatible con armarios de comunicaciones de cada ubicación elegida por Aguas de Burgos.	
Entrada eléctrica	Rango de Tensión	100V nominal = 80V – 128V 120V nominal = 89V – 159V 208V nominal = 160V – 163V 230V nominal = 160V – 294V
	Frecuencia	50/60 Hz
	Eficiencia en línea	94%
Salida eléctrica	En batería regulación	±5% de voltaje nominal

	Regulación en línea	-10% a +6% de voltaje nominal
	Forma de onda de tensión	Onda sinusoidal
	Protección de salida	Detección y control de sobrecarga por firmware
Batería (voltaje)	R/T2200 = 48V R/T3000 = 72V	
Licencia Software	Incluida	
Conectividad de red	Incluida	
Software de monitorización	Software para Windows, Linux y Mac / APP para iOS y Android / Portal WEB	
Garantía	Conforme a lo indicado en el apartado 5.3.10	

Ejemplos de dispositivos con los anteriores requerimientos técnicos:

- Sistema de alimentación ininterrumpida con módulo de baterías adicionales: HPE R/T2200 G5 UPS, R/T3000 G5 UPS, and ERM
- Sistema de alimentación ininterrumpida (para racks de comunicaciones): equivalente al anterior sin módulo de baterías adicionales.

Para asegurar la máxima disponibilidad, eficiencia energética y protección de los equipos en los racks, para los siguientes requisitos en cuanto a las PDU (Unidad de Distribución de Energía), el adjudicatario deberá asegurar su compatibilidad a los equipos adquiridos junto con los SAIs, teniendo en cuenta los puntos de la siguiente tabla de requerimientos. Solo se colocarán 2 PDUs por cada CPD. El resto de racks no necesitarán de PDU.

TABLA DE REQUERIMIENTOS	
PDU (Unidad de Distribución de Energía)	
Montaje y Tamaño	El adjudicatario deberá asegurar que la PDU se ajuste físicamente a cada rack y que tenga el tipo de montaje adecuado (horizontal o vertical).
Número de tomas de corriente	El adjudicatario deberá determinar cuántos dispositivos se conectarán a la PDU y elegir una que tenga suficientes tomas de corriente para las necesidades actuales y futuras.
Capacidad de carga	El adjudicatario deberá asegurar que la PDU pueda manejar la carga total que va a suministrar el UPS. También, deberá verificar la capacidad de carga en amperios (A) y vatios (W) de la PDU.
Voltaje y tipo de corriente	El adjudicatario deberá confirmar que la PDU sea compatible con el voltaje y el tipo de corriente (AC) que el SAI está proporcionando, se estima un voltaje de salida de 208V o 230V AC.
Conectores y tipos de enchufes	El adjudicatario deberá revisará el tipo de conectores necesarios para los equipos y asegurará que la PDU tenga los enchufes adecuados (C13 o C19)

Protección	El adjudicatario deberá verificar que la PDU ofrezca protección contra sobrecargas y cortocircuitos, así como otras características de seguridad que puedan ser relevantes para los equipos.
Redundancia	Cada rack debe tener dos PDUs: una conectada al SAI y la otra conectada a una fuente de energía alterna (corriente de red). Las PDUs deben tener capacidad para recibir energía de dos fuentes distintas (una del SAI y otra de la corriente de red), proporcionando redundancia en caso de fallo de una de las fuentes de energía.
Balance de Carga:	Las PDUs deben permitir una distribución uniforme de la carga eléctrica entre ellas para evitar sobrecargas y optimizar la eficiencia energética.
Licencia Software	Incluida
Conectividad de red	Incluida
Software de monitorización y gestión	Deben contar con capacidades de monitoreo y gestión para supervisar y ajustar la distribución de la carga en tiempo real. Software para Windows, Linux y Mac / APP para iOS y Android / Portal WEB
Garantía	Conforme a lo indicado en el apartado 5.3.10

El adjudicatario deberá asegurar que las PDUs seleccionadas cumplan con todas las normativas y certificaciones de seguridad pertinentes.

5.3.3 Comunicaciones

Aguas de Burgos ha realizado un estudio de los dispositivos de comunicación existentes en los CPD y otras ubicaciones de las redes IT/OT, que como resultado plantea la renovación y reorganización de dichos elementos de comunicación, a fin de mejorar el rendimiento de la red y su seguridad.

El análisis de la infraestructura actual y de la arquitectura de red en los CPD y otras ubicaciones que realizará el adjudicatario al inicio del proyecto, deberá incluir recomendaciones que aumenten la seguridad y rendimiento, que utilizando como base el hardware solicitado, sin excluir otras alternativas.

Todo el equipamiento suministrado por el adjudicatario deberá ser nuevo y no descatalogado, cumpliendo con todos los requisitos técnicos del presente PPT. Todos los equipos a suministrar deberán demostrar una fecha de fin de vida posterior a los años de mantenimiento solicitados en este pliego.

Todo el hardware ofrecido constituirá un mismo sistema que dará servicio de conectividad a los dispositivos de la organización, para maximizar las prestaciones de baja latencia, máximo rendimiento y facilitar la gestión de estos, todo el hardware ofrecido deberá ser del mismo fabricante. Todo el material, conectores, transceptores de fibra monomodo y adaptadores necesarios incluidos, debe ser nuevo y original del fabricante.

Con el fin de reducir la complejidad e integrabilidad de la solución, se valorará que todos los elementos de la solución sean del mismo fabricante.

Los switches podrán gestionarse de forma independiente mediante entorno gráfico o línea de comando y también a través de un controlador on-premise centralizado mediante entorno gráfico. Las configuraciones en el dispositivo deberán:

- Ser fácilmente guardadas o restauradas a través de GUI y CLI a / desde el PC local, la gestión centralizada o almacenamiento USB.
- Proporcionar archivos de configuración de comandos CLI legibles con un bloc de notas.
- El sistema propuesto deberá proporcionar acceso a su gestión a través de como mínimo:
    - GUI usando HTTP o HTTPS con la posibilidad de modificar el puerto de acceso.
    - Consola CLI a través del puerto de consola, SSHv2, Telnet o el dashboard del GUI.

Durante el primer mes de ejecución del contrato, el adjudicatario revisará la infraestructura de los racks, para elegir modelo/s compatibles con las dimensiones de cada uno de los racks, y la compatibilidad entre los mismos de cara a proveer por parte del adjudicatario, de forma justificada y consensuada con Aguas de Burgos, cableado y transceptores para conexiones a la más alta velocidad.

El adjudicatario deberá suministrar, instalar y configurar en las instalaciones de Aguas de Burgos, como máximo y teniendo en cuenta las conclusiones del plan de adecuación y mejoras de la infraestructura IT/OT, los siguientes elementos hardware, incluyendo todo el cableado necesario para las interconexiones y garantizando que suministrará siempre equipos de la misma gama y marca, de forma que puedan ser gestionados desde un software central que será incluido junto con los switches.

NÚMERO DE ELEMENTOS HARDWARE		
CANTIDAD MÁXIMA	**UBICACIÓN**	**ELEMENTO**
9	Diversas ubicaciones	Switches LAN de 24 puertos RJ45 y 4 SFP+
4	2 en CPD Principal y 2 en CPD Secundario	Switches LAN de 24 puertos SFP+
5	3 en CPD Principal y 2 en CPD Secundario	Switches LAN de 48 puertos RJ45 y 4 SFP+

Los requerimientos mínimos de los elementos anteriores, pudiendo ser superiores, son los que se incluyen a continuación. Cada una de las siguientes tablas, recoge los requisitos de cada unidad de los elementos a suministrar.

TABLA DE REQUERIMIENTOS	
SWITCHES LAN DE 24 PUERTOS RJ45 Y 4 SFP+	
Formato	Bastidor 1U
Puertos	24 puertos RJ-45 10/100/1000BASE-T PoE 4 puertos SFP+ 10GbE, o tecnología superior y compatible
Transceptores	1 transceptores SFP+ por Switch larga distancia. Misma marca que el dispositivo.
Alimentación	Adaptada para SAI y Corriente eléctrica, cableado necesario para ambas, con conectividad a PDU del RACK.
Gestión de infraestructura	Gestión interna y externa. Gestión centralizada que permita la administración de todos los switches de este contrato.
Cableado	Cableado y transceptores para conexiones a la más alta velocidad.
Configuración	Todos los switches serán de la misma marca y gama, con configuración compatible entre todos ellos.
Garantía	Conforme a lo indicado en el apartado 5.3.10

TABLA DE REQUERIMIENTOS	
SWITCHES LAN DE 24 PUERTOS SFP+	
Formato	Bastidor 1U
Puertos	24 SFP+ 10GbE, con puertos adicionales de tecnología superior y compatible al resto de la infraestructura de comunicaciones.
Conexiones de Red	El adjudicatario utilizará cables de conexión tipo DAC para la conexión de los componentes con cada switch LAN.
Alimentación	Adaptada para SAI y Corriente eléctrica, cableado necesario para ambas, con conectividad a PDU del RACK.
Gestión de infraestructura	Gestión interna y externa. Gestión centralizada que permita la administración de todos los switches de este contrato.
Cableado	Cableado y transceptores para conexiones a la más alta velocidad.
Configuración	Todos los switches serán de la misma marca y gama, con configuración compatible entre todos ellos.

Garantía	Conforme a lo indicado en el apartado 5.3.10

TABLA DE REQUERIMIENTOS	
SWITCHES LAN DE 48 PUERTOS RJ45 Y 4 SFP+	
Formato	Bastidor 1U
Puertos	48 puertos RJ-45 10/100/1000BASE-T PoE 4 puertos SFP, o tecnología superior y compatible
Adaptador de red	El adjudicatario utilizará cables de conexión tipo DAC para la conexión con cada componente necesario, con el fin de conseguir la mayor velocidad posible sin necesidad de usar transceptores en los casos en los que sea posible.
Alimentación	Adaptada para SAI y Corriente eléctrica, cableado necesario para ambas, con conectividad a PDU del RACK.
Gestión de infraestructura	Gestión interna y externa. Gestión centralizada que permita la administración de todos los switches de este contrato.
Cableado	Cableado y transceptores para conexiones a la más alta velocidad.
Configuración	Todos los switches serán de la misma marca y gama, con configuración compatible entre todos ellos.
Garantía	Conforme a lo indicado en el apartado 5.3.10

Ejemplos de dispositivos con los anteriores requerimientos técnicos:

- Switches LAN de 24 puertos RJ45 Y 4 SFP+: HPE Aruba 6300M (JL662A)
- Switches LAN de 24 puertos SPF+: HPE CX 8100 24x10G SFP+ 4 x 40/100G QSFP28
- Switches LAN de 48 puertos RJ45 Y 4 SFP+: HPE Aruba CX 6100

5.3.4 Firewalls

Los cortafuegos deberán gestionar la seguridad para el ecosistema convergente de IT/OT de Aguas de Burgos garantizando un rendimiento eficiente y seguro para ambas redes.

Se plantea proporcionar a la infraestructura de un servicio de seguridad basado en:

- Firewall perimetral, con capacidades de IPS, IDS y balanceador web.
- Firewall interno para segmentar adecuadamente tanto en el CPD principal como

en el de respaldo. Es necesario disponer de un servicio UTM en los firewalls.

Los cortafuegos perimetrales e internos deben ser de distintos fabricantes (biodiversidad) para garantizar un grado más de seguridad, ambos no deben ejercer las mismas funciones dentro de la arquitectura. Ambos cortafuegos deberán ser totalmente integrables con el resto de herramientas del CCN-CERT de este pliego (SIEM, Sondas, etc.), teniendo presente el adjudicatario el análisis de la infraestructura hardware actual, elaboración del plan de adecuación y propuestas de mejoras para la implantación del nuevo hardware y optimización de la infraestructura IT y OT.

Las configuraciones en el dispositivo deberán:

- Ser fácilmente guardadas o restauradas a través de GUI y CLI a / desde el PC local, la gestión centralizada o almacenamiento USB.
- Proporcionar archivos de configuración de comandos CLI legibles con un bloc de notas.
- El sistema propuesto deberá proporcionar acceso a su gestión a través de como mínimo:
    - GUI usando HTTP o HTTPS con la posibilidad de modificar el puerto de acceso.
    - Consola CLI a través del puerto de consola, SSHv2, Telnet o el dashboard del GUI.

El adjudicatario garantizará que los firewall ofertados no sufrirán degradación conforme se vayan habilitando perfiles de seguridad relacionados con la protección, es decir, tanto a nivel de prevención frente a amenazas conocidas (IPS, Antivirus, Antispyware, URL Filtering, etc.) como frente a amenazas desconocidas (Sandboxing), de forma que sea predecible el impacto en el rendimiento de la solución en la activación progresiva de estas funciones de seguridad, independientemente del número de ellas.

La arquitectura hardware de la plataforma deberá permitir la aplicación paralela de diferentes módulos de seguridad, asegurando una sola inspección por cada paquete. No deberá haber mayor impacto por el hecho de habilitar más o menos firmas en los servicios de inspección de amenazas conocidas (IPS, Antivirus, Antispyware, DNS, URL Filtering…). El servicio de seguridad debe de poder filtrar las peticiones y servicios, así como permitir entornos de conexión VPN.

El adjudicatario seguirá los procedimientos estándar en lo que se refiere a buenas prácticas de instalación y configuración de sistemas y dispositivos, entre otros:

- Instalación en entornos aislados seguros.
- Instalaciones mínimas.

- Actualización de software.
- Desactivación de servicios no necesarios.
- Reforzamiento.
- Elección de la opción de configuración más segura frente a la más cómoda en caso de conflicto.
- Aplicación de principios de seguridad: seguridad en profundidad, principio de mínimo privilegio, etc.
- Inspección.
- Diseño de procedimientos de inspección, mantenimiento, documentación, recuperación frente a desastres, auditoría, actualización, etc.

Es necesario que todos los elementos que conforman el entorno físico de los cortafuegos (switches, enrutadores, SAI, prevención de incendios, etc.) estén sometidos a los mismos requisitos de seguridad física que define la política de seguridad para los cortafuegos.

Toda la configuración, gestión, procedimientos y documentación de los cortafuegos se hará acorde a las pautas marcadas por la guía CCN STIC 408 de Seguridad Perimetral Cortafuegos, en lo que aplique a la arquitectura diseñada para Aguas de Burgos por parte del adjudicatario, con el fin de cumplir con el nivel más alto de certificación del ENS y el NIS2, para lo cual el tipo de arquitectura de protección del perímetro a plantear deberá ser de tipo APP-5 o superior, según la guía CCN STIC 811 de Interconexión en el ENS. Aguas de Burgos podrá valorar si el adjudicatario provee de una solución de virtualización, de forma que el coste de equipos físicos sea más atractivo, sin perder prestaciones de eficiencia, seguridad y redundancia, cumpliendo además con lo especificado en nivel ALTO de ENS y el NIS2 y con las guías CCN STIC mencionadas en este punto.

