PLIEGO DE PRESCRIPCIONES TÉCNICAS

para adjudicar mediante procedimiento abierto el

CONTRATO DE PROYECTOS DE MEJORA TECNOLÓGICA, Y LA GESTIÓN INTEGRAL INFORMÁTICA DE LA FUNDACIÓN AIC

Contenido

I. Introducción 3
II. Equipamiento AIC 3
III. Alcance 4
1. Proyectos de mejora tecnológica 5
1.1 Sistemas 5
1.1.1 Actualización sistemas 5
1.1.2 Plan de Contingencia 5
1.1.3 Migración a nuevo Sistema de Virtualización 5
1.1.4 Mejora de la topología de red 5
1.1.5 Revisión y reconfiguración Firewall 6
1.1.6 Herramienta de gestión de activos y monitorización 6
1.2 Microsoft 7
1.2.1 Separación de Dominios 7
1.2.2 Separación de Tenants 7
1.3 Ciberseguridad 8
1.3.1 Securización entorno Microsoft y M365 8
1.3.2 Endpoint 10
1.3.3 Formación usuarios 10
2. Soporte y Monitorización de los Sistemas Informáticos 11
2.1 Características y Alcance del Soporte 11
2.2 Tareas que incluye el soporte de Mantenimiento 12
2.3 Funcionamiento del Soporte 13
2.4 SLAs. Niveles de servicio – Penalizaciones. 14
3. Soporte y monitorización de la infraestructura de seguridad 14
3.1 Características del Soporte 14
3.2 Funcionamiento del Soporte 15
3.4 Servicios SOC 15
4. Oficina Técnica 17
4.1 Servicios de Asesoramiento 17
4.2 Servicios de Gestión y Soporte 18
IV. Penalizaciones 20
V. Medios humanos y materiales 21
VI. Continuidad del servicio actual 23

I. Introducción

AIC ha abordado en los últimos años un proceso de adecuación de los Sistemas Informáticos y de la CiberSeguridad de toda su Infraestructura informática y comunicaciones.
Como continuación del proceso llevado a cabo, desea abordar nuevos proyectos de mejora tecnológica desde una perspectiva integral, así como consolidar las actuaciones realizadas hasta la fecha.

II. Equipamiento AIC

A título orientativo, no exhaustivo, a continuación de relaciona el principal equipamiento y software de AIC:

Servidores	• 3 Servidores PRIMERGY RX2540 M6
Almacenamiento	• 1 Cabina de almacenamiento Eternus DX200 S5 • 1 Cabina de almacenamiento Eternus DX60 S5 • 1 Cabina de almacenamiento QNAP TS-1232 PXU • 1 Cabina de almacenamiento QNAP TVS-471U-RP • 1 Cabina de almacenamiento QNAP TS-432PXU-RP
Switching	• 50-80 Switches (Ubiquiti, HP, H3C, NetGear, Fortinet)
Firewalling	• 2 Palo Alto 440 • Fortinet (5G)
Software	• Veeam Backup & Replication • Office 365 • Wasabi • Hornet • Kaspersky antivirus • BrightAuthor • Nec – Naviset - Administrator • Windows Server 2022 Data Center • Windows Server 2016 Standard • Windows Server 2019 Standard • SQL Server 2022 Standard • VMWare v.8.0.3 • Linux • Mac OS • Unifi • Hikvision • Windows 10 y Windows 11 • Software de usuario (Sage, Dorlet, etc.)

Otros	• Video-Wall, • Cámaras Hikvision y Ubiquiti • Móviles Android / iPhone • Equipamiento microinformático; Portátiles, Mac, Impresoras, Pantallas, Dock, equipos de sobremesa, surface, teléfonos VoIP (proveedor externo) • Servidor Grabaciones Unifi y Hikvision • APs H3C y Unifi

III. Alcance

El contrato al que se refiere este pliego se prestará sobre la totalidad de los equipos e infraestructuras tecnológicas de AIC.

El alcance de los servicios cubrirá tanto el front-office como el back office, en sus distintos ámbitos, y requerirá llevar a cabo:

1. **Proyectos de mejora tecnológica**
2. **Soporte y Monitorización de los Sistemas Informáticos**
3. **Soporte y Monitorización de la Infraestructura de Seguridad,** con soporte y gestión para los siguientes elementos
    - Firewall
    - End Point
4. **Oficina Técnica**

Únicamente se encuentran excluidos del presente contrato los siguientes elementos:

- Gastos de inversión de nuevos equipos no incluidos dentro de las actuaciones indicadas en el apartado “Proyectos de mejora de los Sistemas Informáticos”.
- Software informático no incluido dentro de las actuaciones indicadas en el apartado “Proyectos de mejora de los Sistemas Informáticos”.
- Sustitución de piezas defectuosas en equipos o sistemas, pero no las horas de trabajo necesarias para la sustitución de dichas piezas de recambio o puesta en funcionamiento de los nuevos equipos.

Sí estará incluida la recuperación de sistemas (servidores, ordenadores y sistemas de comunicaciones) en caso de ciberataque.

