Cruz Roja

SOLICITUD DE SERVICIOS:

CONDICIONES BÁSICAS Y TÉCNICAS PARA LA CONTRATACIÓN DE SERVICIOS DE CIBERSEGURIDAD

CRUZ ROJA ESPAÑOLA

Sept. 2025

Cruz Roja

CONDICIONES BÁSICAS PARA LA CONTRATACIÓN DE SERVICIOS DE CIBERSEGURIDAD

CONDICIONES BÁSICAS PARA LA CONTRATACIÓN DE SERVICIOS DE CIBERSEGURIDAD

ACLARACIONES E INTERPRETACIONES

Las empresas interesadas podrán solicitar a Cruz Roja Española, en el ***e-mail:*** sistemas.informacion@cruzroja.es*; las* ***aclaraciones e interpretaciones*** *que estimen convenientes sobre los documentos que forman parte de esta convocatoria y hasta las 12 h. del* ***viernes 17 de octubre del 2025****.*

A ninguna empresa solicitante se le hará interpretación oral de los documentos que forman parte de esta convocatoria.

Si como resultado de una aclaración o modificación en los documentos de esta convocatoria surgiesen cambios sustanciales, CRE podrá otorgar una ampliación del plazo para la presentación de las ofertas. Lo que, en su caso, ***se publicará en el mismo canal que la convocatoria.***

El plazo de ***entrega de las ofertas*** *será hasta las* ***12 h. del viernes 24 de octubre del 2025****.*

INFORMACIÓN TÉCNICA DE REFERENCIA PARA LA CONTRATACIÓN DE LOS SERVICIOS

Dado el carácter sensible de la información técnica relacionada con los servicios de ciberseguridad, esta ha sido incluida en un documento específico (ANEXO 5).

Para acceder al contenido, las empresas interesadas deberán firmar previamente un Acuerdo de Confidencialidad (NDA), solicitándolo por correo electrónico a sistemas.informacion@cruzroja.es. Una vez recibido el NDA firmado, se enviará el Anexo 5 a la dirección de contacto indicada.

EXPOSITIVO

Cruz Roja Española (en adelante, “CRUZ ROJA”, "CRE" o la “Institución”) es una Institución humanitaria de carácter voluntario y de interés público que desarrolla su actividad bajo la protección del Estado a través del Ministerio de Derechos Sociales y Agenda 2030, ajustándose a lo previsto en los convenios internacionales sobre la materia en los que España es parte, al Real Decreto 415/1996, de 1 de marzo, por el que se establecen las normas de ordenación de la Cruz Roja Española, a sus estatutos aprobados por Orden SCB/801/2019, de 11 de julio, por la que se publica el texto refundido de los Estatutos de Cruz Roja Española, a la legislación que le sea aplicable y a sus propias normas internas.

CRE ha decidido iniciar un procedimiento de convocatoria para la contratación de los servicios de **CIBERSEGURIDAD.**

Los servicios indicados en el presente documento deberán ofrecerse por especialistas acreditados en realizar las actividades asociadas a los servicios durante el período especificado en la CLÁUSULA 15. DURACIÓN DEL CONTRATO.

La entidad que resulte seleccionada para la prestación del servicio entenderá las especificaciones de este documento como requisitos mínimos del servicio a proporcionar, valorándose positivamente las mejoras que aporte en su oferta, siempre y cuando se cumplan los procedimientos aplicables y las condiciones y especificaciones recogidas en la presente petición de oferta y anexos.

La mera participación en el presente proceso de Petición de Ofertas (en adelante RFP o la Convocatoria) implicará la aceptación por parte de las entidades ofertantes de los términos y condiciones establecidas en el presente documento y las aclaraciones o anexos posteriores que se pudieran emitir. En su oferta las entidades deberán indicar explícitamente la aceptación de dichos términos y condiciones incluyendo aquellos recogidos en los *Anexos*.

CRE se reserva el derecho de modificar, suspender o cancelar el proceso de Petición de Ofertas en cualquier momento, así como decidir no seleccionar ninguna entidad, a su entera discreción, sin que el ejercicio de los anteriores derechos dé lugar a indemnización alguna a favor de las entidades solicitantes.