Una vez preparados los firewalls, con acceso a la gestión y con las actualizaciones de firmware, el adjudicatario procederá a la migración y optimización de las reglas actuales, creación de alias, NAT, interfaces y resto de configuraciones del sistema de firewalls de este pliego. Este proceso deberá garantizar al menos el mismo nivel de acceso actual, pero mejorando la seguridad adaptando las reglas a un firewall de capa 7.

Adicionalmente, el adjudicatario implementará las políticas de QoS de cara a garantizar la disponibilidad de las redes WAN y su correcto balanceo, así como unas reglas genéricas que ayuden a la priorización del tráfico de más importante a menos.

El adjudicatario implementará el acceso con Múltiple Factor de Autenticación (MFA) mediante aplicación móvil para los Administradores del sistema. En general, esta propuesta deberá ir encaminada a que Aguas de Burgos pueda seguir prestando sus servicios más críticos, garantizar los accesos necesarios a los diferentes sistemas con

los mínimos permisos y privilegios necesarios, así como proteger las infraestructuras ante posibles ataques tanto externos como internos.

Durante el primer mes de ejecución del contrato, el adjudicatario revisará la infraestructura de los racks, para elegir modelo/s compatibles con las dimensiones de cada uno de los racks, y la compatibilidad entre los mismos de cara a proveer por parte del adjudicatario, de forma justificada y consensuada con Aguas de Burgos, cableado y transceptores para conexiones a la más alta velocidad.

El adjudicatario deberá suministrar, instalar y configurar en las instalaciones de Aguas de Burgos, como máximo y teniendo en cuenta las conclusiones del plan de adecuación y mejoras de la infraestructura IT/OT, los siguientes elementos hardware

NÚMERO DE ELEMENTOS HARDWARE		
CANTIDAD MÁXIMA	**UBICACIÓN**	**ELEMENTO**
4	2 en CPD Principal y 2 en CPD Secundario	Firewalls perimetrales
4	2 en CPD Principal y 2 en CPD Secundario	Firewalls internos

Los requerimientos mínimos de los elementos anteriores, pudiendo ser superiores, son los que se incluyen a continuación. Cada una de las siguientes tablas, recoge los requisitos de cada unidad de los elementos a suministrar.

TABLA DE REQUERIMIENTOS	
FIREWALLS PERIMETRALES	
Formato	Bastidor 1U
Interfaces	8 puertos RJ-45 10/100/1000BASE-T PoE. 4 interfaces 10GbE de conexiones SFP+. Bahías ampliables de RJ45 o SFP+
Adaptadores de red	El adjudicatario utilizará cables de conexión tipo DAC para la conexión con cada switch dentro de cada CPD.
CPU, RAM y HD	Recursos dedicados e independientes para el plano de control y para el de servicio, con el objetivo de poder garantizar que una sobrecarga del hardware destinado a prestar el servicio no afecte a la gestión y viceversa.
IDS	Integrado en el dispositivo
IPS	Integrado en el dispositivo
EDR	conectados con el sistema de protección de sistemas operativos

XDR	conectados con el sistema de protección de sistemas operativos
Alimentación	Adaptada para SAI y Corriente eléctrica, cableado necesario para ambas, con conectividad a PDU del RACK.
Cableado	Cableado y transceptores para conexiones a la más alta velocidad.
Garantía	Conforme a lo indicado en el apartado 5.3.10
Configuración	Activo/pasivo
Capacidades avanzadas de Seguridad	UTM, Unificado para control web, aplicativo y antivirus, Web Filtering, Antispam, Desencriptado SSL, WAF, routing., etc… Capacidad de VPN Capacidad de balanceo LAN

TABLA DE REQUERIMIENTOS	
FIREWALLS INTERNOS	
Formato	Bastidor 1U
Interfaces	8 puertos RJ-45 10/100/1000BASE-T PoE. 4 interfaces 10GbE de conexiones SFP+. Bahías ampliables de RJ45 o SFP+
Adaptadores de red	El adjudicatario utilizará cables de conexión tipo DAC para la conexión con cada switch dentro de cada CPD.
CPU, RAM y HD	Recursos dedicados e independientes para el plano de control y para el de servicio, con el objetivo de poder garantizar que una sobrecarga del hardware destinado a prestar el servicio no afecte a la gestión y viceversa.
IDS	Integrado en el dispositivo
IPS	Integrado en el dispositivo
EDR	Conectados con el sistema de protección de sistemas operativos
XDR	Conectados con el sistema de protección de sistemas operativos
Alimentación	Adaptada para SAI y Corriente eléctrica, cableado necesario para ambas, con conectividad a PDU del RACK.
Cableado	Cableado y transceptores para conexiones a la más alta velocidad, compatibles con el resto de elementos hardware de la red.
Garantía	Conforme a lo indicado en el apartado 5.3.10
Capacidades avanzadas de Seguridad	UTM, Unificado para control web, aplicativo y antivirus, Web Filtering, Antispam, Desencriptado SSL, WAF, routing., etc… Capacidad de VPN Capacidad de balanceo LAN

5.3.5 Sondas

Las sondas SAT-ICS y SAT-INET pueden ser servidores físicos dedicados para las sondas, o bien virtualizados, en cuyo caso se necesitará una interfaz física dedicada para enviar el port mirror del tráfico que se quiera monitorizar.

Durante la fase de adecuación e implantación, el adjudicatario realizará un estudio de ambas alternativas, cuyas conclusiones serán tenidas en cuenta por Aguas de Burgos de cara a la elección de la solución a implantar, pero sin que dichas conclusiones sean vinculantes para Aguas de Burgos.

En caso de elegir soluciones virtualizadas, no serán facturables los dispositivos físicos que se recogen en la siguiente tabla a modo de previsión.

NÚMERO DE ELEMENTOS HARDWARE		
CANTIDAD MÁXIMA	**UBICACIÓN**	**ELEMENTO**
2	1 en CPD Principal y 1 en CPD Secundario	Sondas SAT-ICS
2	1 en CPD Principal y 1 en CPD Secundario	Sondas SAT-INET

Los requerimientos mínimos de los elementos anteriores, serán los adecuados a la infraestructura IT y OT de Aguas de Burgos, y a las recomendaciones y requerimientos del CCN-CERT. Cada una de las siguientes tablas, recoge los requisitos de cada unidad de los elementos a suministrar.

TABLA DE REQUERIMIENTOS	
SONDA SAT-INET	
Formato	Bastidor 1U o Virtual
Procesador	16 núcleos
Memoria	32 GB de RAM
Almacenamiento	2 Discos Duros 146GB SAS, en RAID 1 (Espejo) en caso de dispositivo físico
Red - Interfaz/ces de análisis (tantas como redes a analizar)	Tarjeta/s de red Gigabit Ethernet de tecnología Intel (driver e1000e o igb) en caso de dispositivo físico
Red - Interfaz de gestión	Tarjeta de red Gigabit Ethernet con distinto driver que la/s interfaz/ces de análisis (p.e. Broadcom…) en caso de dispositivo físico
Sistema Operativo	Hardware compatible con CentOS 7.3 (Instalado por el CCN-CERT)
Licencia Sistema Operativo	Windows/Linux incluida

Configuración	Gestión y administración de la sonda realizado por el personal técnico del CCN-CERT, según
Garantía	Conforme a lo indicado en el apartado 5.3.10 en caso de dispositivo físico

TABLA DE REQUERIMIENTOS	
SONDA SAT-ICS	
Formato	Bastidor 1U o Virtual
Procesador	16 núcleos
Memoria	32 GB de RAM
Almacenamiento	2 Discos Duros 146GB SAS, en RAID 1 (Espejo) en caso de dispositivo físico
Red - Interfaz/ces de análisis (tantas como redes a analizar)	Tarjeta/s de red Gigabit Ethernet de tecnología Intel (driver e1000e o igb) en caso de dispositivo físico
Red - Interfaz de gestión	Tarjeta de red Gigabit Ethernet con distinto driver que la/s interfaz/ces de análisis (p.e. Broadcom…) en caso de dispositivo físico
Sistema Operativo	Hardware compatible con CentOS 7.3 (Instalado por el CCN-CERT)
Garantía	Conforme a lo indicado en el apartado 5.3.10 en caso de dispositivo físico

5.3.6 Copias de seguridad

El adjudicatario deberá suministrar, instalar y configurar en las instalaciones de Aguas de Burgos, como máximo y teniendo en cuenta las conclusiones del plan de adecuación y mejoras de la infraestructura IT/OT, los siguientes elementos hardware.

Durante el primer mes de ejecución del contrato, el adjudicatario revisará la infraestructura de los racks, para elegir modelo/s compatibles con las dimensiones de cada uno de los racks, y la compatibilidad entre los mismos de cara a proveer por parte del adjudicatario, de forma justificada y consensuada con Aguas de Burgos, cableado y transceptores para conexiones a la más alta velocidad.

NÚMERO DE ELEMENTOS HARDWARE		
CANTIDAD MÁXIMA	**UBICACIÓN**	**ELEMENTO**
1	CPD Principal	Sistema de backup en disco

1	CPD Principal	Sistema de backup en cinta

Los requerimientos mínimos de los elementos anteriores, pudiendo ser superiores, son los que se incluyen a continuación. Cada una de las siguientes tablas, recoge los requisitos de cada unidad de los elementos a suministrar.

TABLA DE REQUERIMIENTOS	
SISTEMA DE BACKUP EN DISCO	
Formato	2U
Numero de discos	8
Procesadores	Intel® Xeon® Silver 4514Y o superior 16 núcleos de procesador 2,00 GHz de velocidad del procesador 30 MB L3 de Caché del procesador
Memoria	32 GB de memoria DDR5 RDIMM
Tipo de Unidad	Opciones para discos duros de gran formato (LFF), incluyendo soporte para NVMe.
Discos duros	12 discos LFF 8 TB HDD, SATA 7200 rpm (3,5'') intercambiables en caliente.
Interfaz	SATA.
Interfaz de red	2 puertos SFP28 25GbE, o tecnología superior y compatible con SPF28
Capacidad	8 TB
Velocidad	7200 rpm
Alimentación	Adaptada para SAI y Corriente eléctrica, cableado necesario para ambas, con conectividad a PDU del RACK.
Compatibilidad	Misma marca y compatible con la infraestructuras y discos existentes.
Garantía	Conforme a lo indicado en el apartado 5.3.10

TABLA DE REQUERIMIENTOS	
SISTEMA DE BACKUP EN CINTA	
Formato	2U

Numero de cintas	24
Tipo de Unidad	LTO-9 Ultrium 45000
Velocidad de transferencia	2,16 TB/h (2 LTO-9)
Interfaz	FC12 Gb/s SAS (LTO-9). Incluir cables compatibles para ir acorde a la red de SPF28 25GbE. El adjudicatario utilizará cables de conexión tipo DAC para la conexión con cada switch SAN
Interfaz de red	2 puertos SFP28 25GbE, o tecnología superior y compatible con SPF28
Alimentación	Adaptada para SAI y Corriente eléctrica, cableado necesario para ambas, con conectividad a PDU del RACK.
Capacidad	Capacidad Nativa: 24 cintas x 18 TB = 432 TB 1,08 PB (LTO-9) con compresión 2,5:1 para autocargador de cintas HPE 1/24 con LTO-9
Cintas LTO-9	40 cintas LTO-9 incluidas con las siguientes características: • Capacidad Nativa (sin compresión): 18 TB por cinta. • Capacidad Comprimida (con un ratio de compresión de 2.5:1): 45 TB por cinta. • Vida útil: 30 años • Misma marca y compatible con el sistema de backup en cinta. • Pack de etiquetas para la gestión de las cintas por parte del robot
Cintas limpieza	2 cintas de limpieza incluidas
Garantía	Conforme a lo indicado en el apartado 5.3.10

Ejemplos de dispositivos con los anteriores requerimientos técnicos:

- Sistema de backup en disco: HPE ProLiant DL380 Gen11, controladora HPE Smart Array P408i-a SR Gen11 - P70458-421
- Sistema de backup en cinta: HPE MSL2040

5.3.7 Migración infraestructura

El adjudicatario realizará todas las tareas para migrar toda la infraestructura virtualizada del hardware actual al nuevo hardware, incluyendo el desmontaje de los servidores actuales del rack del CPD y la redistribución de los elementos dentro del rack. El adjudicatario revisará y migrará las reglas de los firewalls actuales a los nuevos a instalar y configurar.

Los switches LAN que actualmente utiliza Aguas de Burgos están distribuidos entre un rack de servidores otro rack contiguo comunicaciones. El adjudicatario instalará los nuevos switches de este pliego en un único rack, y realizará los cambios de cableado que sean necesarios para una mejor distribución del cableado.

Los trabajos de migración que requieran de cortes de servicio, se realizarán fuera del horario de trabajo habitual de los usuarios de Aguas de Burgos (de lunes a viernes de 7:30 a 15:30).

El adjudicatario trasladará el actual hardware (hosts, almacenamiento, SAI, servidor de copias, switches) desde el CPD principal de Aguas de Burgos, a los racks de un segundo CPD de Aguas de Burgos (también en la ciudad de Burgos).

El adjudicatario dejará montado y preparado el hardware para su aprovechamiento en actuaciones relacionadas con la seguridad de la información, de tal forma que se liberen los recursos utilizados de forma previa a la migración de la infraestructura, y queden disponibles como si fueran nuevos para ser utilizados en futuros proyectos de ciberseguridad de Aguas de Burgos como, por ejemplo:

- Instalación de señuelos (*deceptors*) de ciberseguridad.
- Creación de entornos aislados para testing de seguridad.
- Mejoras en la ciberresilencia en caso de desastre.

5.3.8 Replicación CPD

El adjudicatario deberá suministrar, instalar, configurar y poner en marcha, en las instalaciones de Aguas de Burgos, el hardware de forma redundante entre los dos CPD que forman parte de la infraestructura IT de Aguas de Burgos.

Los CPD actuarán de forma que, en caso de fallo de uno de ellos, el que haga de secundario entre en funcionamiento y permita la continuidad de operaciones de Aguas de Burgos.

El adjudicatario utilizará técnicas de replicación que a la vez que garantizan la disponibilidad en dos ubicaciones de los servicios, permitan realizar balanceos de carga en aquellas aplicaciones que lo requiriesen.

El adjudicatario, dentro de los trabajos correspondientes a la instalación y configuración del hardware, será el encargado de realizar todas las configuraciones hardware y software necesarias para obtener la redundancia de los CPD, pudiendo dichas configuraciones actuar en modo activo/activo cuando sea necesario.

Será objeto de redundancia:

- Servidores físicos (hosts)
- Sistemas almacenamiento SAN
- Switches SAN
- Switches LAN

- Servidores almacenamiento NAS
- Firewalls perimetrales
- Firewalls internos
- Sondas SAT-INET (condicionado al estudio del apartado “5.3.5 Sondas”)
- Sondas SAT-ICS (condicionado al estudio del apartado “5.3.5 Sondas”)

El adjudicatario, durante el primer mes del contrato, analizará la red y dispositivos de comunicaciones entre los CPD y elaborará un informe de mejoras y recomendaciones técnicas con el objetivo de mejorar y garantizar el cumplimiento de los puntos objetivo de recuperación (RPO) y los tiempos objetivo de recuperación (RTO), definidos en el análisis de riesgos.