1. Proyectos de mejora tecnológica

1.1 Sistemas

1.1.1 Actualización sistemas

La oferta incluirá la actualización general de entornos versiones de software y firmware de distintos fabricantes: VMWARE, Veeam, Firmware hosts, software servidores, switches, Firewalls, Windows 10, Windows 11, Windows Server 2022 Data Center, Windows Server 2016 y 2019 (lista ilustrativa, pero no exhaustiva).

Se deberán actualizar todos los sistemas a las últimas versiones recomendadas por los fabricantes. Soporte mínimo de fabricantes deseado 3 años.

La oferta del licitante deberá incluir el módulo TPM 2.0 o similar (a efectos estimativos para 3 máquinas).

Tiempo estimado: 8 Jornadas

1.1.2 Plan de Contingencia

La oferta deberá incluir la separación del sistema replicado a otra ubicación.

Tiempo estimado: 2 Jornadas

1.1.3 Migración a nuevo Sistema de Virtualización

El sistema actual de virtualización es VMWARE (finalización de soporte 2027). El servicio deberá incluir la migración a un sistema de virtualización para entornos más pequeños como, por ejemplo, Proxmox, Hyper-V, Azure o AWS.

Tiempo estimado: 10 Jornadas

1.1.4 Mejora de la topología de red

Revisión de la topología de red para mejora y redundancia: Se estima la necesidad de implantar entre 8-10 switches core en Stack, y conectar a ellos el segundo nivel en alta disponibilidad.

Dentro de la topología actual de red existe fibra óptica y cableado UTP.

El hardware deberá estar incluido en la oferta del licitador (estimación ocho switches en stack UNIFI)

Tiempo estimado: 10 Jornadas

1.1.5 Revisión y reconfiguración Firewall

Revisión de las políticas del firewall adaptándolas a las nuevas necesidades, y limpieza de configuraciones de reglas y usuarios obsoletos.

Tiempo estimado: 2 Jornadas

1.1.6 Herramienta de gestión de activos y monitorización

La red de dispositivos de AIC es extensa, con muchos dispositivos conectados: Switches, servidores, PC, cámaras, Antenas WIFI, dispositivos O.T….

Por ello, se considera necesario incorporar una herramienta que gestione todos estos activos, estado, versiones de firmware, comprobación de vulnerabilidades… Además, el servicio deberá incluir una capa de monitorización para ver en tiempo real el estado de los dispositivos y servicios, tiempos de caída de servicio, etc.

En este sentido,

- Se deberá incluir un servicio de monitorización de los dispositivos y servicios de AIC (por ejemplo, PRTG). Este software deberá permitir monitorizar las IP (encendido o apagado) de los dispositivos, pero también distintos parámetros que nos indicarán la salud de la instalación, como, por ejemplo: uso de CPU, uso de RED, servicios web, de BBDD, espacio en disco….

  Se estima la necesidad de gestión de 2500 sensores aproximadamente. El servicio incluirá la instalación, configuración y licencias para, al menos, 3 años.

  Tiempo estimado: 8 jornadas

- Por otro lado, la propuesta incluirá un servicio tipo Lansweeper para la gestión de activos de AIC. El software deberá permitir gestionar el inventario de dispositivos IT y OT, auto-descubrir dispositivos, tener centralizada la información de modelos, números de serie versiones de firmware y software, puertos abiertos… El propio software indicará vulnerabilidades encontradas de los dispositivos y las versiones más recientes de firmwares de cada dispositivo.

  Deberá permitir gestionar al menos 2000 dispositivos, y la oferta incluirá la instalación y configuración, así como las licencias para, al menos, 3 años.

  Tiempo estimado: 8 jornadas

1.2 Microsoft

1.2.1 Separación de Dominios

Separación de Active Directory on-premise

Separar el Active Directory AD actual (compartido por dos empresas) en dos entornos lógicos independientes. Análisis del entorno actual (80-100 usuarios), diseño del nuevo bosque/dominio, preparación de nuevo dominio, relación de confianza entre dominios, servidor de datos conjunto o compartido, migración de cuentas de usuario, grupos y equipos, revisión de GPO, pruebas y soporte al arranque.
Tiempo estimado: 12 jornadas

Controlador de Dominio en Azure (DC en la nube)

Mejorar la disponibilidad del AD desplegando un DC adicional en Azure. El coste de las posibles licencias asociadas se considerará incluido en el precio ofertado (3 años).
Diseño de red (VPN/ExpressRoute según aplique), despliegue de VM DC en Azure, promoción a DC, replicación, hardening básico, pruebas de conmutación, documentación.
Tiempo estimado: 1 jornada

Gestión de actualizaciones (Patch Management)

Implantar una solución centralizada de parches para servidores y equipos.
Evaluación de herramientas (ManageEngine Patch Manager vs Azure Update Manager con ARC), despliegue de la opción seleccionada, alta de servidores y equipos, definición de ventanas de mantenimiento, grupos piloto, informes de cumplimiento.
La oferta incluirá las licencias de la opción escogida por AIC, como referencia tomar 100 computers and single user license / 40 Servers and Single User License.
Tiempo estimado: 3 jornadas.