CRE se reserva el derecho de incluir/excluir en la descripción del servicio de esta RFP cualquier elemento de las soluciones previamente presentadas por los proveedores, como posibles alternativas.

Las propuestas de ofertas se presentarán siguiendo las indicaciones del apartado *"Instrucciones para la presentación de ofertas"* de este documento y antes del plazo límite indicado. Cualquier oferta entregada fuera de tiempo no se tendrá en cuenta.

CONDICIONES Y REQUISITOS EXIGIBLES PARA LA CONTRATACIÓN DE LOS SERVICIOS

CLÁUSULA 1. OBJETO

La presente convocatoria o RFP tiene por objeto solicitar a las entidades interesadas para que hagan llegar sus propuestas (técnica y económica) con un precio y condiciones vinculante para la contratación de un servicio integral de atención al usuario, orientado a la atención, gestión y resolución de incidencias, solicitudes y requerimientos relacionados con los servicios tecnológicos.

Las características técnicas objeto del servicio, se definen en el documento que se acompaña como **Anexo 1- Condiciones y Requisitos Técnicos (CRT)**, que reviste idéntico carácter obligacional que las presentes condiciones básicas, en cuanto forman parte inescindible de la presente convocatoria.

Las entidades ofertantes que así lo consideren podrán añadir a su oferta, además de lo solicitado en las CRT, las eventuales mejoras que estimen convenientes, prevaleciendo en este sentido el criterio de la Institución sobre la adecuación de la propuesta a las necesidades de CRE.

La entidad seleccionada habrá de mantener igualmente con la Institución, compromiso de atención prioritaria a CRE en las condiciones ofertadas.

Tienen carácter contractual los siguientes documentos, relacionados por orden de prelación en cuanto al valor de sus especificaciones en caso de omisión o aparente contradicción:

A. Las condiciones fijadas en el propio documento del contrato que finalmente se concrete como resolución de la presente RFP.
B. Las presentes Condiciones Básicas y Técnicas y las Condiciones y Requisitos Técnicos (CRT)

C. El resto de documentación que conforman el encargo.

CLÁUSULA 2. PRESUPUESTO

En la oferta económica que presenten las entidades se deben detallar las funciones y tareas a realizar.

CRE no establecerá un presupuesto máximo para estos servicios. Cada entidad ofertante deberá realizar su propia estimación económica en función de los requerimientos y condiciones establecidas en las presentes condiciones, asegurando la viabilidad y adecuación de su oferta a las necesidades descritas.

Las ofertas económicas deben presentarse con el IVA desglosado y el presupuesto incluirá todos los gastos asociados directa o indirectamente al presente proyecto.

CLÁUSULA 3. LUGAR DE ENTREGA

La documentación técnica de la convocatoria podrá obtenerse de la propia página web de Cruz Roja.

CLÁUSULA 4. ANUNCIOS

La convocatoria se publicará en la página web institucional de Cruz Roja Española en internet (www2.cruzroja.es) en el apartado de *Licitaciones*.

CLÁUSULA 5. PROCEDIMIENTO DE SELECCIÓN

CRE seleccionará para la prestación del servicio a la entidad que haya presentado la oferta que resulte más ventajosa a juicio del órgano designado por CRE para dicha valoración, de entre todas las presentadas en el plazo habilitado para ello.

CLÁUSULA 6. PROPOSICIONES DE LAS ENTIDADES OFERTANTES: NORMAS GENERALES

Podrán presentar sus proposiciones a esta convocatoria las personas naturales o jurídicas, nacionales o extranjeras de Estados miembros de la Unión Europea, que, teniendo plena capacidad de obrar, acrediten su solvencia técnica, económica y financiera.

Las entidades concurrentes habrán de respetar el CÓDIGO DE CONDUCTA DE CRE, http://www.cruzroja.es/docs/2006_34_CN/CodigodeconductaCRE.pdf, que comprende el compromiso de respeto a los 10 PRINCIPIOS DEL PACTO MUNDIAL DE LAS NACIONES UNIDAS y estarán sujetos a principios de la ética empresarial que garanticen, al menos, su integridad, objetividad, así como su competencia profesional y diligencia debida, en garantía del correcto desempeño de la actividad desarrollada por la Institución y del buen fin del contrato.