5.3.9 Software

El adjudicatario durante el primer mes del proyecto, realizará un análisis del licenciamiento de la infraestructura IT actual, en el que se incluye el software de virtualización, sistemas operativos de servidores, software de backup, antivirus. Todo el software deberá ser compatible con el hardware adquirido.

Partiendo de dicho análisis, incluirá dentro del plan de adecuación y mejoras de la infraestructura IT/OT del apartado 5.3. de este pliego, la identificación de las licencias comerciales necesarias para alcanzar los objetivos de este pliego y las funcionalidades a cubrir por dichas herramientas. El adjudicatario realizará una valoración de los productos software, cantidad de licencias, tipo, importe económico, prestaciones y otras características que resulten las más beneficiosas para Aguas de Burgos.

El resultado de este plan, deberá servir de base para la elaboración de los correspondientes pliegos de prescripciones técnicas y administrativas, que Aguas de Burgos licitará para obtener el suministro de dichas licencias.

Entre el software licenciado que se debe incluir en el plan, y que tendrán en cuenta las licencias ya existentes, se encontrarán los siguientes paquetes:

- Software de virtualización. Las licencias del software de virtualización, serán las utilizadas en los servidores físicos (hosts) del apartado 5.3.1
- Software de backup de servidores virtualizados. Las licencias del software de virtualización, serán las utilizadas en los servidores físicos (hosts) del apartado 5.3.1.
- Software de backup de equipos.

- Software de encriptación de cintas de backup.
- Sistemas operativos de servidores. Las licencias de servidores, servirán para actualizar los actuales servidores.
- Bases de datos. Las licencias de servidores, servirán para actualizar los actuales sistemas de bases de datos.
- Antivirus
- Software de acceso remoto
- Plataformas de gestión de certificados
- Software de securización de Office 365
- MDM
- Herramientas de monitorización
- Servidores web, proxies y WAF.
- Servicios en la nube de seguridad.
- Otras herramientas de ciberseguridad

Una vez Aguas de Burgos disponga de las licencias de virtualización y backup de los servidores, el adjudicatario procederá a realizar los trabajos de instalación, configuración y migración de la infraestructura actual, teniendo en cuenta los plazos establecidos en el apartado “9.1 Fase de adecuación e implantación”.

5.3.10 Garantía

El adjudicatario estará obligado a garantizar todos los activos hardware del presente procedimiento de contratación, durante un plazo mínimo de **5 años**, salvo mención expresa en los requisitos técnica.

La modalidad de garantía requerida será **in-situ en modalidad NBD** (Next Business Day).

La fecha de inicio del servicio de garantía comenzará a partir de la fecha de aceptación del equipamiento por parte de Aguas de Burgos, que coincidirá con el suministro, instalación y configuración de los activos en su ubicación final.

5.3.10.1 Gestión de garantías

La gestión de garantías es el servicio que deberá proporcionar el adjudicatario para la resolución de incidencias del hardware. La garantía tiene las condiciones siguientes:

- La actuación se llevará a cabo en las instalaciones de Aguas de Burgos en donde esté instalado el elemento.
- El adjudicatario está obligado a asumir la garantía de todos los dispositivos o elementos suministrados.
- El adjudicatario está obligado a la continuidad en la prestación del servicio de garantía cualquiera que sea la circunstancia en la que concurra el proveedor de los activos, bien sea quiebra técnica, bien cualquier tipo de situación y/o casuística.
- El adjudicatario será responsable de los elementos objeto de la gestión de garantía in situ, y en caso de que se produzca cualquier incidencia en relación a los mismos deberá articular los mecanismos que sean necesarios para su resolución de la forma siguiente:
    - Utilización de stock existente para la sustitución de los elementos averiados o defectuosos.
    - La garantía incluiría la reparación de averías o funcionamientos defectuosos del hardware y software incluido en los equipos suministrados, e implica obligación de reparar o reemplazar, si fuera necesario, los componentes o piezas defectuosas, incluyendo la mano de obra, las piezas de recambio necesarias y los desplazamientos precisos.
    - En el caso de que se prevea que la reparación de equipo puede superar las 24 horas o que el equipo averiado tenga que ser reparado fuera de las dependencias de la entidad, el adjudicatario tiene la obligación de sustituir temporalmente el equipo averiado por otro de características iguales o superiores, hasta que este sea repuesto en perfecto estado de funcionamiento.
    - El adjudicatario estará en disposición de recibir comunicaciones de avería o incidencias, tanto de hardware como de software, y de prestar un servicio de atención de las mismas con una disponibilidad de 8 horas al día, entre las 07:30 y las 15:30 horas de lunes a viernes. Este procedimiento contemplará, al menos, la apertura de incidencias a través de vía telefónica, mail o web.
    - Al informar de una incidencia, la empresa adjudicataria proporcionará un número de identificación único de la misma para su seguimiento y control.

- La empresa adjudicataria dispondrá de medios suficientes para personarse en el lugar de la intervención tras las comunicaciones telefónicas o electrónicas mencionadas, y proceder a la reparación o sustitución en un plazo máximo de 24 horas.
- Todos los gastos derivados del suministro, mantenimiento y reparaciones, serán por cuenta del adjudicatario.
- Tras la resolución de cualquier actuación de mantenimiento, se entregará un informe indicando el número de incidencia, fecha, identificativo del ordenador, diagnóstico de la incidencia, proceso de resolución y componentes reemplazados o reparados.

- En cuanto al software base de los dispositivos (firmware, drivers, utilidades del fabricante), el adjudicatario deberá proporcionar los parches y actualizaciones necesarias, para el correcto funcionamiento del mismo durante todo el plazo de garantía.

5.3.11 Inventario

Todos los bienes suministrados mediante el presente expediente requieren ser etiquetados tanto a nivel físico como lógico para su inventariado por parte de Aguas de Burgos, de cara a cumplir con lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en cuanto a lo que se refiere al inventario y etiquetado de todos los activos.

Aguas de Burgos establecerá con el adjudicatario un procedimiento de inventariado, en el cual se definan una serie de normas específicas para el correcto etiquetado tanto físico como lógico de todo el inventario de bienes suministrado en el contrato, así como del correcto registro en la herramienta que recoja todo el inventario suministrado a Aguas de Burgos.

De cara a la realización de las etiquetas para el inventariado, se estará a disposición de Aguas de Burgos con el fin de que se incluyan en las mismas los logos cofinanciadores conforme a la normativa en materia de información y comunicación, tal y como se establece en el apartado “14 Información y comunicación” de este pliego.

5.3.11.1 Etiquetado físico

El etiquetado físico se realizará mediante etiquetas que proporcionará el suministrador del contrato. El proceso completo de etiquetado debe realizarlo la empresa suministradora, y los costes asociados a este proceso estarán incluidos dentro de los trabajos a realizar dentro de esta contratación. La empresa suministradora deberá realizar todos los pasos indicados en el procedimiento de inventariado de bienes contratados con la opción de etiquetado incluidos en la presente memoria y tomar todas

las medidas necesarias para garantizar que los bienes son inventariados en la herramienta negociada junto con Aguas de Burgos y con la correspondiente etiqueta adherida al equipo en los términos que describe el procedimiento de inventariado, negociado previamente con Aguas de Burgos.

5.3.11.2 Etiquetado lógico

Para aquellos bienes que permitan un etiquetado lógico, será obligatorio seguir una nomenclatura unificada para Aguas de Burgos. Será responsabilidad del adjudicatario cumplir con la normativa de nomenclatura según se indique en el procedimiento de inventariado de bienes.

El adjudicatario deberá realizar una revisión proactiva periódica de al menos una vez al mes del inventario para mejorar el control y seguimiento de activos.

5.4. Adecuación infraestructura IT/OT

Aguas de Burgos dispone de infraestructura de redes IT y OT que es gestionada por personal interno. La excelencia en la administración y securización de esta infraestructura requiere de recursos adicionales de administración de redes, sistemas y ciberseguridad, adecuando la infraestructura de forma previa a la fase de operación por el SOC. Esta adecuación implica la realización de trabajos de revisión del estado actual y elevar la securización de la infraestructura hasta un nivel que permita la correcta operación, vigilancia y gestión de incidentes por parte del SOC, en aplicación del ENS y otras normativas en vigor.

El adjudicatario asignará al proyecto técnicos especialistas en administración de redes, sistemas y ciberseguridad de redes IT/OT que, de forma coordinada con la OTSI y con los técnicos del departamento de Nuevas Tecnologías de Aguas de Burgos, y según la priorización de tareas acordada entre Aguas de Burgos y la OTSI, realice de forma continua trabajos de securización de sistemas y redes IT/OT.

Los trabajos a realizar por estos técnicos cumplirán los siguientes requisitos:

- Dedicación al proyecto. El adjudicatario deberá contar con un número suficiente de técnicos especialistas que permita contar con al menos dos perfiles simultáneos con 100% de dedicación a tiempo completo, para la realización de las tareas encomendadas.

- Inicio de los trabajos en fecha acordada con Aguas de Burgos, como muy tarde, 2 semanas después de la firma del contrato, tras la primera priorización inicial de los trabajos a realizar.

- Presencialidad en las instalaciones de Aguas de Burgos cuando sea necesario por la naturaleza de los trabajos a realizar.

- Fin de los trabajos en fecha acordada con Aguas de Burgos.

Las tareas a realizar por estos técnicos especialistas, incluirán entre otras y sin que se trate de una relación exhaustiva, las siguientes:

- Securización de servidores y actualización de versiones de sistema operativo.
- Securización de equipos de usuario (ordenadores, portátiles, móviles, tabletas, etc.).
- Securización de infraestructura de virtualización.
- Securización de sistemas gestores de base de datos.
- Securización de aplicaciones cliente-servidor y aplicaciones web.
- Securización de servidores de aplicaciones, servidores web, sistemas de acceso remoto.
- Securización, segmentación y separación de redes cableadas IT/OT e inalámbricas.
- Securización de identificación, accesos locales y remotos a redes IT/OT.
- Securización de copias de seguridad.
- Realización de copias de seguridad en la nube (en la infraestructura del adjudicatario del contrato de telefonía y comunicaciones de Aguas de Burgos).
- Securización de correo electrónico, navegación segura, prevención de fuga de datos.
- Securización de dispositivos y redes IT: firewall, switches, routers, IDS/IPS, DMZs, VPNs, APs WIFI, etc.
- Securización de dispositivos y redes OT: SCADA, HMI, PLCs, equipos autónomos (caudalímetros, traductores de presión, etc), etc.
- Auditoría de la calidad de servicio y capacidad de las redes de comunicaciones.
- Implantación y configuración de herramientas de seguridad: MDM, WAF, proxies, etc.
- Revisión y gestión de políticas de grupo (GPOs) aplicadas a los usuarios del Directorio Activo.
- Realización y ejecución de test internos de vulnerabilidades, penetración, cumplimiento ENS, etc, utilizando herramientas del CCN-CERT o de libre distribución, e implantación de medidas correctoras detectadas.
- Análisis de resultados de los test de vulnerabilidades, penetración, cumplimiento

ENS, etc. que Aguas de Burgos encargue a proveedores externos. El resultado de este análisis servirá para actualizar la documentación generada por la OTSI.

- Implantación de medidas correctoras de las vulnerabilidades de los test de penetración y vulnerabilidades que Aguas de Burgos encargue a proveedores externos.
- Implantación y securización de una herramienta de inventariado y ticketing open-source.
- Automatización de tareas de securización de sistemas.
- Auditorías de configuración de dispositivos y redes IT/OT. Entre otras, podrá utilizarse la herramienta ROCIO para auditorías de equipos de comunicaciones: enrutadores, conmutadores y cortafuegos.
- Documentación de todos los trabajos realizados.
- Formación y transferencia de conocimiento a los técnicos de Aguas de Burgos.

Todas las tareas de securización incluyen el parcheado, migración y actualización de sistemas de información y del software base (sistemas operativos, bases de datos, librerías, componentes, etc.) en caso de que fuera necesario por cuestiones de seguridad, así como la instalación y configuración de nuevos servidores, middlewares, herramientas de monitorización y control, herramientas de protección, y en general cualquier elemento software relacionado con la ciberseguridad.

Todas las tareas de securización seguirán, entre otras buenas prácticas, las definidas en las guías de configuración seguras del CCN-STIC del CCN-CERT.

Estos técnicos especialistas no participarán en la implantación de las herramientas del CCN-CERT ni en los trabajos a realizar por la OTSI, ni en los trabajos relacionados con la renovación del hardware, los cuales serán realizados por otros perfiles dedicados al proyecto. Es decir, serán perfiles dedicados exclusivamente a los trabajos indicados en este apartado 5.4, y adicionales a los necesarios en el resto de trabajos de este pliego.

Para realizar estas tareas, el adjudicatario disponibilizará una bolsa horas de trabajo de técnicos especialistas, de la que Aguas de Burgos podrá disponer un número variable, entre 0 horas y el máximo establecido en el PCAP.

Periódicamente se establecerá el programa de tareas asignadas a los técnicos especialistas, según las necesidades de Aguas de Burgos y las recomendaciones de la OTSI. La programación se realizará por el Jefe de Proyecto (Responsable de la OTSI) según la priorización de las necesidades de Aguas de Burgos.

Por su parte, el Director del Proyecto del adjudicatario deberá presentar una propuesta justificada con la duración prevista para cada tarea asignada, que será tenida en cuenta para la planificación. Para esta propuesta se partirá de la premisa básica de que los

técnicos especialistas cuentan con la formación, experiencia, capacidad, habilidad y conocimientos expertos en las diferentes áreas y recursos necesarios para abordar los trabajos de forma diligente. No se admitirán demoras injustificadas, en particular aquellas que denoten falta de formación o conocimientos por parte de los técnicos especialistas.

El retraso en la ejecución de las tareas programadas será un indicador clave en los Acuerdos de Nivel de Servicio (ANS).

5.5. Centro de Operaciones de Seguridad (SOC)

El adjudicatario implantará un Centro de Operaciones de Seguridad que consistirá en un centro unificado para la ciberseguridad de las redes IT y OT de Aguas de Burgos. Este centro será el encargado de llevar a cabo las tareas técnicas de prevención, detección, respuesta y recuperación de las redes IT y OT tras un ciberataque.

Los grandes ejes sobre los que pivotará el SOC de Aguas de Burgos son:

- Operación.
- Vigilancia.
- Gestión de incidentes.
- Transferencia.

El Centro de Operaciones de Seguridad que se despliegue en el ámbito del presente pliego formará parte de la Red Nacional de Centros de Operaciones de Seguridad. La coordinación de los centros integrados en esta red nacional se llevará a cabo a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes. Esta plataforma permitirá el intercambio de información y el seguimiento de incidentes entre los operadores de servicios esenciales o proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia, siendo las herramientas LUCIA y REYES la base de dicha Plataforma.