1.2.2 Separación de Tenants

Separación de tenant de Microsoft 365

Disponer de un tenant independiente, alineado con la separación de AD. Revisión de licencias actuales (Business Basic, Business Standard, Exchange Online Plan 2), diseño de estrategia de migración (identidades, buzones, OneDrive, SharePoint/Teams), configuración de nuevo tenant, migración de los aproximadamente 100 usuarios y servicios, pruebas y soporte.
Tiempo estimado: 12 jornadas

1.3 Ciberseguridad

1.3.1 Securización entorno Microsoft y M365

Cambio a Microsoft 365 Business Premium (100 buzones)

Unificar licencias en Business Premium para habilitar funcionalidades avanzadas de seguridad y gestión.
Revisión de licencias, planificación del cambio, reasignación de licencias, comprobaciones de servicio, revisión de funcionalidades de seguridad disponibles tras el cambio.
El licitador debe incluirlas las licencias en el precio ofertado.
Tiempo estimado: 2 jornadas

Refuerzo de seguridad AD y Entra ID (Secure Score)

Incrementar el Secure Score y reducir riesgos de identidad.
Revisión de recomendaciones de Secure Score, priorización según riesgo e impacto, implementación de medidas (políticas de contraseña, bloqueo de legacy auth, hardening de roles, alertas básicas, etc.), documentación.
Tiempo estimado: 3 jornadas

Implantación de MFA y Acceso Condicional

Reforzar la protección de todos los accesos a Microsoft 365/Entra ID con MFA y políticas de acceso condicional. Diseño de escenarios (oficina, teletrabajo, dispositivos gestionados/no gestionados), definición de políticas (ubicaciones confiables, bloqueo geográfico, riesgo de sesión, etc.), piloto con grupo reducido, despliegue al resto de usuarios, guía rápida para empleados.
Tiempo estimado: 3 jornadas

Despliegue MDM con Intune (Attack Surface Reduction)

Gestionar y securizar todos los PCs corporativos desde Intune.
Alta y configuración de Intune, enrolamiento de aproximadamente 100 PCs, creación de baseline de seguridad, configuración de Attack Surface Reduction (ASR), políticas de antivirus/antimalware, cifrado de disco, control de dispositivos externos, documentación y formación básica al equipo de IT.
Tiempo estimado: 5 Jornadas

Microsoft Defender for Office 365

Protección avanzada del correo y colaboración. Filtro avanzado de phishing y malware, safe links/safe attachments, políticas anti-spoofing. Diseño, despliegue, pruebas y formación.

Tiempo estimado: 1 jornada

Implantación solución PAM (BeyondTrust u otra)

Gestionar cuentas privilegiadas y accesos administrativos de forma controlada y auditada. Análisis de cuentas privilegiadas actuales, diseño de arquitectura PAM (cofre de contraseñas, sesiones remotas, acceso just-in-time), instalación y configuración de la plataforma, alta de sistemas críticos, formación al equipo de IT. Licencia Beyondtrust Password Safe para los usuarios de IT y externos (aproximadamente 20 personas) que deban acceder al sistema como administradores se considerarán incluidas en el precio ofertado por el licitador.

Tiempo estimado: 8 jornadas

AD Audit (5 DC, 2 tenants y servidores)

Auditoría continua de cambios en AD, tenants y servidores críticos.

Instalación y configuración de la herramienta de auditoría (p.ej. ManageEngine AD Audit Plus), alta de los 5 DC, integración con los 2 tenants y servidores definidos, creación de alertas y cuadros de mando básicos, formación a IT.

Tiempo estimado: 3 jornadas

(tomar como estimación 5 Domain Controller / 20 Windows Servers / 2 Azure AD tenants / 2 File servers)

SIEM en la nube (Microsoft Sentinel u otra plataforma)

Centralización de logs de AD, Azure, Microsoft 365, firewall y otros sistemas críticos.

Correlación de eventos y creación de reglas de detección de incidentes.

Puesta en marcha inicial y casos de uso básicos.

Tiempo estimado: 2 Jornadas

1.3.2 Endpoint

Revisión consola Kaspersky

Estabilizar la protección actual mientras se prepara el posible cambio de EDR.
Revisión de la consola, análisis de equipos sin comunicación o con errores, ajuste de políticas, elaboración de informe de hallazgos y recomendaciones.
Microsoft Sentinel:1 jornada

Implantación MDR tipo Sophos

Diseño de arquitectura y políticas, coordinación con partner MDR, despliegue del agente en aproximadamente 100 dispositivos, configuración de exclusiones, pruebas, documentación básica y formación al equipo de IT. Licencia: Sophos MDR Essentials para 100 usuarios y Sophos MDR Essentials for servers deberán estar incluidas en el precio ofertado.
Tiempo estimado: 4 jornadas