La Institución se reservará el derecho de anular en cualquier momento el contrato que la vincule con un proveedor en el caso de que las actividades de este, no respeten los criterios éticos establecidos por la Institución, comprometan de alguna forma el adecuado cumplimiento de sus fines, la actividad social que desarrolla, o el respeto y el prestigio debidos a su nombre y emblema.

Tampoco podrán contratar con CRE aquellas entidades cuyos órganos de gobierno o administración formen parte, por sí o por persona interpuesta, alguna persona directiva o empleada de CRUZ ROJA ESPAÑOLA. Siendo además un requisito imprescindible para contratar que las entidades concurrentes estén al corriente del cumplimiento de sus obligaciones: para con su personal empleado o trabajador, tributarias y con la Seguridad Social de acuerdo con las disposiciones normativas que resulten de aplicación.

CLÁUSULA 7. PRESENTACIÓN DE OFERTAS

7.1.- La presentación de ofertas implica el conocimiento y la aceptación incondicional de las cláusulas de las presentes condiciones y de los documentos técnicos que rigen esta Convocatoria, así como la declaración responsable de que la entidad concurrente reúne todas y cada una de las condiciones exigidas para contratar.

A tal efecto la oferta que se proponga deberá plantearse de acuerdo con el modelo que se adjunta como **Anexo 4 - Proposición económica y criterios automáticos** de las presentes Condiciones y revestirá carácter vinculante. Asimismo, se habrá de presentar declaración responsable suscrita por persona con capacidad bastante para representar a la entidad, y en los términos previstos en el **Anexo 3 - Declaración Responsable**, por el cual la entidad ofertante manifieste reunir todas y cada una de las condiciones exigidas para contratar.

7.2.- Las interpretaciones respecto a estas Condiciones y demás documentos rectores de la convocatoria se resolverán **exclusivamente por escrito** y las consultas que se pretendan formular deberán dirigirse a la siguiente dirección de correo electrónico: **sistemas.informacion@cruzroja.es**

7.3.-Las entidades participantes deberán presentar sus ofertas en dos sobres físicos (Sobre A y Sobre B), conforme a lo establecido en la Cláusula 8 del presente pliego. La documentación podrá presentarse en formato papel; no obstante, se recomienda que sea en **formato digital**, almacenada en un dispositivo físico de memoria (por ejemplo, pendrive), que deberá incorporarse dentro del correspondiente sobre.

La entrega de los sobres deberá realizarse en el Registro General de la Oficina Central de Cruz Roja Española, situada en la Avenida Reina Victoria, número 26, en Madrid, antes de las **12:00 horas del viernes 24 de octubre de 2025**, dirigida a la Secretaría General de la Institución. La presentación podrá ser realizada por cualquier persona en nombre de la entidad interesada.

Adicionalmente, con el fin de facilitar el proceso de revisión, se solicita que se remita una copia en formato PDF de la documentación contenida en el Sobre B (oferta técnica y económica) al correo electrónico sistemas.informacion@cruzroja.es.

7.4.-En ningún caso se admitirán las propuestas entregadas en el mencionado Registro fuera del plazo anteriormente establecido.

La entidad ofertante presentará también un escrito donde figure su nombre o razón social. La copia sellada por el encargado del Registro servirá de justificante a los efectos de dicha presentación.

7.5.- CRE se reserva el derecho de requerir a las entidades participantes la defensa de sus ofertas. En caso de ser necesario, dichas sesiones podrán convocarse en las semanas siguientes a la fecha límite de presentación de ofertas.

CLÁUSULA 8. DOCUMENTACIÓN QUE HAN DE PRESENTAR LAS ENTIDADES OFERTANTES

La documentación se presentará en 2 sobres cerrados, designados con las letras A y B, debiendo figurar en cada sobre y caja el nombre de la entidad y la referencia de contratación: **“CIBERSEGURIDAD”**

El sobre A debe contener la documentación general para contratar con CRE, el sobre B debe contener la documentación específica relativa a la oferta que efectivamente se habrá de valorar y documentación técnica.