El SOC deberá estar en disposición de poder operar todas las herramientas del CCN-CERT sin ningún tipo de restricción o limitación impuesta por terceros, que impida el acceso a todos los niveles de soporte de todas las herramientas del CCN-CERT. Para ello, el adjudicatario deberá tener los acuerdos, formación, certificaciones o cualquier otro elemento habilitante que le permita cumplir con los requisitos exigidos para poder operar las herramientas del CCN-CERT y tener acceso a todos los niveles de soporte.

Del mismo modo, todas las tareas realizadas dentro de los trabajos del apartado “5.2 Implantación de herramientas del CCN-CERT”, deberán garantizar que el SOC pueda utilizar las herramientas desde el primer día, sin que para ello sea necesaria ninguna tarea de adaptación, certificación o configuración adicionales.

5.5.1 Operación

Corresponderá al adjudicatario la gestión diaria 24x7 de todos los elementos y configuraciones que forman parte de las redes IT y OT y que son necesarios para garantizar la seguridad de las mismas. El servicio del SOC se prestará desde las instalaciones del adjudicatario.

Esta gestión diaria, incluirá la continuidad de todas las tareas y trabajos de securización realizados descritos en el apartado “5.4 Adecuación infraestructura IT/OT”.

El SOC realizará la gestión y operación de las herramientas del CCN-CERT, tanto de las actualmente existentes, como de aquellas que en el futuro queden a disposición del sector público y Aguas de Burgos solicite su utilización.

El SOC tendrá entre sus objetivos la orquestación, automatización y respuesta de seguridad (SOAR) desde un enfoque de ciberseguridad que mejore la eficiencia y eficacia de los procesos de respuesta a incidentes.

El adjudicatario será el responsable de realizar las siguientes tareas, y todas aquellas que sean necesarias para la correcta operación de las mismas durante el periodo de vigencia del contrato:

- **PILAR**
    - Mantener actualizado el inventario de activos IT/OT y análisis de riesgos realizados por el adjudicatario en la fase de adecuación.
    - Integración con todas las herramientas del CCN-CERT de este pliego.
- **LUCIA**
    - Gestionar grupos de usuarios y sus roles.
    - Administración de colas de trabajo. Estas engloban una serie de propiedades y procesos para su correcto funcionamiento.
    - Controlar los permisos otorgados a colas y demás objetos de LUCIA.
    - Gestionar usuarios gestores externos, que son aquellos a los que se desea dar acceso a alguno de los tickets creados manteniendo oculto el resto. Tal sería una empresa subcontratada que brinda apoyo en la resolución de ciertos incidentes a una entidad pero que no quiere que vea el resto de los incidentes.
    - Monitorizar y controlar la sincronización con el servidor central de LUCIA en el CCN-CERT.
    - Gestionar campos personalizados, notificaciones y plantillas de

procesos.

- Exportación de tickets a terceras plataformas.
- Copias de seguridad.
- Integración con todas las herramientas del CCN-CERT de este pliego.

- **REYES**
  - Integración de la información y configuración de REYES en el resto de herramientas del CCN-CERT.

- **GLORIA**
  - Mantenimiento correctivo, mantenimiento adaptativo y el mantenimiento evolutivo de la solución GLORIA, así como de las sondas desplegadas durante el tiempo de la prestación del servicio, lo cual incluirá instalación y actualización de parches de seguridad de todo el software, así como de los sistemas operativos.
  - Copias de seguridad.
  - Servicio remoto de detección y respuesta (Nivel 1 de operación):
    - Monitorización de eventos de seguridad mediante la plataforma GLORIA.
    - Análisis de tráfico y control de integridad de las sondas implantadas en los CPDs
    - Correlación y análisis de eventos
    - Operación y notificación de alertas
    - Coordinación de respuestas a incidentes
  - Las incidencias detectadas por parte del Nivel 1 del servicio SOC deberán ser comunicadas y gestionadas por parte del SOC a través de la herramienta de ticketing que apruebe Aguas de Burgos, así como por LUCÍA.
  - Servicio remoto de prevención y alerta temprana: Este servicio consiste en la notificación temprana de la publicación de nuevas vulnerabilidades y actualizaciones de seguridad sobre las tecnologías monitorizadas a través de la plataforma GLORIA.
  - Como parte del servicio 24x7, el adjudicatario será el encargado de la monitorización de la plataforma GLORIA, así como de las sondas desplegadas dentro de la presente licitación. No obstante, a lo anterior,

se podrá integrar la monitorización de los citados elementos dentro de la monitorización corporativa de Aguas de Burgos.

- Integración con todas las herramientas del CCN-CERT de este pliego.

- **EMMA**
  - Establecer controles de acceso a todos los dispositivos en función de su contexto y la lógica del negocio (autenticando por identidad/entidad, 2FA, etc.).
  - Aplicar segmentación dinámicamente para reducir la superficie de ataque, aislar dispositivos críticos y responder ante ataques de manera centralizada.
  - Conseguir unas líneas base de seguridad, tanto en los dispositivos de la red como los endpoints.
  - Integración con ROCIO para contrastar las configuraciones de los dispositivos de red, de manera centralizada, con el Esquema Nacional de Seguridad.
  - Integración con todas las herramientas del CCN-CERT de este pliego.
  - Establecer un proceso para monitorizar cualquier desviación.
  - Crear dashboards de manera dinámica con todos los datos del inventario de Aguas de Burgos.
  - Dar visibilidad, contexto y control de todos los dispositivos en entornos IT/OT.
  - Mantenimiento correctivo, mantenimiento adaptativo y el mantenimiento evolutivo de la solución EMMA, así como de los agentes desplegados durante el tiempo de la prestación del servicio, lo cual incluirá instalación y actualización de parches de seguridad de todo el software, así como de los sistemas operativos.
  - Copias de seguridad.

- **ROCIO**
  - Vigilancia de las deficiencias en las configuraciones de la electrónica de la red.
  - Facilitar partes de la auditoría de las configuraciones de manera centralizada y automatizada.
  - Copias de Seguridad de los dispositivos.

- Documentar y gestionar todas las copias de seguridad de las configuraciones y versiones de los firmwares de los dispositivos
- Integración con todas las herramientas del CCN-CERT de este pliego.

- **CLARA**
  - Asegurar la correcta configuración de los dispositivos de electrónica de red, para garantizar el cumplimiento del ENS/STIC.
  - Documentar y gestionar toda la información relacionada y su integración con el resto de herramientas del CCN-CERT de este pliego.
  - Coordinarse para las labores de implantación de Seguridad y Cumplimiento del ENS/NIS2 marcadas junto con Aguas de Burgos.
  - Integración con todas las herramientas del CCN-CERT de este pliego.
- **ANA CENTRAL**
  - El SOC hará uso de ANA CENTRAL, con el fin de lograr toda la información necesaria para actuar sobre el plan de acción elaborado junto con Aguas de Burgos, incluyendo entre otras tareas:
    - Crear los usuarios con los roles oportunos para las empresas externas o empleados internos.
    - Los informes de EMMA se subirán a ANA CENTRAL de forma manual:
      - Las importaciones/exportaciones de datos de una a otra herramienta se harán con la mayor frecuencia posible para lograr tener una integración lo más actual posible.
    - Acceder en tiempo real a problemas localizados, reproducirlos y seguir su evolución en el tiempo
    - Generar dinámicamente informes del estado real de la entidad por departamento, servidor, aplicación o cualquier activo definido
    - Centralizar y normalizar todas las inspecciones de seguridad realizadas
    - Remediación eficiente y efectiva de los problemas encontrados, siguiendo una metodología aprobada por Aguas de Burgos.
    - Realizar informes de los resultados de Auditoría de forma periódica, negociado con Aguas de Burgos.
  - Por otro lado, dentro de las tareas de prevención, ANA pondrá en relación

todo el trabajo de los auditores externos de Aguas de Burgos, quienes cargarán vulnerabilidades, con el trabajo a realizar por el SOC.

- Integración con todas las herramientas del CCN-CERT de este pliego.

- **CARMEN**
  - Mantenimiento correctivo, mantenimiento adaptativo y el mantenimiento evolutivo de la solución CARMEN, así como de las sondas desplegadas durante el tiempo de la prestación del servicio, lo cual incluirá instalación y actualización de parches de seguridad de todo el software, así como de los sistemas operativos.
  - Copias de seguridad.
  - Dirigirá el servicio gestionado de detección de Amenazas Avanzadas Persistentes (APT) y otras amenazas, siendo el SOC el equipo especializado de analistas de seguridad. Este equipo, usando principalmente la herramienta CARMEN, analizará los diferentes movimientos en la infraestructura, tales como patrones de comunicación de o hacia Internet y la actividad en los puestos finales, y detectará comportamientos anómalos para identificar código dañino instalado en los sistemas del cliente y determinar qué organización puede estar detrás de esta actividad para detectar otras infecciones o tomar medidas preventivas.
  - Realizará el análisis exhaustivo especializado de los datos de tráficos de red recopilados por CARMEN para la detección de APT, tráfico malicioso, ciberataques, infecciones y cualesquiera otras amenazas que puedan poner en riesgo la seguridad de Aguas de Burgos.
  - Estará encargado de realizar las siguientes prestaciones:
    - El soporte y asesoramiento en la captura de datos y en la adaptación de CARMEN al entorno tecnológico de Aguas de Burgos.
    - El mantenimiento y administración de la plataforma de CARMEN.
    - La atención a las incidencias de funcionamiento del sistema CARMEN.
    - La obtención y aplicación de las actualizaciones de la plataforma instalada de CARMEN.
    - Durante la vigencia del soporte contratado se garantizará la instalación de mejoras y nuevas versiones de CARMEN, incluyendo un mínimo de dos actualizaciones anuales para la

plataforma, así como los parches o correcciones que puedan ser necesarios para su funcionamiento óptimo.

- La instalación de mejoras y nuevas versiones y la aplicación de parches y correcciones serán siempre ejecutadas por personal del adjudicatario en horarios estimados por Aguas de Burgos como de menor impacto para el servicio.
- Las intervenciones podrán realizarse en remoto mediante conexiones que garanticen la integridad, la confidencialidad y la disponibilidad de la información tratada.
- Un soporte para la implantación y despliegue de la herramienta CLAUDIA, del CCN-CERT, en los equipos de Aguas de Burgos, y su explotación efectiva mediante CARMEN.
- Un soporte telefónico especializado a través del Centro de Servicios del adjudicatario, en horario 8x5, entre las 9:00 y las 19:00 h) para consultas e incidencias relacionadas con el funcionamiento del sistema CARMEN, los hallazgos detectados y las alertas comunicadas, destinado a los administradores de sistemas y los responsables de seguridad TIC del CSN.
- Un soporte para la prevención y mitigación de las amenazas detectadas, en caso de hallazgos, y para la comunicación de los incidentes de seguridad al CCN-CERT a través de las herramientas de este pliego.

- Configuración de Backups.
- Integración con todas las herramientas del CCN-CERT de este pliego.

- **CLAUDIA y microCLAUDIA**
  - Cada uno de agentes desplegados se comunica periódicamente con CARMEN, a través de canales seguros, para actualizar su estado y notificar de situación relevantes desde el punto de vista de seguridad que puedan suponer un riesgo para la organización, se garantizará esta comunicación para el control de:
    - Eventos de normativa (perfil Normativa)
      - Controlador de dominio
      - Servidor miembro
    - Eventos de seguridad (perfil APT)
      - Microsoft System Monitor

- Integración con todas las herramientas del CCN-CERT de este pliego.
- Integración mediante la API con el resto de herramientas de Aguas de Burgos que sea necesario para su control/monitorización.
- Plan de instalación/desinstalación/actualización de agentes en los equipos de la infraestructura de red.

- **Sondas SAT-ICS, SAT-INET, SAT-Distribuido / GLORIA**
  - El SOC deberá realizar la gestión y mantenimientos necesarios para asegurar la actualización, implantación de seguridad y cumplimiento ENS de los servidores físicos, así como de las conexiones necesarias de las sondas.
  - Cada sonda se gestionará completamente desde el CCN-CERT, no siendo necesaria la realización de tareas de administración por parte del personal de Aguas de Burgos. Eventualmente se le solicitaría apoyo al SOC en el caso que fuera necesaria la realización de tareas puntuales que no pudieran realizarse de manera remota.
  - La conexión entre la sonda y el sistema central se realiza siempre de forma segura, a través del establecimiento de un túnel cifrado. Esta conexión se realizará a través de salida a Internet de Aguas de Burgos. El establecimiento de este túnel cifrado se iniciará desde la sonda hacia el sistema central, no siendo necesaria ninguna infraestructura adicional por parte de Aguas de Burgos para el establecimiento de túneles cifrados.
  - De forma general, salvo que se pacte otra cosa, la sonda vigilará el tráfico de Internet de la red corporativa de Aguas de Burgos y el de las DMZ's de servicios que se ofrezcan a Internet. Con los eventos recibidos se realiza una correlación avanzada de eventos en el sistema central, permitiendo la detección de ataques hacia los distintos organismos adscritos al sistema o la presencia de código dañino en estas redes.
  - La gestión, actualización y mantenimiento del sistema central estará a cargo del CCN-CERT, que lleva a cabo tareas de administración, maduración de las reglas de detección e inclusión de nuevas funcionalidades y herramientas. De hecho, periódicamente se realiza la integración de numerosas reglas de detección, propias y externas, completando y ampliando la inteligencia del servicio y su capacidad de detección.
  - Como parte del servicio 24x7, el SOC será el encargado de la monitorización de las sondas SAT-INET/SAT-ICS, así como de las sondas desplegadas dentro de la presente licitación. No obstante, a lo anterior, se deberá integrar la monitorización de los citados elementos

dentro de la monitorización corporativa de Aguas de Burgos. Corresponde al SOC el mantenimiento correctivo, mantenimiento adaptativo y el mantenimiento evolutivo de las soluciones SAT-INET/SAT-ICS, así como de las sondas desplegadas durante el tiempo de la prestación del servicio, lo cual incluirá instalación y actualización de parches de seguridad de todo el Software, así como de los Sistemas Operativos.

- Los técnicos de Aguas de Burgos podrán acceder en tiempo real a información relevante de los eventos generados por esta sonda, a informes periódicos y a la información de los incidentes de seguridad notificados a través de un portal accesible en internet.
- Integración con todas las herramientas del CCN-CERT de este pliego.
- Integración mediante la API con el resto de herramientas de Aguas de Burgos que sea necesario para su control/monitorización.

- **INES**
  - Utilizará la herramienta INES del CCN-CERT para:
    - Utilizar el Asistente con el fin de elaborar la Planificación y Análisis del Estado de la Seguridad:
      - Generar el Plan de Adecuación.
      - Obtención de declaración de aplicabilidad.
      - Generación de la Política de Seguridad.
    - Implantación de Seguridad con AMPARO a partir del plan generado con INES.
    - Evaluar periódicamente el estado de la seguridad y el cumplimiento normativo en todas aquellas actuaciones en las que sea necesario.
  - Además, el CCN-CERT ha desarrollado una serie de módulos y asistentes para llevar a cabo todas las acciones relacionadas con la creación de un Plan de Adecuación para priorizar, planificar las tareas a realizar en las primeras fases de la adecuación al ENS, así como la hoja de ruta de implantación de medidas de seguridad.
    - Preparar y elaborar la Política de Seguridad, incluyendo la organización del Comité de Seguridad.
    - Determinar el Alcance de la Certificación, mediante la identificación de los servicios prestados y los sistemas en los que

están sustentados.