1.3.3 Formación usuarios

Implantación sistema de concienciación al usuario

Formación de concienciación en ciberseguridad + campaña de phishing simulado
Despliegue de herramienta de sesiones formativas para usuarios finales (buenas prácticas, phishing, uso seguro de M365).
Campaña de phishing simulado para medir el riesgo y repetir tras la formación.
Preparación, sesiones y análisis de resultados) + licencia de herramienta por usuario de concienciación para 100 usuarios.
Tiempo estimado: 2 jornadas

2. Soporte y Monitorización de los Sistemas Informáticos

2.1 Características y Alcance del Soporte

AIC necesita un servicio de Mantenimiento integral de sus sistemas informáticos, tales como:

- Servidores Físicos
- Servidores Virtuales
- Entorno de virtualización
- Gestión de los Backup
- Cabinas de Almacenamiento Principal
- Cabinas de Almacenamiento Secundario
- Aplicaciones que corren en los servidores
- Switches
- AP
- Entorno WIFI
- Gestión del Filtrado de Correo
- Firewall

El mantenimiento debe cubrir las siguientes áreas de trabajo:

- Mantenimiento del Hardware Físico
- Mantenimiento del entorno de Virtualización
- Mantenimiento de las Máquinas Virtuales
- Mantenimiento de los Sistemas Operativos
- Mantenimiento y Gestión de la solución de Filtrado de Correo.

A efectos estimativos, se considerarán;

- 2 Firewalls
- 3-5 NASes
- 3 servidores físicos
- 10-20 equipos independientes (semi servidor)
- 2-5 cabinas de almacenamiento
- 50 máquinas virtuales
- 50-80 switches
- 70-100 APs

Todos estos elementos descritos son el CORE de la infraestructura informática de AIC, y para asegurar su buen funcionamiento la oferta incluirá la monitorización de los mismos.
La empresa adjudicataria tendrá actuar de forma proactiva ante una posible incidencia.

Deben estar incluidas las intervenciones tanto a nivel Software como Hardware.

El adjudicatario debe asegurarse que los servidores estén permanentemente bajo el soporte de fabricante.

La disponibilidad de los sistemas debe ser del 100%.

Los trabajos que supongan corte de servicio a los usuarios deberán ser realizados fuera de horario normal.

Así mismo, el alcance de los trabajos comprende:

- Documentación y generación de informe de la Instalación.
- Desplazamientos que resulten necesarios para la correcta ejecución del servicio.
- Transmisión de Conocimiento.

2.2 Tareas que incluye el soporte de Mantenimiento

El soporte de mantenimiento debe incluir las siguientes tareas:

- Diagnóstico de la incidencia mediante pruebas “in situ” o por soporte remoto.
- Trámites y Gestión de incidencias en garantía con el fabricante.
- Asistencia “in situ” para reparación y configuración.
- Trabajos complementarios para completar la reparación efectuada por el fabricante.
- Recuperación de datos desde las copias de seguridad a causa de una avería.
- Monitorización diaria de los Backup.
- Préstamo de equipo sustitutorio.
- Diagnóstico inicial de la instalación. Checklist.
- Actualización de parches y versiones recomendadas por los fabricantes para la mejora del sistema.
- Supervisión de las condiciones eléctricas, medioambientales y de seguridad que afectan a los sistemas informáticos.
- Servicio todo incluido: Piezas*, mano de obra, desplazamiento y otros gastos de la intervención incluidos.

    *Mano de obra incluida. Para el material se reutilizarán otros equipos si esto fuera posible, o bien se propondrá a AIC la compra del repuesto necesario.
- Checklist periódico preventivo.
- Implantación de un sistema de monitorización en servidores y dispositivos críticos. El sistema tiene que monitorizar en 24x7 como mínimo los siguientes elementos:

    - Alertas ante cualquier error hardware en los elementos monitorizados (Servidores, Almacenamiento Principal, Almacenamiento Secundario, Entorno de Virtualización, Servidores Virtuales, etc.)
    - Agentes de tarjetas de red
    - Alertas de agentes de almacenamiento
    - Reinicio inesperado del servidor.
    - Caída del proceso del programa de copias.
    - Espacio en disco mínimo en particiones de sistema (<80% warning, < 90% Alerta)
    - Memoria RAM usada superior al 90% durante más de 8 horas.
    - CPU por encima del 95% durante más de 4h.
    - Equipo sin conexión durante más de 1 hora.
    - Uso y evolución de datastores, NASs de backup
- Todas las alertas emitidas por los componentes críticos deberán ser supervisadas diariamente en tiempo real por el departamento técnico del adjudicatario. El objetivo es actuar antes de que se produzca una incidencia evitando de este modo que el funcionamiento de la plataforma se vea afectado.
- La empresa adjudicataria deberá hacer revisiones periódicas de la infraestructura, para lo que desarrollará un plan de inspecciones.
- Se tendrá de llevar a cabo la sustitución de componentes dudosos.
- Llevar a cabo Auditorias, análisis y consultoría preventivas.
- Implantación de alertas en los sistemas de Backup, control de las copias de seguridad.
- Control de las garantías de todos los elementos Hardware y Software.