Estos sobres/paquete han de estar firmados por la entidad o persona que lo represente, y en su interior se incorporará una relación, en hoja independiente, en la que haga constar

los documentos aportados ordenados numéricamente. Las entidades ofertantes podrán indicar qué información de su propuesta tienen carácter confidencial, sin que, en ningún caso, pueda declarar como tal la oferta económica. CRE garantizará la confidencialidad de la información expresamente designada como tal.

SOBRE "A": DOCUMENTACIÓN IDENTIFICATIVA DE LA ENTIDAD Y ACREDITATIVA DE SU CAPACIDAD PARA CONTRATAR CON CRE:

Se debe aportar la documentación que se relaciona como DOCUMENTACIÓN GENERAL, **la siguiente documentación a incluir será imprescindible para la participación**:

1º) **Anexo 2 – Datos Identificación** debidamente cumplimentado; esto es, con identificación de esta, y datos del contacto de la entidad o empresa, que será el interlocutor para todo lo relacionado con estas condiciones, el proceso de selección y la propuesta, a saber:

- Nombre
- Teléfonos de contacto,
- Dirección de correo electrónico,
- Cargo que ocupa,
- Domicilio legal del proveedor,
- Personas de contacto alternativas.

2º) Certificación expedida por el órgano de dirección de la entidad ofertante, conforme acompaña como **Anexo 3 - Declaración Responsable**. Declaración responsable por parte del representante legal de la empresa, en la que se manifieste, entre otras cuestiones, que cumple las condiciones y los requisitos de solvencia técnica y económica establecidos en las presentes condiciones, así como expresiva de no encontrarse incursa en situación de incompatibilidad. Esta declaración responsable habrá de ser firmada por la entidad ofertante según el modelo.

CRE manifiesta que tiene entre sus propósitos facilitar la integración e inserción en el mundo laboral de personas con discapacidad y otros colectivos vulnerables. Así, para apoyar que el personal contratado por terceros colaboradores pertenezca a colectivos vulnerables, en todo o en parte, se tendrá en cuenta la contratación de este personal cuando así se haga constar expresamente por las entidades ofertantes. A tal efecto al menos, deberá señalar el porcentaje de personas empleadas de que se dispone en plantilla con discapacidad; o bien susceptible de incluirse en condición de carácter vulnerable.

Las empresas no españolas presentarán declaración expedida por su órgano de dirección de someterse a la Jurisdicción de los Juzgados y Tribunales españoles de cualquier orden, para todas las incidencias que de modo directo o indirecto pudieran surgir del contrato, con renuncia, en su caso, al fuero jurisdiccional extranjero que pudiera corresponderles

Las empresas extranjeras no españolas de Estados miembros de la Unión Europea o signatarios del Acuerdo sobre el Espacio Económico Europeo habrán de acreditar su capacidad de obrar mediante presentación de certificación o declaración jurada.

SOBRE "B": DOCUMENTACIÓN TÉCNICA Y ECONÓMICA:

Se presentará la oferta económica **Anexo 4** - Proposición económica y criterios automáticos junto con una Oferta Técnica explicativa de la proposición presentada, de acuerdo con los requisitos que se indican en cada uno de los puntos de estas Condiciones y que contendrá al menos, la siguiente información:

Aspectos Generales

A la hora de preparar la Oferta técnica, las entidades solicitantes deberán tener en cuenta

lo siguiente:

La estructura y contenido de la Oferta técnica en general y de la Memoria Técnica en particular debe ajustarse estrictamente a lo establecido en este apartado. Toda información que no se encuentre dentro de dicha estructura no se tendrá en cuenta.