- Categorización del Sistema, atendiendo a la valoración de las dimensiones de seguridad de los servicios prestados y de la información que manejan.
- Descargar los modelos de procedimientos y normativas necesarios para la adecuación al ENS y gestionar la documentación del marco normativo.
- Recabar una postura de seguridad adaptada en base a una Declaración de Aplicabilidad provisional.
- Utilización del Módulo de Verificación de Perfiles de Cumplimiento en cuanto al Riesgo (MVPCR) para realizar un análisis de riesgos formal, incluyendo la valoración de las medidas definidas en la Declaración de Aplicabilidad.
- Validar la Declaración de Aplicabilidad definitiva y la postura de seguridad asociada.
- Llevar a cabo el proceso de implantación y así adecuarse al ENS de forma guiada gracias a sus Asistentes de Implantación (estándar, μCeENS y μCeENS-NG), que señalan los pasos que se deben seguir, muestran ayudas a lo largo de todo el proceso y evalúan automáticamente la conformidad del sistema para detectar carencias.
- Gestionar la seguridad del sistema, donde será posible llevar a cabo los registros de usuarios, registros de soportes, formación y cualquier otro registro necesario para mantener la seguridad en el ENS.

  - Completar la auditoría de Certificación de Conformidad a realizar con AMPARO. El CCN-CERT ha desarrollado el Asistente del Plan de Adecuación de INES y el Asistente de Implantación y Gestión de la Conformidad - AMPARO, como herramientas de Apoyo para la Obtención y Gestión de la Declaración/Certificación de Conformidad en el ENS, que junto con EMMA y ANA permiten, además, realizar la Gestión Continua de la Seguridad.
  - Integración con todas las herramientas del CCN-CERT de este pliego.

- **AMPARO**

  - Utilizará la herramienta AMPARO del CCN-CERT para asegurar la adecuación al ENS y el cumplimiento normativo en todas aquellas actuaciones en las que sea necesario, de cara a la Implantación de la

Seguridad elaborado desde INES. A través de AMPARO es posible, entre otras cosas:

- Elaborar hoja de ruta de implantación de seguridad.
- Implantación de Medidas Técnicas de Seguridad.
- Gestionar la Conformidad mediante un panel de gestión que permita mantener la comunicación con la organización, entidad u organismo auditado, ver el estado del sistema y facilitar todo el proceso de auditoría.
- Remitir y notificar el Resumen de Hallazgos de Auditoría al CCN-CERT por parte de las EC y los OAT.
- Disponer de una sección de Documentos de Conformidad donde poder incorporar el Plan de Auditoría, Informe de Auditoría, Certificado de Conformidad y cualquier otro documento relevante para la conformidad del sistema.
- Notificar Certificados de Conformidad para ser publicados en el Portal de Gobernanza: https://gobernanza.ccn-cert.cni.es/
- Disponer de un módulo de análisis de datos.

  - Integración con todas las herramientas del CCN-CERT de este pliego.

- **ADA**

  - El SOC utilizará la herramienta ADA del CCN-CERT para asegurar la adecuación al ENS y el cumplimiento normativo en todas aquellas actuaciones en las que sea necesario. A través de ADA es posible, entre otras cosas:

    - Prevención e identificación de vectores de ataque e infección, ofreciendo protección frente a posibles amenazas.
    - Almacenar y consolidar los resultados generados, de forma que pueden ser consultados con rapidez, ya sea para ampliar una investigación o para enriquecer los resultados de cada nuevo análisis.
    - Gracias a la profundidad de la visión estadística aportada, realizar un seguimiento de la evolución de las amenazas.
    - El adjudicatario deberá documentar y gestionar todas la información relacionada y su integración con el resto de herramientas del CCN-CERT de este pliego.

- Integración con todas las herramientas del CCN-CERT de este pliego.

- **ELSA**
  - Deberá tener bajo control la superficie de exposición al exterior de la red de Aguas de Burgos, realizando todas las tareas necesarias de administración requeridas para que los escaneos de la herramienta ELSA a la red, de forma que dichos escaneos se hagan de manera controlada y aporte la información requerida para defender a Aguas de Burgos de Amenazas de la red y realizar las gestiones y notificaciones de Ciberincidentes necesarias para asegurar la implantación de Seguridad y Cumplimiento de ENS/NIS2.
  - Por todo ello, se deberá realizar las gestiones necesarias para conseguir la mayor integración de ELSA con el resto de herramientas de este pliego.
  - Integración con todas las herramientas del CCN-CERT de este pliego.
- **IRIS**
  - Deberá realizar un análisis del estado de la Ciberseguridad de Aguas de Burgos de forma periódica, haciendo uso de la herramienta IRIS con el fin de aportar el mayor número de datos posible para defender a Aguas de Burgos de Amenazas de la red y realizar las gestiones y notificaciones de Ciberincidentes necesarias para asegurar la implantación de Seguridad y Cumplimiento de ENS/NIS2.
  - Por todo ello, se deberá realizar las gestiones necesarias para conseguir la mayor integración de IRIS con el resto de herramientas de este pliego, facilitando así la toma de decisiones en la gestión de incidentes sobre amenazas, centralizando y unificando la información del SAT y las herramientas LUCIA, CARMEN, GLORIA, MONICA, INES y PILAR del Centro Criptológico Nacional.
  - Integración con todas las herramientas del CCN-CERT de este pliego.
- **CARLA**
  - Revisión, gestión, configuración, inventariado, control de las políticas de protección para ficheros y/o carpetas, y control de usuarios protectores y consumidores.
  - Elaboración de informes del estado de la protección de los documentos.
  - Monitorización del estado de protección de los documentos y/o carpetas.
  - Gestión y control de accesos de cuentas de usuarios y a los documentos

protegidos.

- Configuración de alertas de correo y mensajes por correo para la integración de CARLA y su uso por parte de los usuarios.
- Integración con todas las herramientas del CCN-CERT de este pliego.

5.5.2 Vigilancia

La evaluación y vigilancia permanente 24x7 de todos los recursos de las redes IT y OT con posibilidad de ser atacados es una actividad crítica para Aguas de Burgos. Por ello, el adjudicatario debe realizar una labor continua de prevención de las deficiencias de seguridad que pueden ser de los siguientes tipos:

- Técnicas (bugs, configuraciones erróneas, servicios activos inesperados, puertas traseras, etc.).
- Humanas (falta de concienciación, inexperiencia, formación inadecuada, etc.).
- De procedimiento (inexistencia de documentación, acciones incorrectas o fuera de procedimiento definido, ausencia de verificaciones, etc.).
- Legislativas/normativas (desviación frente a los requisitos definidos como de obligado cumplimiento).

Algunos de los controles y medidas de detección recomendables son:

- Monitorización y correlación de eventos (SIEM).
- Inclusión de reglas de detección desde los puntos finales al perímetro externo.
- Gestión de incidentes y análisis forense.
- Búsqueda de amenazas ocultas (Threat Hunting). Gestión de alertas, incluidas las AntiDDoS.
- Análisis de código dañino.
- Estudio de anomalías en la red o en el comportamiento de equipos y usuarios.
- Control de la superficie de exposición de las redes, internas y externas.
- Control de suplantación de identidad y movimientos laterales.
- Uno de los objetivos fundamentales será la identificación de movimientos externos, como exfiltraciones o comunicaciones con sistemas de comando y movimientos laterales de mantenimiento de persistencia o robo de información

en la red corporativa.

El SOC realizará la gestión y operación de las herramientas del CCN-CERT. El adjudicatario será el responsable de realizar las tareas que sean necesarias para la correcta operación de las mismas durante el periodo de vigencia del contrato, con el fin de lograr el mayor control de la implementación, mantenimiento y gestión de la seguridad en todos los niveles de Aguas de Burgos.

5.5.3 Gestión de incidentes

Corresponderá al SOC la gestión de incidentes de ciberseguridad y las respuestas a los mismos 24x7. Para ello será preciso el análisis de los registros y evidencias generadas por las diferentes fuentes para que el SOC pueda actuar sobre los sistemas comprometidos de forma mucho más rápida. Para cada incidente aportará documentación técnica y protocolos a seguir para su resolución y prevención futura.

La comunicación de los incidentes se realizará por medio de la herramienta LUCIA del CCN-CERT.

El adjudicatario pondrá a disposición de Aguas de Burgos, un servicio de DFIR (Digital Forensics and Incident Response), que permita el acceso a técnicos multidisciplinares en caso de incidentes de ciberseguridad que afecten a la continuidad de las operaciones de Aguas de Burgos, los cuales junto con los profesionales que forman el SOC, permitan recuperar la normalidad en las operaciones. Para este tipo de incidentes, el adjudicatario deberá elaborará al menos los siguientes tipos de informes:

- Informe técnico.
- Informe pericial.

5.5.4 Transferencia

El adjudicatario elaborará un plan de transición del servicio del SOC, en el que describirá el proceso de traspaso del servicio a la finalización del contrato, bien a Aguas de Burgos o al nuevo proveedor al que Aguas de Burgos decida adjudicar el servicio. Este plan de transición contemplará los aspectos de coordinación, colaboración y traspaso de información, garantizando que este cambio de adjudicatario no influya en la continuidad del servicio ni en los niveles de calidad del mismo, e incluirá una planificación de la transición, que no excederá tres meses de duración.

El adjudicatario del servicio del SOC estará obligado, si así lo solicita Aguas de Brugos, a devolver el control del servicio una vez transcurrido el periodo de cobertura del contrato o por rescisión del contrato. Dicho traslado se realizará en un periodo máximo de tres meses, de forma que exista solapamiento con el nuevo adjudicatario, y de forma que no se produzca una interrupción o un menoscabo en la prestación del servicio.

Este traspaso incluye:

- Traspaso de toda la documentación generada, actualizada, en soporte papel y electrónico.
- Traspaso del conocimiento del servicio y del conocimiento técnico y funcional del hardware y software de ciberseguridad al personal (propio o externo) designado por Aguas de Burgos. Dicho traspaso será realizado por aquellos integrantes del equipo de trabajo que, en su momento, se consideren más adecuados por ambas partes.

Con anticipación suficiente al inicio del nuevo expediente del servicio, se hará una evaluación y planificación de todas estas actividades. Los costes de devolución del servicio serán asumidos por el adjudicatario saliente, considerándose incluidos en el precio ofertado a este expediente.

El nuevo adjudicatario deberá prestar el servicio en la fase inicial de manera gradual, asumiendo progresivamente y por fases un porcentaje mayor de servicios. Las fases y servicios a asumir en cada una de ellas se definirán de manera consensuada con Aguas de Burgos.

En el caso de que la devolución del servicio no pueda realizarse antes de la finalización del contrato, el adjudicatario del presente expediente (adjudicatario saliente) estará obligado a prorrogar la prestación del servicio durante el tiempo que requiera el nuevo adjudicatario (entrante) para asumir dicha prestación, a los precios vigentes en el presente expediente.

6. Ejecución, seguimiento y control

6.1. Medios técnicos y materiales

El licitador se compromete a poner a disposición de la ejecución del contrato todos los medios técnicos y materiales para garantizar la correcta ejecución de los servicios.

El licitador se comprometerá a cumplir los controles de calidad, auditorías y las verificaciones que establezca Aguas de Burgos para la aceptación de estos medios, se podrán realizar estas verificaciones, en cualquier momento durante la vigencia del contrato.

6.2. Medios personales

6.2.1 Jefatura de proyecto

El licitador se compromete a asignar un jefe de proyecto, durante toda la duración del contrato. Las funciones generales que desarrollará el jefe de proyecto serán las siguientes:

- Interlocutor entre Aguas de Burgos y la empresa adjudicataria.
- Responsable de la OTSI.
- Responsable último de la implantación de las herramientas del CCN-CERT.
- Responsable último de la implantación del hardware y software.
- Responsable del seguimiento y coordinación con el SOC. El SOC podrá a su vez tener un jefe de proyecto específico para sus funciones.
- Responsable del seguimiento y cumplimiento de los Acuerdos de Nivel de Servicio.
- Responsable de la generación y entrega de documentación, informes, etc.

El licitador deberá presentar en la memoria técnica un esquema organizativo del proyecto donde se detalle el equipo técnico designado a la ejecución del contrato y la persona designada como responsable de su coordinación.

Durante el transcurso del contrato se realizarán, al menos con carácter mensual, reuniones de seguimiento con el Responsable del Contrato designado por el Órgano de Contratación, al objeto de verificar el adecuado avance de su implantación.

Adicionalmente a las reuniones de seguimiento, se realizarán todas las reuniones de trabajo necesarias para la correcta ejecución del proyecto.

6.2.2 Equipo de trabajo

Dado el carácter de los trabajos a realizar, será necesario la intervención de diferentes especialistas que, disponiendo de la titulación, perfil y experiencia adecuados, garanticen la correcta ejecución de los trabajos a realizar.

El adjudicatario dispondrá de los elementos técnicos y administrativos necesarios para la prestación del servicio, cubriendo los gastos por desplazamiento, alojamiento y dietas en los que pudiera incurrir.

El adjudicatario establecerá los mecanismos de coordinación e información permanente con Aguas de Burgos, garantizando la prestación del servicio de forma ininterrumpida en las condiciones contratadas asumiendo cualquier incidencia que pueda producirse en el desempeño de las funciones (vacaciones, licencias, bajas, etc) por lo que siempre contará con personal apto, con los conocimientos y titulaciones requeridos, y disponible a los efectos de realizar las sustituciones que sean necesarias.

El adjudicatario asignará a la ejecución del contrato un equipo con efectivos suficientes para la adecuada prestación de los servicios a contratar y se deberá garantizar la estabilidad de dicho equipo durante toda la vigencia del contrato.

El equipo de trabajo deberá estar especializado y contar con experiencia demostrable para abordar con garantías los requisitos planteados descritos en el contenido y alcance de los trabajos a realizar.

Aguas de Burgos considera que los siguientes perfiles son los mínimos indispensables para llevar a cabo el presente proyecto. No obstante, deja a criterio de las empresas licitantes la incorporación de perfiles adicionales si así lo considera necesario.

- Dirección de proyecto
    - 1 Jefe de proyecto.
- OTSI e implantación herramientas CCN
    - 1 Especialista en Activos IT.
    - 1 Especialista en Activos OT.
    - 1 Especialista en Riesgos IT/OT.
    - 1 Especialista en RGPD.
    - 1 Especialista en Continuidad de Negocio.
    - 1 Especialista en ISO 27001/ENS.
    - 1 Técnico especialista en Ciberseguridad Industrial.
    - Técnicos especialistas en herramientas del CCN-CERT
- Adecuación infraestructura IT/OT
    - Especialistas en administración de redes, sistemas y ciberseguridad.
- SOC
    - Especialistas SOC Nivel 1-2.
    - Especialistas SOC Nivel 2-3.
- Implantación hardware y software
    - Técnicos especialistas.