2.3 Funcionamiento del Soporte

El Soporte mínimo será de 9:00 a 18:00 de lunes a jueves. Viernes de 08:00h a 14:30. En caso de incidencia grave o muy grave, el soporte deberá ser 24 horas.
Las notificaciones de una incidencia podrán reportarse de las siguientes maneras, siendo la interlocución exclusiva entre la persona designada por AIC y el gestor/responsable que designe el contratista:

- Llamada Telefónica
- Correo Electrónico

2.4 SLAs. Niveles de servicio – Penalizaciones.

La licitante presentará en su oferta los niveles de servicio comprometidos, al menos en los apartados descritos a continuación.

Solicitud	**Tiempo máximo de Respuesta**
Incidencia Alta – Muy Grave	Inmediato
Incidencia Media– Grave	<= 4 horas
Incidencia Baja – Leve	<= 8 horas
Cambio de configuración	<= 8 horas
Petición de información	<=48 horas

3. Soporte y monitorización de la infraestructura de seguridad

Tanto la infraestructura de Firewall como la infraestructura de End Point al ser elementos críticos dentro de AIC deberán ser tratado por un soporte especializado.
Este servicio supondrá la gestión de las diferentes plataformas de seguridad por personal con experiencia contrastada en ellas, encargándose del funcionamiento, configuración, actualización y gestión de las diferentes incidencias que puedan suceder.

3.1 Características del Soporte

El Soporte tanto para la infraestructura de Firewall como para la infraestructura de End Point debería tener las siguientes características:

- Análisis y Gestión de Incidencias del Producto
- Consultas sobre el producto contratado
- Intervenciones del Soporte remoto sobre las consolas
- Aplicaciones de medidas extraordinarias contra amenazas
- Actualizaciones críticas de versión
- Monitorización, como mínimo, de:
    - Fallos en el clúster de HA
    - Estado de la CPU
    - Estado de la Memoria
    - Error de Paquetes
    - Sesiones

    - Estado de las Interfaces
- Modificación de reglas
- Modificación de perfiles de acceso
- Aplicación de la solución ante incidencias
- Actualización y parches
- Actualizaciones de la Plataforma
- Presentación de informes del servicio semestralmente
- Monitorización 24x7

3.2 Funcionamiento del Soporte

El Soporte mínimo será de 9:00 a 18:00 de Lunes a jueves y Viernes de 08:00h a 14:30. En caso de incidencia grave o muy grave deberá ser de 24 horas.
Las notificaciones de una incidencia podrán reportarse, al menos, de las siguientes maneras, siendo la interlocución exclusiva entre la persona o personas designadas por AIC y el gestor/responsable que designe el contratista:

- Llamada Telefónica
- Correo Electrónico

3.3 SLAs. Niveles de servicio

El licitador presentará en su oferta los niveles de servicio comprometidos, al menos en los apartados descritos en la tabla a continuación.

Solicitud	**Tiempo máximo de Respuesta**
Incidencia Alta – Muy Grave	Inmediato
Incidencia Media– Grave	<= 4 horas
Incidencia Baja – Leve	<= 8 horas
Cambio de configuración	<= 8 horas
Petición de información	<=48 horas

3.4 Servicios SOC

La empresa deberá implementar servicios SOC para su infraestructura de Firewall y End Point, así como servicios SOC para el Microsoft 365, AD, Servidor de ficheros, etc.
La empresa licitadora deberá disponer de varios SOC replicados.
Los servicios mínimos que debe dar la empresa contratada son los siguientes:

- Monitorización de seguridad (IT)
- Gestión extendida de vulnerabilidades

- Respuesta frente a incidentes
- Listados de IOCs
- Actividad Red Team
- Threat Intelligence services

La empresa licitadora deberá implementar los siguientes Servicios:

- Servicio SIEM gestionado
- Monitorización y alerta de seguridad (IT) 24x7x365
- Gestión de vulnerabilidades extendida
- Asesoramiento a incidentes según horario establecido / críticos 24x7x365
- Inteligencia IOCs
- Actividad Red Team
- Vigilancia Deep/Dark Web – ID Protection
- Gestión del Servicio entre personal del servicio e interlocutor de AIC:
    - Informe mensual
    - Reunión mensual de seguimiento
        - Servicio: Volumetría, taxonomía amenazas, etc.
        - Recomendaciones: Medidas evolutivas, planificación, etc.
    - Portal (Ticketing, histórico, …)
    - Plataforma ejecutiva de visualización
        - Dashboard Amenazas
        - Dashboard Riesgos
        - Dashboard Amenazas mundiales (Globo terráqueo con IPs maliciosas)
        - Dashboards parametrizables a medida
    - Reporting

En la oferta presentada tiene que estar descrito con todo tipo de detalle el proceso de implementación del Servicio, incluyendo como mínimo las siguientes Fases:

- Fase 1. Proyectos de mejora y Prestación Servicio.
- Fase 2. Prestación del Servicio y Mejora Continua.
- Fase 3. Devolución del Servicio.