Los medios personales adscritos al proyecto, deberán realizar su trabajo tanto de forma presencial en la sede de Aguas Burgos, o en las instalaciones de Aguas de Burgos que sea necesario, como de forma remota cuando sea posible.

Aguas de Burgos considera que, para una óptima ejecución de las tareas de identificación de activos IT/OT, análisis de riesgos IT/OT, adecuación al ENS implantación de herramientas del CCN-CERT y adecuación de infraestructura IT/OT, es

necesario que los siguientes 4 grupos de perfiles desempeñen su trabajo con un nivel de presencialidad suficiente, en las instalaciones de Aguas de Burgos, en especial durante los primeros meses de ejecución del proyecto:

- Perfil de especialistas en Activos IT, Activos OT, Riesgos IT/OT e ISO 27001/ENS.
- Perfil de técnico especialista en Ciberseguridad Industrial.
- Perfil de técnicos especialistas en herramientas del CCN-CERT.
- Perfil de especialistas en administración de redes, sistemas y ciberseguridad.

La suma del número de jornadas presenciales de los 4 grupos de perfiles anteriores será de un mínimo de 150 durante la fase de adecuación e implantación. A efectos del cálculo del número de jornadas presenciales realizadas, el número de jornadas máximo computable a un mismo grupo de perfiles no excederá del 60% del total. El número de jornadas mínimo computable a un mismo grupo de perfiles será del 10% del total.

Tendrá la consideración de una jornada presencial, aquella que tenga lugar en las instalaciones que Aguas de Burgos determine, con horario de entrada entre las 07:30 y 08:30. Sólo se considerarán aquellas jornadas que sean completas al 100% de una jornada laboral ordinaria de un trabajador. En caso de que un mismo trabajador desempeñase diversos perfiles, sólo se tendrá en cuenta en uno de los grupos a efectos de contabilización de las jornadas realizadas.

Se contabilizará una jornada por cada trabajador que cumpla las condiciones anteriores, teniendo en cuenta que el máximo de jornada computables en un mismo día será de 6 jornadas correspondiente a:

- 2 jornadas presenciales máximo por día, correspondiente a especialistas en Activos IT, Activos OT, Riesgos IT/OT o ISO 27001/ENS.
- 1 jornada presencial máximo por día, correspondiente a especialistas en Ciberseguridad Industrial.
- 2 jornadas presenciales máximo por día, correspondientes a técnicos especialistas en herramientas del CCN-CERT.
- 1 jornada presencial máximo por día Especialistas en administración de redes, sistemas y ciberseguridad.

Otros perfiles necesarios en el proyecto, también requerirán de presencialidad en todas aquellas actuaciones que no puedan realizarse de forma remota. En el caso del Jefe de Proyecto, acudirá de forma presencial a las instalaciones de Aguas de Burgos, a todas las reuniones mensuales de seguimiento, y en todas aquellas ocasiones en que sea requerido.

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, podrá implicar la obligación de sustitución del mismo o la resolución del contrato

En el caso de que el servicio no se prestara de manera adecuada, Aguas de Burgos requerirá al adjudicatario que subsane las deficiencias producidas, pudiendo exigirle, si se hace necesario, la sustitución de las personas contratadas por este.

En caso de que, a petición del adjudicatario, sea necesario sustituir a algún miembro del equipo, el adjudicatario deberá comunicarlo a Aguas de Burgos, y la sustitución deberá realizarse por un perfil que cumpla con las mismas características profesionales y técnicas requeridas y ofertadas y que será aprobada por Aguas de Burgos.

En cualquier sustitución de personas del equipo de trabajo, se exigirá un período de formación, a cargo del adjudicatario, para el nuevo miembro que se incorpora, así como un período de convivencia entre el profesional que se da de baja y el que se incorpora.

Los medios humanos aportados por el contratista para la ejecución del contrato estarán sometidos al poder de dirección y organización del adjudicatario en todo ámbito y orden legalmente establecido; será por tanto el adjudicatario el único responsable de dicho personal, no teniendo en ningún momento, por tanto, vinculación jurídico-laboral alguna con Aguas de Burgos. 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.

6.3. Acuerdos de Nivel de Servicio

6.3.1 Oficina Técnica de Seguridad Integral (OTSI)

La calidad del servicio prestado se medirá en base a unos indicadores clave (KPIs) sobre los que se establecerán unos niveles objetivos. Estos indicadores se agregarán de forma ponderada en un único indicador que representará la calidad del servicio prestado. Sobre este indicador agregado se definirá un “ANS de Oficina Técnica de Seguridad Integral (OTSI)”.

Este ANS se calculará de forma mensual, teniendo en cuenta el avance de las actividades del cronograma del plan detallado de proyecto las actividades estimadas o realizadas en dichos intervalos, según la priorización de tareas. En la siguiente tabla se define la configuración del ANS.

Indicador (KPI)	Peso	Valor máximo
Actualización del plan de proyecto y programa de tareas asignadas a la OTSI	10%	5 días laborables
Avance de las tareas del plan de proyecto	90%	n/a

Para el cálculo de estos indicadores, se tendrá en cuenta plan de proyecto y programa de tareas asignadas a la OTSI en lo referente a las tareas de los trabajos a realizar de los apartados “5.1 Oficina Técnica de Seguridad Integral (OTSI)” y “5.2 Implantación de herramientas del CCN-CERT”.

El indicador de actualización del plan de proyecto y programa de tareas asignadas a la OTSI, se calculará como el porcentaje de los casos que han cumplido el objetivo frente al total de casos ocurridos durante el trimestre.

El indicador de avance de las tareas del plan de proyecto, se calculará con el porcentaje real de avance respecto a la última planificación aprobada por Aguas de Burgos, y su porcentaje dentro de las tareas del plan de proyecto de los apartados 5.1 y 5.2.

Los valores de cada indicador se agregarán mediante la media ponderada (Peso). La suma de los pesos será de 100.

El incumplimiento del “ANS de Oficina Técnica de Seguridad Integral (OTSI)”, salvo causa de fuerza mayor, comportará las penalizaciones recogidas en el apartado “10 Penalizaciones y causas de resolución del contrato” del presente pliego.

6.3.2 Herramientas CCN-CERT

El adjudicatario se compromete a un ANS de resolución de incidencias que afecten a las herramientas del CCN-CERT, que como mínimo, tendrá los niveles definidos en las tablas siguientes.

Tipo	Herramienta	Tiempo máximo de resolución
Caída o funcionamiento incorrecto	SAT-INET	24 horas (servidor virtual) 48 horas (servidor físico)
	SAT-ICS	24 horas (servidor virtual) 48 horas (servidor físico)
	GLORIA	48 horas

	EMMA	48 horas
	CARMEN	48 horas

Como tiempo máximo de resolución, se considera el tiempo transcurrido desde la caída o inicio funcionamiento incorrecto hasta que éste es resuelto.

El cumplimiento reiterado por parte de la empresa adjudicataria de las condiciones especificadas en este apartado, podrá ser causa de resolución del contrato. Se considerará reiterado cuando ocurra alguna de las siguientes circunstancias:

- Caída o funcionamiento incorrecto de las sondas SAT-INET o SAT-ICS o de las herramientas GLORIA, EMMA, CARMEN en más de 4 ocasiones en un periodo de 60 días consecutivos.
- Caída o funcionamiento incorrecto de las sondas SAT-INET o SAT-ICS o de las herramientas GLORIA, EMMA, CARMEN durante más del 25% de los días en un periodo de 60 días consecutivos.
- Retrasos en la estimación o inicio de los trabajos de adecuación de la infraestructura IT/OT en más del 25% de las peticiones realizadas.

El incumplimiento del “ANS de Adecuación de Infraestructura IT/OT”, salvo causa de fuerza mayor, comportará las penalizaciones recogidas en el apartado “10 Penalizaciones y causas de resolución del contrato” del presente pliego.

6.3.3 Adecuación infraestructura IT/OT

La calidad del servicio prestado se medirá en base a unos indicadores clave (KPIs) sobre los que se establecerán unos niveles objetivos. Estos indicadores se agregarán de forma ponderada en un único indicador que representará la calidad del servicio prestado. Sobre este indicador agregado se definirá un “ANS de Adecuación de Infraestructura IT/OT”.

Este ANS se calculará de forma mensual, teniendo en cuenta las actividades estimadas o realizadas en dichos intervalos. En la siguiente tabla se define la configuración del ANS.

Indicador (KPI)	Peso	Valor máximo
Entrega de la estimación solicitada	20%	5 días laborables

Inicio de las actividades solicitadas una vez aprobadas por Aguas de Burgos	20%	5 días laborables
Entrega de las actividades solicitadas dentro de los plazos estimados	30%	25% de retraso
Realización de las actividades en las horas aprobadas	30%	10% de desviación respecto a lo estimado

En caso de solicitud de un nuevo trabajo de adecuación de la infraestructura IT/OT en base a la bolsa de horas, ésta debe ser atendida y estimada en el plazo máximo de la tabla anterior (5 días) desde la notificación de la misma. Una vez aprobado la realización del trabajo por Aguas de Burgos, deberá iniciarse el proceso para su ejecución en un plazo máximo de 5 días desde la aprobación de la misma.

Para cada indicador (KPI) se calculará el porcentaje de los casos que han cumplido el objetivo frente al total de casos ocurridos durante el mes. Estos resultados se agregarán mediante la media ponderada (Peso). La suma de los pesos será de 100.

La entrega de actividades que se retrase más de un mes, se tendrá en cuenta como incumplimiento en el cálculo en todos aquellos meses en los que se incurra el retraso.

Las desviaciones por encima de lo estimado, podrán ser compensadas con desviaciones por debajo de lo estimado.

El incumplimiento del “ANS de Adecuación de Infraestructura IT/OT”, salvo causa de fuerza mayor, comportará las penalizaciones recogidas en el apartado “10 Penalizaciones y causas de resolución del contrato” del presente pliego.

6.3.4 Centro de Operaciones de Seguridad (SOC)

El adjudicatario se compromete a un ANS de resolución de incidentes de ciberseguridad y prestación de servicio por parte del SOC, que como mínimo, tendrá los niveles definidos en las tablas siguientes.

Tipo	Prioridad	Tiempo máximo de resolución
Incidencia	Crítica	3 horas
	Alta	6 horas
	Media	24 horas
Petición	Baja	72 horas

Las prioridades se clasificarán atendiendo a la siguiente tabla:

Prioridad	Descripción de la incidencia
Crítica	Se considerarán incidentes críticos aquellos que cumplan al menos uno de los siguientes criterios: • Afectan a más del 40% de los servidores físicos o virtuales de Aguas de Burgos. • Afectan a más del 40% de las estaciones de trabajo de Aguas de Burgos. • Afectan a más del 40% de los usuarios de Aguas de Burgos. • Imposibilitan o afectan de forma significativa a la capacidad de Aguas de Burgos para prestar sus servicios.
Alta	Se considerarán incidentes de prioridad alta, aquellos que cumplan al menos uno de los siguientes criterios, y no cumplan las condiciones de críticos: • Afectan a más del 10% de los servidores físicos o virtuales de Aguas de Burgos. • Afectan a más del 10% de las estaciones de trabajo de Aguas de Burgos. • Afectan a más del 10% de los usuarios de Aguas de Burgos. • Imposibilitan o afectan a cualquier elemento individual del servicio o infraestructura hardware o software, existiendo una solución parcial, pero la capacidad de Aguas de Burgos para prestar sus servicios está degradada.
Media	Se considerarán incidentes de prioridad media, aquellos que no sean de prioridad crítica o alta. Incluye fallos que pueden ser localizados de manera individual, para los que existe una solución parcial, pero la capacidad de mantener el sistema se ha degradado ligeramente.

Las peticiones se clasificarán con prioridad baja, según la siguiente tabla:

Prioridad	Descripción de la petición
Baja	Consultas sobre las funciones o configuraciones particulares. Solicitudes de documentación o información.

Como tiempo máximo de resolución, para las incidencias (prioridades crítica, alta o media), se considera el tiempo transcurrido desde que Aguas de Burgos sufre los efectos negativos del incidente de seguridad hasta que éste es resuelto. No se

considerará el inicio del tiempo el momento en que el adjudicatario detecte la amenaza o el ataque, sino el comienzo del impacto sobre la organización, que puede ser anterior en caso de que el servicio de monitorización no funcione adecuadamente.

Como tiempo máximo de resolución, para las peticiones de consulta de información (prioridad baja), se considera el tiempo transcurrido desde que Aguas de Burgos realiza la petición al adjudicatario.

El adjudicatario deberá disponer de las herramientas y los procedimientos necesarios para la verificación de los niveles de servicio comprometidos.

El adjudicatario deberá informar al interlocutor de Aguas de Burgos de la evolución de los incidentes. Es condición necesaria la notificación de resolución del incidente por parte del adjudicatario para que se deje de computar tiempo.

En el caso de que se notifique y se compruebe el incidente persiste no se dejará de contabilizar el tiempo de resolución. Una vez finalizado el incidente, el adjudicatario tendrá que reportar obligatoriamente al responsable del proyecto de Aguas de Burgos, la resolución de la misma, indicando las acciones llevadas a cabo para su resolución.

El incumplimiento de los plazos mencionados anteriormente, salvo causa de fuerza mayor, comportará las penalizaciones recogidas en el apartado “10 Penalizaciones y causas de resolución del contrato” del presente pliego.

7. Capacitación

El adjudicatario ofrecerá todo el soporte técnico e informático necesario para aclarar dudas o facilitar el proceso de aprendizaje y el conocimiento del hardware, software e infraestructura de ciberseguridad desplegada a Aguas de Burgos para que resuelvan todas las dudas durante toda la vigencia del contrato, así como ofrecer la capacitación necesaria al personal designado por Aguas de Burgos.

El adjudicatario elaborará un plan de capacitación, que podrá ser actualizado durante la vigencia del contrato, y que deberá ser validado por Aguas de Burgos en cada una de sus versiones, en el que se incluirá como mínimo:

- Contenidos:
    - Capacitación para el conocimiento del hardware instalado.
    - Capacitación para el conocimiento del software base (copias de seguridad, virtualización, etc.).
    - Capacitación para el conocimiento de comunicaciones, configuración de equipos de Red, VPNs, Firewall, WAN, LAN, etc.

- Capacitación específica para el personal de Aguas de Burgos sobre la instalación, administración, parametrización realizadas sobre las herramientas del CCN-CERT y sobre el uso y explotación de los cuadros de mando de las mismas.
    - Arquitectura del sistema desplegado. Funcionalidades de sus componentes.
    - Administración básica de la plataforma.
    - Administración y gestión de casos de uso.
    - Administración y gestión de recolección de datos.
    - Gestión de alerta temprana.
    - Perfiles de usuarios a capacitar (administradores, técnicos informáticos, gestores, usuarios consulta, fontaneros/instaladores de contadores, etc.).
- Capacitación específica a los responsables de riesgos de Aguas de Burgos para poder realizar el mantenimiento de activos IT/OT en la documentación y herramientas utilizadas.
- Capacitación para las transferencias de la OTSI y el SOC.