En la oferta también tiene que ser descrita la metodología de trabajo.

4. Oficina Técnica

4.1 Servicios de Asesoramiento

AIC necesita disponer de una Oficina Técnica para asesoramiento en todo lo relacionado a los Sistemas y Seguridad de la empresa que abarca distintos ámbitos:

- Asesoramiento con todo lo relacionado con la parte de Infraestructura de Sistemas:
  - Servidores
  - Almacenamiento
  - Virtualización
  - Sistemas Operativos de Servidores
- Asesoramiento en todo lo relacionado con la parte de Infraestructura de Seguridad:
  - Firewall
  - End Point
  - Seguridad Perimeral
- Soporte en las decisiones de Ciberseguridad y tecnologías de Ciberseguridad que se puedan plantear en los distintos ámbitos de decisiones desde el ámbito técnico al directivo.
- Alineamiento de los procesos de Ciberseguridad con los procesos internos y con las buenas prácticas, normas internacionales o requerimientos legales de los que se dispone en la actualidad y en el futuro.
- Formación y sensibilización en materia de Ciberseguridad y tecnologías de Ciberseguridad tanto al personal técnico interno, gestores o directivos, como a los prestadores de servicio que puedan interactuar con activos de AIC.
- Asesoramiento por expertos de los distintos ámbitos de las Ciberseguridad:
  - Asesoramiento experto en Políticas, normas y procedimientos
  - Asesoramiento experto para el diseño de integración de soluciones.
  - Asesoramiento experto para la monitorización y gestión de incidentes
  - Asesoramiento experto para auditorías técnicas de seguridad
  - La prevención de incidentes de Ciberseguridad.
  - La resolución de incidentes de Ciberseguridad.
  - La minimización de impactos si el incidente se produce.
- Asesorar a AIC en la toma de decisiones estratégicas en relación con los temas informáticos y de Ciberseguridad.
- Llevar a cabo la gestión de las cámaras de seguridad de AIC y, en general VLANs existentes y de nueva creación que se requieran (por ejemplo, CCTV seguridad,

elementos o dispositivos nuevos IoT…), así como la gestión de la aplicación de accesos implementada.

4.2 Servicios de Gestión y Soporte

Los servicios que se presten por parte de la Oficina Técnica podrán ser en remoto desde el centro de trabajo del contratista, salvo los relativos a la prestación de soporte técnico a los usuarios, que deberá prestarse en AIC.

Las funciones de la oficina técnica serán las siguientes:

- Dar soporte a la infraestructura de Sistemas
- Dar soporte a la infraestructura de Firewall
- Dar soporte a la infraestructura de End Point
- Dar soporte a la infraestructura de red
- Gestión del Parque de Equipos Informáticos, incluidos portátiles, pantallas, equipos de sobremesa, proyectores, video-wall, TV, etc. tanto el hardware como el software.
- Gestión del Parque de Equipos de impresión
- Gestión de teléfonos
- Gestión de las comunicaciones entre edificios y/o Salida de Internet
- Gestión Parque Wifi Privado y Público.
- Mantenimiento Preventivo de las infraestructuras de AIC.
- Atención de Usuarios (CAU).
- Ser el interlocutor entre las distintas áreas de soporte contratadas.
- Realizar una mejora continua de los Sistemas Informáticos, tanto a nivel de puestos, Servidores, Seguridad, etc.
- Gestión tecnológica de las cámaras de seguridad de la AIC y, en general de las VLANs, así como la gestión de la aplicación de accesos implementada actualmente
- Disponer de conocimiento de entorno Mac ya que parte de la infraestructura de microinformática de AIC está basada en Sistemas Mac.

Este soporte incluirá también las tareas de creación de nuevas cuentas, migración de cuentas, preparación de nuevos equipos, tanto de personal propio, como de personal colaborador (se estiman alrededor de 25 nuevos equipos / modificaciones al año), y cualquier otra tarea relacionada con la gestión microinformática.

El equipo adscrito al servicio deberá tener conocimiento específico y experiencia en los distintos elementos de hardware y software descritos en el pliego, así como en proyectos de alcance similar.

Funcionamiento del Soporte a Usuarios

El soporte a usuarios (CAU) ofrecido por la adjudicataria será el primer nivel de recepción de averías, problemas o consultas técnicas sobre el servicio. La adjudicataria deberá registrar la incidencia, activar un ticket o avería asociada y el procedimiento para su resolución. Deberá posteriormente informar al llamante de la evolución de la avería o problema, y finalmente, de su resolución o respuesta final.

Deberá disponer de una formación específica en trato y atención al público. Aquella persona que así lo desee deberá poder comunicarse en Euskera con este servicio.

La adjudicataria pondrá a disposición del público un número de teléfono de bajo coste para el llamante.