- Concienciación y capacitación de usuarios en ciberseguridad.
    - Concienciación y capacitación continua de los usuarios de Aguas de Burgos en competencias de ciberseguridad.
    - Acciones de carácter periódico para evaluar la efectividad de las acciones de concienciación y formación realizadas.
    - Simulaciones de incidentes de seguridad realistas y adecuados al entorno de Aguas de Burgos.
    - Píldoras formativas.
- Recursos de apoyo y repositorio de información
    - Manuales de usuario.
    - Materiales de e-learning.
    - Herramientas de concienciación en ciberseguridad.
    - Videos formativos.
    - Webinars, etc.

- Mecanismos de revisión del plan de capacitación en fase de mantenimiento.
- Herramientas para realizar informes sobre el éxito o el alcance de la concienciación a los usuarios.

El adjudicatario tendrá la obligación de realizar jornadas de capacitación al personal designado por Aguas de Burgos, tanto de forma on-line como presencial, en función de las necesidades de Aguas de Burgos requiera, y conforme a la actualización del plan de capacitación, con una duración de hasta 80 horas de capacitación por cada 12 meses de contrato, acumulables en caso de no hacer uso de las mismas en alguna anualidad.

8. Documentación

Todos los documentos estarán estructurados de la misma forma, siguiendo un estándar y plantillas comunes. Se utilizarán convenciones de numeración y denominación para asegurar que todos los documentos tengan referencias únicas, siguiendo las pautas establecidas en las Guías CCN-STIC del CCN-CERT.

La empresa adjudicataria será la responsable de mantener actualizada la documentación del proyecto a lo largo del mismo.

La empresa adjudicataria deberá mantener un registro histórico de los cambios producidos en la documentación con una breve explicación de la causa que origina el cambio. Cada documento tendrá señalado el tiempo máximo de validez, y deberá identificar el número de versión del mismo.

La documentación será clara, concisa, precisa y fácil de mantener de forma que permita cumplir, dependiendo del tipo de documento, las funciones para las que ha sido diseñada. La documentación deberá ser aprobada por la dirección del proyecto por parte de Aguas de Burgos.

La documentación técnica a realizar durante la ejecución del proyecto, debe incluir como mínimo:

- Inventario de activos, incluyendo la Ficha de Servicios, disponiendo de los datos esenciales de cada servicio, tipos de información tratados y los sistemas de información sobre los que se prestan, así como una valoración inicial del nivel de seguridad de cada una de las dimensiones de seguridad aplicables al servicio/información de que se trate.
- Gestión y Documentación de los Certificados de toda la infraestructura, caducidad y plan de renovación e instalación previo a su caducidad para evitar pérdidas de servicio o conexiones inseguras.
- Documento de categorización del sistema o subsistemas, que incluya todas las actividades relativas a la valoración de los sistemas:

- Criterios seguidos y razonamientos aplicados.
- Opiniones o consideraciones de terceros que se han considerado relevantes.
- Leyes, reglamentos, normas o prácticas sectoriales de aplicación, con especial énfasis en las aplicables sobre seguridad nuclear.
- Circunstancias particulares que puedan tener un impacto en la valoración.
- Revisiones o ajustes que se lleven a cabo por terceras partes.

- Declaración de aplicabilidad provisional con la relación de medidas de referencia a implementar, conforme el Anexo II del 311/2022 ENS.
- Informe de análisis de riesgos conforme metodología MAGERIT y uso de herramienta PILAR, así como el fichero utilizado en la herramienta.
- Continuidad del negocio:
  - Análisis de Impacto en el Negocio.
  - Planes de Recuperación ante Desastres y pruebas asociadas.
  - Planes de pruebas.
- Requisitos técnicos y estimaciones económicas para la elaboración de pliegos de prescripciones técnicas.
- Documentación de implantación de todas las herramientas del CCN-CERT, que incluya al menos:
  - Plan detallado de puesta en marcha y configuración.
  - Estudio de implantación de sondas SAT-INET y SAT-ICS.
  - Proceso de instalación, que incluya todos los elementos que son necesarios para disponer del equipamiento y las herramientas totalmente operativas.
  - Identificación de partes involucradas en el despliegue y dependencias entre ellas. Necesidades de infraestructura hardware, conectividad de red, direccionamiento IP necesario.
  - Configurar sistema de alertas para recepción y envío de las mismas.
  - Plan de configuración del sistema.
  - Propuesta de integración con sistemas externos.

- Propuesta de políticas generales de configuración.
- Propuesta de definición de alertas e incidentes.
- Arquitectura del sistema desplegado. Diagramas físicos y lógicos.
- Requisitos y configuración para monitorización de las herramientas de ser necesaria por otros sistemas. Sistema de alertas implementado par aviso en caso de fallos, pérdida del servicio por conexión, fallo del Hardware o del software.
- Configuración e implementación de Backups, plan y contingencia, como recuperarse ante un desastre. Respaldo y restauración de datos.
- Plan de Dimensionamiento de virtualización, necesidades a corto, medio y largo plazo.
- Guías de mantenimiento para actualizaciones y parches, tanto de las herramientas como de los Sistemas Operativos.

- Documentación de implantación del hardware y software, que incluya al menos:
  - Plan de adecuación y mejoras de la infraestructura IT/OT.
    - Análisis de la infraestructura actual y de la arquitectura de red en los CPD y otras ubicaciones,
    - Optimización y mejoras necesarias en la infraestructura IT/OT.
    - Licencias comerciales
  - Plan detallado de puesta en marcha, configuración e instalación.
  - Configuración de la infraestructura. Equipamiento del que disponen (gráficos, inventario de conexiones).
  - Arquitectura del sistema desplegado. Diagramas físicos y lógicos.
  - Albaranes, licencias, garantías.
  - Procedimiento en caso de avería para soporte, sustitución o actualización.
- Documentación de gestión del SOC
  - Plan de gestión del SOC.
  - Plan de trabajo de operaciones recurrentes.
  - Procedimientos para la gestión de alertas e incidentes.

- Informe de seguimiento mensual del SOC, que será utilizado para la comprobación del cumplimiento de los ANS, que incluya al menos:
  - Vulnerabilidades identificadas y actuaciones llevadas a cabo para resolverlas.
  - Resultados de la monitorización de redes y servidores, identificando los intentos de intrusión o ataque detectados y bloqueados.
  - Incidentes de seguridad ocurridos, las actuaciones llevadas a cabo para resolverlos y recomendaciones para evitarlos en el futuro.

- Documentación de gestión del proyecto
  - Plan detallado de proyecto.
  - Plan de calidad y mejora continua.
  - Informes de seguimiento mensual. Incluirá un informe mensual con la evolución de los trabajos, el avance real y la planificación prevista.
  - Acta de cada reunión de seguimiento.
  - Informes de mejora continua mensuales con propuestas de acciones y medidas cuyo propósito sea mejorar la gestión de la seguridad IT/OT.
  - Plan de transición del servicio del SOC.
  - Plan de capacitación.
  - Propuestas de nuevas herramientas y necesidades.

Además, el adjudicatario elaborará todos los documentos que la Aguas de Burgos le solicite en el marco del desarrollo de las actividades descritas en el presente pliego.

9. Plazos y duración contrato

Los plazos de ejecución del proyecto, que se contabilizarán a partir del día siguiente de la fecha de la firma del contrato, son los siguientes:

- Plazo de ejecución: 28 meses. Incluye las siguientes fases:
  - Fase de adecuación e implantación: hasta 16 meses, con fecha máxima de finalización el 01/06/2026. Este plazo podrá ser reducido por el adjudicatario según lo especificado en el PCAP.

Todos los trabajos de la fase de adecuación e implantación, están vinculados al calendario de obligaciones impuestos por la primera convocatoria de subvenciones (2022) en concurrencia competitiva de proyectos de mejora de la eficiencia del ciclo urbano del agua (PERTE digitalización del ciclo del agua). Según dichas obligaciones, todas las actuaciones del proyecto DIGITAGUABUR, entre las que se incluye la fase de adecuación e implantación de este proyecto, deben estar ejecutadas y certificadas antes del 31/12/2025 o del 01/06/2026 en caso de prórroga del mismo.

- Fase de operación: 12 meses, que se contabilizarán a partir del día siguiente a la finalización de los trabajos de la fase de adecuación e implantación.

  Los trabajos de la fase de operación, estarán vinculados a las actuaciones del proyecto DIGITAGUABUR, en proporción al periodo de elegibilidad del proyecto aprobado.

- Posibles prórrogas. Dos posibles prórrogas de 12 meses de duración cada una, correspondientes a la fase de operación, obligatorias para el adjudicatario en caso de que Aguas de Burgos lo solicite.

El proyecto, por tanto, tendrá una duración de 28 meses, con dos posibles prórrogas de 12 meses, pudiendo llegar a 52 meses de duración.

9.1. Fase de adecuación e implantación

Durante esta fase, la ejecución por parte del adjudicatario de las tareas de este pliego, deberá cumplir con los siguientes hitos y plazos máximos:

- UN (1) MES para el análisis de la infraestructura hardware actual, elaboración del plan de adecuación y propuestas de mejoras para la implantación del nuevo hardware, optimización de la infraestructura IT/OT y licenciamiento software necesario desde la fecha de firma del contrato.

- UN (1) MES para el suministro, instalación y configuración del servidor de almacenamiento NAS desde la fecha de firma del contrato. La instalación de este servidor permitirá aumentar la disponibilidad de almacenamiento actualmente disponible, a la espera del resto de suministro, instalación y configuración del resto de elementos identificados en el apartado “5.3 Suministros de ciberseguridad”.

- UN (1) MES para la elaboración de un plan de proyecto detallado, con el cronograma y desglose de actividades y tareas, recursos, hitos y entregables de la fase de adecuación e implantación desde la fecha de firma del contrato. Este plan reflejará el porcentaje que representa cada una de las tareas, respecto al

total del proyecto. Este plan, deberá ser validado por Aguas de Burgos.

- DOS (2) MESES para la implantación del hardware y software que renueven al actualmente ya existente en el CPD de Aguas de Burgos desde el suministro de las licencias software identificadas durante los trabajos del primer mes, las cuales serán licitadas por Aguas de Burgos en un proceso independiente de contratación pública. Los trabajos de implantación se regirán por los planes elaborados en el primer mes.
- CUATRO (4) MESES para la implantación de las herramientas CLARA, CLAUDIA y microCLAUDIA, desde la fecha de firma del contrato.
- SEIS (6) MESES para la implantación inicial del Sistema de Gestión de Seguridad de la Información (SGSI) de Aguas de Burgos por parte de la OTSI desde la fecha de firma del contrato, en el que se incluya una primera versión completa del análisis de riesgos, incluido el inventariado del 100% de los activos IT/OT.
- NUEVE (9) MESES para la implantación y/o utilización de al menos el 60% de las herramientas del CCN-CERT desde la fecha de firma del contrato.
- DOCE (12) MESES para la realización de los trabajos de adecuación al ENS por parte de la OTSI desde la fecha de firma del contrato.
- DIECISEIS (16) MESES para los trabajos de adecuación de la infraestructura IT/OT desde la fecha de firma del contrato.
- DIECISEIS (16) MESES para la realización del 100% de los trabajos de la OTSI.
- DIECISEIS (16) MESES para la implantación del 100% de las herramientas del CCN-CERT descritas en el pliego desde la fecha de firma del contrato.

En caso de que el adjudicatario oferte una reducción del plazo de ejecución de esta fase, los plazos de los hitos de las tareas con una duración igual o superior a SEIS (6) MESES, se verán reducidos de forma proporcional a la reducción del plazo total de ejecución de esta fase.

9.2. Fase de operación

Esta fase, dará comienzo una vez finalizados y certificados los trabajos de la fase de adecuación e implantación. Aguas de Burgos podrá cancelar la ejecución de esta fase, si no se han alcanzado los objetivos de la fase anterior o se ha excedido el plazo de la misma. Durante esta fase, el adjudicatario operará el SOC durante un periodo de DOCE (12) MESES prorrogables, hasta en dos ocasiones, en periodos de 12 meses.

Una vez puesto en marcha el SOC, serán los recursos asignados al SOC quienes operen todas las herramientas del CCN-CERT, inclusive aquellas destinadas al aseguramiento de la correcta implantación de la seguridad, adecuación al ENS, cumplimiento normativo y acceso a la información de indicadores (ANA Central, AMPARO, CLARA, INES, IRIS, PILAR) inicialmente gestionadas por la OTSI.

El adjudicatario deberá continuar ofreciendo los servicios de adecuación al ENS que siguieran siendo necesarios, y los servicios recogidos en el apartado "5.1.2 Gestión de la seguridad" de este pliego, inicialmente gestionados por la OTSI, que también siguieran siendo necesarios, bien integrados dentro del SOC, bien manteniendo una estructura simplificada de la OTSI.

10. Penalizaciones y causas de resolución del contrato

10.1. Graduación de faltas por incumplimiento del pliego

La clasificación de las faltas por incumplimiento del pliego de prescripciones técnicas, se realizará en función de su gravedad:

- **CON CARÁCTER LEVE**
    - Deficiencias en la organización general del trabajo.
    - Carencia de medios adecuados y suficientes para ejecutar un trabajo.
    - Deficiencias en la cumplimentación de datos, en soporte papel o informático, tramitación de documentos, conservación y custodia de los mismos.
    - No establecer los mecanismos adecuados para rectificar deficiencias en la gestión.
    - El incumplimiento de los tiempos máximos resolución del SOC por cada incidente con prioridad media dentro de un mes.
    - El incumplimiento de los tiempos máximos resolución del SOC por cada 2 peticiones de consulta de información (prioridad baja) dentro de un mes.
    - El incumplimiento en un periodo mensual del "ANS de Adecuación de Infraestructura IT/OT" obteniendo un valor entre 70 y 90 puntos.
- **CON CARÁCTER GRAVE**
    - Incumplimiento de órdenes de Aguas de Burgos comunicadas de forma fehaciente.
    - La reincidencia de 3 faltas del mismo tipo catalogadas como leves dentro

de un trimestre.

- El incumplimiento de los tiempos máximos resolución del SOC por cada incidente con prioridad alta dentro de un mes.
- El incumplimiento de los tiempos máximos resolución del SOC por cada 6 peticiones de consulta de información (prioridad baja) dentro de un mes.
- El incumplimiento en un periodo mensual del "ANS de Adecuación de Infraestructura IT/OT" obteniendo un valor superior a 40 e inferior a 70 puntos.