La adjudicataria dispondrá de una cuenta de correo electrónico de entrada, que podrá ser utilizada por clientes, usuarios, técnicos de AIC y contratas de mantenimiento para la notificación de incidencias. La respuesta a una notificación por esta vía debe ser inmediata, con un email de acuse de recibo e indicación de código de incidencia asignada.

En general la adjudicataria asumirá todos los costes asociados a los canales de comunicación salientes con el exterior y con AIC. La adjudicataria podrá proponer cuantas vías adicionales de contacto considere adecuadas como mejora, siendo éstas tenidas en cuenta en la valoración de la oferta.

Los cortes de servicio programados motivados por mantenimiento preventivo o nuevas instalaciones serán comunicados al CAU, y deben ser atendidos como incidencia, con una clasificación que los distinga.

Uno o múltiples avisos o eventos de red detectados podrán generar una incidencia, que puede clasificarse en avería, preventivo, problema o consulta. La persona operadora del CAU deberá asignar la resolución de la incidencia y realizar un posterior seguimiento de la evolución de la incidencia, anotando líneas de progreso y explicaciones sobre el detalle de la incidencia a medida que se van conociendo.

La adjudicataria incluirá para la gestión de las incidencias una aplicación, cuyo coste estará incluido en el servicio, que deberá describir adecuadamente en su propuesta, en el apartado de medios materiales. Se deberá justificar adecuadamente las características y ventajas que la nueva herramienta aportaría al servicio. Se deberá permitir el acceso a los responsables técnicos de AIC en los diferentes perfiles, de consulta o incluso generación, modificación y cierre de incidencias.

AIC deberá tener completa accesibilidad a los datos internos contenidos en la aplicación. Las licencias asociadas a esta nueva aplicación deberán ser suministradas a AIC y deberán poder ser utilizadas por ésta en el futuro sin costes adicionales. En cualquier caso AIC se reserva la decisión de implantar la herramienta propuesta u otra, en este segundo caso, el coste correrá

a cuenta de AIC.

Se estima que, del personal interno de AIC que deba tener acceso a la aplicación, 2 de ellos deberán tener perfiles operativos/administrativos, y se requerirán 2 perfiles consultivos.

La adjudicataria será responsable de la explotación de los datos de la aplicación de incidencias, preparará y entregará a AIC los informes que éste requiera. Estos informes tendrán una periodicidad mensual, y tendrán detalles de desglose de incidencias por día y mes, según tipos de incidencias, etc. También contendrán reportes de cumplimientos de los SLA de AIC, en función de los tiempos y nº de incidencias de cada servicio. La cantidad de informes, su contenido y presentación podrán variar durante la prestación del servicio según las instrucciones de AIC dentro de un proceso de mejora continua.

IV. Penalizaciones

AIC y la adjudicataria acordarán un modelo de relación, en la fase de arranque del servicio, en el que se establecerán las pautas principales que regirán la prestación del servicio y la comunicación entre ambas entidades.

Dentro de este modelo se deberán contemplar al menos los compromisos derivados de los pliegos técnicos, la oferta de la adjudicataria y los términos del contrato firmado en la adjudicación. Se definirán las periodicidades de reuniones y análisis conjuntos, frecuencia, formato y contenido de los informes, roles, etc.

Siempre deberá respetar los compromisos adquiridos y reflejados en los pliegos, oferta de la adjudicataria y contrato firmado. Se establecerá un acuerdo de nivel de servicio (SLA) con la adjudicataria, que contendrá al menos los siguientes puntos:

SLA	**Descripción y cálculo**	**Penalizaciones relacionadas**
SLA1 Cumplimiento de la calidad del servicio	Recoge el cumplimiento con la calidad adecuada de los compromisos recogidos en los pliegos, oferta, contrato y modelo de relación, que no estén incluidos en el resto de SLAs acordados. Se mide en nº de no conformidades con el servicio.	200 € por cada No conformidad leve 600 € por cada No conformidad grave o muy grave (comporta discontinuidad en la prestación del servicio, o 3 No conformidades leves en un mismo año)
SLA2 Entrega de documentación	Mide los plazos de entrega, formato y contenido de los informes según los criterios recogidos en el modelo de relación.	50 € por cada informe presentado con errores. 50 € por cada día de retraso en la entrega de informes con respecto al plazo acordado.

El oferente podrá asumir compromisos adicionales de nivel de servicio dentro de su oferta.
La no obtención de los niveles de calidad requeridos se reflejará en el incumplimiento de los SLA acordados, que comportará la consiguiente penalización, según se indica en la Tabla anterior.
El cálculo y aplicación de las penalizaciones se realizará en base a los siguientes criterios:

- La penalización se calculará por cada periodo establecido en el modelo de relación, con una periodicidad mínima anual. Será acumulativa en caso de más de un incumplimiento durante el periodo. No superará nunca un límite del 20% de la facturación del periodo.
- La penalización se detraerá de la facturación del mes o meses siguientes al periodo afectado.
- La obtención de los valores de los indicadores de cada servicio al final de sus correspondientes periodos de cálculo, y en su caso, los importes de las penalidades asociadas, deberá ser realizada por la Adjudicataria y presentadas a AIC dentro de los cinco días laborables siguientes a la finalización del periodo de cálculo.
- Los datos presentados por la Adjudicataria podrán ser contrastados y supervisados por AIC en cualquier momento. La manipulación intencionada de los datos presentados será considerada como falta grave y penalizada con un 5% adicional a las penalidades que hubiesen correspondido.
- AIC se reserva el derecho de condonar cualquier penalidad a cambio de compromisos del adjudicatario, cuantificables en tiempo y costo, conducentes a conseguir mejoras tangibles en los indicadores incumplidos. La existencia de penalidades que alcancen o superen el 10% del importe de la facturación durante tres periodos consecutivos, será considerada como una falta grave, pudiendo ser causa de rescisión del Contrato con un preaviso de dos meses de antelación.

V. Medios humanos y materiales

Adicionalmente, y en atención a la naturaleza eminentemente técnica del contrato, los licitadores deberán adscribir a la ejecución del mismo, como mínimo, los medios humanos y materiales mínimos siguientes:

- Un gestor / responsable del Servicio que deberá acreditar la posesión de una experiencia de al menos ocho años en el ámbito del objeto del contrato que asumirá las funciones de interlocutor con AIC, encontrándose localizable las 24 horas. Entre sus funciones se encuentran las siguientes:
    - Participar en el Comité Técnico de seguimiento que se constituya para la

regulación y seguimiento de la puesta en marcha, evaluación del proyecto y decisiones estratégicas que se adopten.

- Velar por el cumplimiento de las condiciones establecidas en el modelo de relación. Para ello participará en cuantas reuniones periódicas o extraordinarias se convoquen, y aportará la documentación e informes precisos para la toma de decisiones en dicho comité.
- Proponer mejoras o modificaciones en la operativa del servicio que ayuden a mejorar las prestaciones. Obtención de datos y presentación de informes sobre la calidad del servicio prestado, aportando datos objetivos de cumplimiento de SLAs del proyecto.
- Coordinación de asistencias a reuniones, generando las convocatorias, agendas del día, actas posteriores, etc.
- Atender a las indicaciones de AIC con respecto a las correcciones o modificaciones pedidas para la prestación efectiva del servicio adecuándose a las prescripciones de este pliego.
- Realizar la elaboración y revisión periódicas de los procesos y procedimientos que deben regir como referencia para la ejecución del contrato, y que deben ser de obligado cumplimiento para la empresa adjudicataria. AIC se reserva el derecho de aprobar las modificaciones propuestas por la adjudicataria.
- Adaptar la organización de la adjudicataria para incluir dentro del servicio aquellos nuevos subsistemas de red, monitorización o aplicaciones de gestión que AIC decida adoptar para la atención a usuarios y monitorización y gestión del servicio. Asimismo, deberá adaptar su organización para soportar ampliaciones de red, nuevos clientes, SLAs o actividades en general que aborde AIC durante la vigencia del contrato.
- Atender y orientar adecuadamente el tratamiento en horario laboral de aquellas incidencias de especial relevancia, aconsejando a los técnicos del CAU.
- Mantener cuantas reuniones sean precisas con los responsables de AIC, así como acudir al centro cuando sea preciso.

- Técnicos suficientes con la dedicación y cualificación necesaria para dar respuesta a las distintas necesidades del pliego; Sistemas, Microinformática, Entorno Windows, Entorno Mac, CAU, SOC, Ciberseguridad, gestión de servicios TI, Mac, M365…

En concreto, para la correcta prestación de este servicio de soporte técnico a los usuarios se deberá garantizar la asistencia permanente de, al menos, un técnico a las instalaciones de Amorebieta, los 12 meses del año, de lunes a jueves de 9:00 a 18:00 y los viernes de 8:00 a 14:30. Únicamente no habrá presencia física los días festivos de cierre completo del Complejo

(festivos nacionales y locales, que se indicarán al inicio del contrato). El resto de fechas, aunque el calendario de AIC no determine día laboral, habida cuenta de que en el Complejo hay otras empresas trabajando, deberá haber presencia física.
El personal contará, al menos, con nivel inglés equivalente a «FIRST» (B2 Cambridge English).

VI. Continuidad del servicio actual

La empresa adjudicataria deberá asegurar la continuidad del servicio procurando una transición adecuada con el proveedor actual. Para ello deberá, en un plazo máximo de dos meses desde la firma del contrato, haber realizado la migración del servicio. El coste de esta transición será por cuenta de la adjudicataria y estará incluido en el precio global ofertado.
Se adoptarán los procedimientos actuales de recepción de llamadas, asignación de resolutores, clasificación, líneas de progreso, etc.

MARIA TERESA ALBA ZUBIZARRETA - 16053810V

Firmado digitalmente por MARIA TERESA ALBA ZUBIZARRETA - 16053810V
Fecha: 2025.12.23 16:27:31 +01'00'