- **CON CARÁCTER MUY GRAVE**
  - Incumplimiento en los requisitos de los perfiles asignados a la OTSI por cada mes del proyecto.
  - Incumplimiento en los requisitos de los técnicos asignados a los trabajos de adecuación de la infraestructura IT/OT por cada mes del proyecto.
  - Incumplimiento en los requisitos de los perfiles asignados al SOC por cada mes del proyecto.
  - Incumplimientos de las obligaciones en materia de prevención de riesgos laborales.
  - La reincidencia de 3 faltas del mismo tipo catalogadas como graves dentro de un trimestre.
  - Deficiencias que afecten a la imagen de Aguas de Burgos.
  - Extravíos de documentación o fugas de información que puedan afectar de forma grave a la gestión o a la imagen de Aguas de Burgos para con sus clientes.
  - Suministrar información falsa o incompleta con el objetivo de encubrir deficiencias en la gestión, encubrir incumplimientos en los acuerdos de nivel de servicio o para incrementar los importes facturados.
  - El incumplimiento de los tiempos máximos resolución del SOC de cada incidente con prioridad crítica dentro de un mes.
  - El incumplimiento en un periodo mensual del "ANS de Adecuación de Infraestructura IT/OT" obteniendo un valor inferior a 40 puntos.

10.2. Forma de hacer efectiva la penalización

Tendrán penalización los trabajos cuya realización no se ajuste a lo indicado en este Pliego y tengan la consideración de grave o muy grave. La cuantía de las mismas sería de 400 euros para las faltas graves y 1.000 euros para las calificadas como muy graves. A dicho importe se le añadiría el coste total de la intervención por Aguas de Burgos u otro adjudicatario para la corrección del incumplimiento, además de lo indicado en PCAP sobre causas de resolución del Contrato.

Todas las penalizaciones serán acumulativas.

Terminado el trabajo en que se hubiera producido una penalización, ésta se hará efectiva de acuerdo a lo dispuesto en el PCAP.

10.3. Causas específicas de resolución

Además de las causas indicadas en el PCAP, así como las causas previstas en la legislación que sean de aplicación, será motivo de resolución del Contrato con el adjudicatario afectado las siguientes:

- Pérdida o caducidad sin renovación de las certificaciones, adhesiones y cumplimientos que forman parte de los requisitos de solvencia del PCAP.
- Concurrencia durante un semestre en un número superior a cinco (5) penalizaciones graves o muy graves.
- Concurrencia durante un año en ocho (8) penalizaciones graves o muy graves.
- No atender en el plazo de diez (10) días hábiles el requerimiento que hiciera Aguas de Burgos por incumplimiento de las condiciones técnicas o administrativas exigidas para ser admitido a la licitación o para ser admitida la oferta. Entre ellas se incluye la adscripción al contrato de los medios técnicos y humanos mínimos exigidos en este Pliego.
- No cumplir con los compromisos que han sido valorados para la adjudicación.
- El incumplimiento de los hitos y objetivos indicados en el contrato.
- El incumplimiento de los plazos temporales para la realización de los hitos y objetivos indicados en el contrato.
- Las señaladas en este pliego en relación a retrasos de los trabajos, insuficiencia de medios o inobservancia de medidas de seguridad y prevención de riesgos.

En todos los casos anteriores la resolución del contrato con el adjudicatario afectado supondrá la pérdida de fianza definitiva y el resarcimiento de los daños y perjuicios causados a Aguas de Burgos, en su caso.

10.4. Otras penalizaciones y causas de resolución

Aguas de Burgos, salvo justificación aceptada por la propia empresa, podrá imponer al adjudicatario las siguientes penalizaciones, las cuales será acumulativas a las faltas por incumplimiento:

- 0,60 euros por cada 1.000 euros del precio del contrato por cada incumplimiento de cualquiera de las condiciones especiales de ejecución previstas en los pliegos.

- En caso de producirse demora respecto al plazo de DOS (2) MESES para el suministro, instalación, configuración y puesta en marcha en las instalaciones de Aguas de Burgos del hardware y software que renueven al actualmente ya existente en los dos CPD de Aguas de Burgos desde el suministro de las licencias software identificadas durante los trabajos del primer mes, una penalización diaria en la proporción del 0,10% del importe total de la implantación del hardware y software, IVA excluido, por cada día natural de retraso que exceda los DOS (2) MESES para la ejecución de dichos trabajos, hasta un máximo del 25% del importe total de dicha fase.

- En caso de que el cálculo mensual del "ANS de Oficina Técnica de Seguridad Integral (OTSI)" tenga un valor de menos de 85 puntos, se aplicará una penalización, en cada facturación mensual, del 1% del importe mensual de los trabajos correspondientes la Oficina Técnica de Seguridad Integral (OTSI) e Implantación de herramientas del CCN, IVA excluido, por cada punto por debajo de 85 puntos. El importe de la penalización minorara el importe total pendiente de facturación de la fase de adecuación e implantación.

- En caso de producirse demora respecto al plazo de DIECISEIS (16) MESES para la fase de adecuación e implantación, o plazo inferior propuesto por el adjudicatario, una penalización mensual en la proporción del 5% del importe total de la fase de adecuación e implantación, IVA excluido, por cada mes de retraso para la ejecución de dichos trabajos.

- En caso de que el adjudicatario no cumpla con los compromisos de su oferta en cuanto a la presencialidad de medios personales adscritos a la ejecución del proyecto dedicados a la identificación de activos IT/OT, el análisis de riesgos IT/OT y la adecuación al ENS, se aplicará una penalización de 250€ por cada jornada de trabajo de diferencia entre lo ofertado por el adjudicatario y el trabajo presencial efectivamente realizado en instalaciones de Aguas de Burgos.

- En caso de que el cálculo mensual del "ANS de Adecuación de Infraestructura IT/OT" tenga un valor de menos de 40 puntos, se aplicará una penalización de 2 veces el importe equivalente a la desviación de las horas realizadas en el que se hubiera incurrido en el mes respecto a lo estimado.

- En caso de que el cálculo mensual del "ANS de Adecuación de Infraestructura IT/OT" tenga un valor superior a 40 e inferior a 70 puntos, se aplicará una penalización de 1,5 veces el importe equivalente a la desviación de las horas realizadas en el que se hubiera incurrido en el mes respecto a lo estimado.

- En caso de que el cálculo mensual del "ANS de Adecuación de Infraestructura IT/OT" tenga un valor de entre 70 y 90 puntos, se aplicará una penalización de 1 vez el importe equivalente a la desviación de las horas realizadas en el que se hubiera incurrido en el mes respecto a lo estimado.

- 3,5% de la facturación mensual en la fase de operación, IVA excluido, por cada 24 de horas de retraso en la resolución de una incidencia que implique la caída o mal funcionamiento de una o más de las sondas o herramientas SAT-INET, SAT-ICS, GLORIA, EMMA, CARMEN que exceda el plazo máximo de resolución definido en el apartado "6.3.2 Herramientas CCN-CERT" de este pliego.

- 0,4% de la facturación mensual en la fase de operación, IVA excluido, por cada hora de retraso en la resolución, por parte del SOC, de cada incidente con prioridad alta que exceda el plazo máximo de resolución definido en el apartado "6.3.4 Centro de Operaciones de Seguridad (SOC)" de este pliego.

- 1% de la facturación mensual en la fase de operación, IVA excluido, por cada hora de retraso en la resolución, por parte del SOC, de cada incidente con prioridad alta que exceda el plazo máximo de resolución definido en el apartado "6.3.4 Centro de Operaciones de Seguridad (SOC)" de este pliego.

- En caso de que el adjudicatario no facilite la transferencia de información y conocimiento según lo indicado en el apartado "5.1.3.3 Transferencia" de este pliego, se aplicará una penalización del 5% del importe de adjudicación del contrato.

- En caso de que el adjudicatario no facilite la transferencia de información y conocimiento según lo indicado en el apartado "5.5.4 Transferencia" de este pliego, se aplicará una penalización del 5% del importe de adjudicación del contrato.

Cuando la suma de las penalizaciones impuestas en los puntos anteriores alcance el treinta por ciento (30%) del importe de adjudicación del contrato, Aguas de Burgos tendrá derecho a resolver el contrato en los términos previstos en los pliegos.

11. Confidencialidad

El adjudicatario y las empresas ofertantes estarán obligadas a tratar de forma confidencial y reservada tanto la información recibida como la derivada de la ejecución del contrato, no pudiendo ser objeto de difusión, publicación o utilización para fines

distintos a los establecidos en este pliego. Esta obligación seguirá vigente una vez que el contrato haya finalizado o haya sido resuelto.

12. Protección de Datos

Según recogido en la cláusula 32 del PCAP.

13. Evaluación del principio DNSH

Las actuaciones que se lleven a cabo durante la ejecución del contrato respetarán el principio de «no causar un perjuicio significativo al medio ambiente» (principio do no significant harm - DNSH) en cumplimiento con lo dispuesto en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, y su normativa de desarrollo, en particular el Reglamento (UE) 2020/852, relativo al establecimiento de un marco para facilitar las inversiones sostenibles y la Guía Técnica de la Comisión Europea (2021/C 58/01) sobre la aplicación de este principio, así como con lo requerido en la Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del plan de recuperación y resiliencia de España y su documento Anexo. En tal sentido, AGUAS DE BURGOS ha realizado la evaluación inicial del impacto de DNSH para las actuaciones:

- A4. PLAN DIRECTOR DE SEGURIDAD INTEGRAL (GESTIONAR E INTEGRAR LA SEGURIDAD FÍSICA, LÓGICA Y DE LAS PERSONAS)
- A12. CIBERSEGURIDAD

El adjudicatario del contrato colaborará con los servicios técnicos de AGUAS DE BURGOS en la justificación del cumplimiento del DNSH. En concreto, deberá presentar los siguientes informes y declaraciones responsables que acrediten el cumplimiento de estas medidas.

Con el fin de dar cumplimiento a los requisitos establecidos en la Orden HPP/1030/2021, así como en el artículo 17 del Reglamento 2020/852 (principio DNSH), el adjudicatario deberá tener en cuenta que para cumplir los siguientes requisitos DNSH, deberá acreditarlo mediante los siguientes mecanismos de verificación:

Requisito DNSH	Mecanismo de Verificación
En la ejecución de las actuaciones se cumplirán con los requisitos relacionados con el consumo energético establecidos de acuerdo con la Directiva 2009/125/EC para servidores y almacenamiento de datos, o computadoras y servidores de computadoras o pantallas electrónicas, de manera que se compren	1. Marcado CE de los equipos. 2. En su defecto, ficha técnica donde se pueda comprobar el cumplimiento de la norma a verificar

equipos energéticamente eficientes, que sean absolutamente respetuosos con el Code of Conduct for ICT de la Comisión Europea.	
Los equipos utilizados no contendrán las sustancias restringidas enumeradas en el anexo II de la Directiva 2011/65/UE, excepto cuando los valores de concentración en peso en materiales homogéneos no superen los enumerados en dicho anexo.	1. Marcado CE de los equipos. 2. En su defecto, ficha técnica o equivalente donde quede claro que no se han utilizado ninguno de las sustancias calificadas como peligrosas en la mencionada Directiva.

El contratista elaborará un informe acerca del cumplimiento del principio DNSH, que deberá entregar a la finalización de los trabajos objeto del pliego, sin perjuicio del deber de comunicar cualquier riesgo de desviación cuando lo detecte.

14. Información y comunicación

Las actuaciones que se realicen durante la ejecución del contrato deberán cumplir con las obligaciones en materia de información y comunicación conforme a lo establecido en el Artículo 34 del Reglamento (UE) 2021/241, de 12 de febrero, por el que se establece el Mecanismo de Recuperación y Resiliencia; en el Artículo 10 del Acuerdo de Financiación entre la Comisión y el Reino de España; y en el Artículo 9 de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.

Todos los receptores de fondos de la UE tienen la obligación general de reconocer el origen y garantizar la visibilidad de la financiación de la UE recibida, mostrar el emblema de la UE de forma correcta y destacada y reflejar una declaración de financiación sencilla, mencionando la ayuda de la UE.

Se adjunta Manual de comunicación para gestores y beneficiarios del Plan de Recuperación, Transformación y Resiliencia, elaborado por la Secretaría General de Fondos Europeos del Ministerio de Hacienda (edición actualizada a febrero de 2024): https://www.fondoseuropeos.hacienda.gob.es/sitios/dgpmrr/es-es/Documents/MANUAL%20DE%20COMUNICACI%C3%93N%20PARA%20LOS%20GESTORES%20DEL%20PLAN.pdf

Y en todo caso se estará a disposición de lo que establezca al inicio de los trabajos por los responsables técnicos de AGUAS DE BURGOS.

15. Etiquetado verde y digital

De igual modo, se realizará un seguimiento y evaluación del cumplimiento del

compromiso de etiquetado verde y digital conforme dispone la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia, sobre el cual se ha hecho la correspondiente evaluación inicial.

Etiquetado Verde y Digital

METODOLOGÍA DE SEGUIMIENTO PARA EL ETIQUETADO VERDE			
Código	**Descripción del Campo de intervención**	**Coeficiente para el cálculo de la ayuda a los objetivos climáticos**	**Coeficiente para el cálculo de la ayuda a los objetivos medioambientales**
040	Gestión del agua y conservación de los recursos hídricos (incluida la gestión de las cuencas fluviales, medidas específicas de adaptación al cambio climático, reutilización, reducción de fugas)	40%	100%

Esta componente de inversión contribuye sustancialmente a los objetivos medioambientales (Reglamento (UE) 2020/852, del Parlamento Europeo y del Consejo, de 18 de junio de 2020, relativo al establecimiento de un marco para facilitar las inversiones sostenibles y por el que se modifica el Reglamento (UE) 2019/2088), puesto que proporciona la base que permite el uso de herramientas digitales de gestión y ofrece un amplio horizonte temporal de actualizaciones y soporte que garantiza la ciberseguridad de los mismos.

METODOLOGÍA DE SEGUIMIENTO PARA EL ETIQUETADO VERDE		
Código	**Descripción del Campo de intervención**	**Coeficiente para el cálculo de la ayuda a la transición digital**
No aplica	No aplica	No aplica

El adjudicatario del contrato colaborará con los servicios técnicos de Aguas de Burgos en la justificación del cumplimiento de estos compromisos. En concreto, deberá presentar los informes y declaraciones responsables que acrediten el cumplimiento de

estas medidas, cuando sea requerido para ello por el supervisor del contrato.

16. Cuestiones adicionales

16.1. Transferencia tecnológica

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete a facilitar en todo momento a los responsables técnicos de Aguas de Burgos, la información y documentación que éstos soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, herramientas y otros recursos utilizados para resolverlos.

Esta transferencia se realizará de acuerdo con los responsables técnicos de Aguas de Burgos.

16.2. Consultas sobre el pliego de prescripciones técnicas

Los licitadores podrán solicitar información adicional sobre el presente pliego hasta diez días antes de que venza el plazo de licitación que se indica en el pliego de Cláusulas Reguladoras Particulares.

La solicitud se realizará a través de correo electrónico a la dirección contratacion@aguasdeburgos.com

Por Aguas de Burgos se procederá a la contestación de las solicitudes de información adicional que pudieran recibirse mediante correo electrónico. En el caso de que se trate de la resolución de una duda frecuente o que se estime que su conocimiento por todos los licitadores es necesario para garantizar los principios de transparencia e igualdad, se publicará en el perfil de contratante de Aguas de Burgos (https://perfildelcontratante.aguasdeburgos.com/)

No serán atendidas las solicitudes de información adicional que se reciban fuera del plazo habilitado al efecto, o realizadas por procedimiento distinto a los reseñados.