Sobre la Memoria Técnica:

- En el caso de establecerse limitaciones de extensión de la Memoria Técnica, el contenido de las páginas que excedan dicha extensión no se tendrá en cuenta a la hora de la valoración de los criterios sujetos a un juicio de valor y, en consecuencia, los 'Aspectos a valorar' afectados se puntuarán con 0 puntos.
- La mesa de contratación podrá exigir a las entidades solicitantes documentación justificativa que acredite cualquier aspecto incluido en la Oferta técnica, así como precisiones o aclaraciones sobre las ofertas presentadas o información complementaria relativa a ellas, si bien las respuestas no podrán suponer una modificación de los elementos fundamentales de la oferta.

Contenido de la Oferta Técnica

La oferta técnica estará formada por un único documento y constará obligatoriamente de los siguientes apartados:

1. **Portada** en la que se identifique claramente la Convocatoria para la selección de contratista.
2. **Índice** de la oferta técnica.
3. Acatamiento de las presentes condiciones e identificación de la entidad ofertante, en una página con la siguiente información:
   - Párrafo en el que la entidad ofertante exprese el **acatamiento** de la totalidad de lo establecido en las condiciones y en el que se declare la veracidad de la información incluida en la oferta técnica.
   - Cuadro en el que se incluyan los **datos de la entidad ofertante** y los de la persona de contacto
4. **Resumen Ejecutivo** dónde se explique de forma concisa y sencilla la solución propuesta y los aspectos relevantes a destacar de la oferta. El Resumen Ejecutivo no será objeto de valoración (no se puntuará), si bien ayudará a la comprensión global de la oferta.
5. **Memoria Técnica**, que contiene de forma ordenada todos los criterios cuya valoración está sujeta a un juicio de valor.

Memoria Técnica

La Memoria Técnica deberá ajustarse obligatoriamente a la siguiente estructura y contenido:

#	Aspecto	Descripción
1	**Adecuación a los Requisitos de los Servicios**	Grado de cumplimiento y detalle técnico de los servicios solicitados (SOC, SIEM, EDR, ASM, etc.)
2	**Fases del Servicio**	Claridad, planificación y realismo en la ejecución por fases.
3	**Modelo de Servicio, Metodología y Gestión de la Calidad**	Claridad del modelo de prestación, metodología de trabajo, y mecanismos de control de calidad.
4	**Modelo de Gobierno del Servicio**	Propuesta de gobernanza, seguimiento, escalado y control.
5	**Homogeneidad Tecnológica**	Coherencia e integración entre las soluciones propuestas.
6	**Referencias y Casos de Éxito**	Experiencia demostrada en servicios/proyectos similares y clientes relevantes.

Limitaciones de Extensión de la Oferta técnica

Se establecen las siguientes limitaciones en la extensión de la Oferta técnica:

- Resumen Ejecutivo (punto 4 de la Oferta técnica): 4 páginas
- Memoria Técnica (punto 5 de la Oferta técnica): 100 páginas

En ambos casos las páginas se ajustarán a las siguientes características:

- Tamaño hoja: A4
- Tipo letra: Arial o tipo con tamaño de letra equivalente
- Tamaño letra mínima: 11 ppp. (puntos por pulgada)
- Márgenes mínimos: 2 cm a cada borde
- Interlineado mínimo: sencillo

Cada entidad solicitante no podrá presentar más que una sola proposición económica.

CLÁUSULA 9. PROCEDIMIENTO DE SELECCIÓN DEL CONTRATISTA

El contrato se adjudicará a la oferta que resulte más ventajosa a juicio de CRE de entre todas las presentadas en el plazo habilitado para ello.

CLÁUSULA 10. ADJUDICACIÓN DEL CONTRATO

10.1.- Valoradas las ofertas, CRE seleccionará a la entidad cuya oferta resulte más ventajosa para los intereses de la Institución, notificando su decisión a dicha entidad, que deberá aceptarla a la mayor brevedad y, en todo caso, antes del transcurso de los cinco (5) días naturales siguientes a la comunicación. De no verificarse en dicho plazo, se procederá a efectuar la selección a la siguiente entidad cuya oferta se considere más ventajosa para los intereses de CRE, siempre que cumpla los requisitos y se ajuste a lo solicitado.

10.2.- Cruz Roja Española tendrá la facultad de decidir no seleccionar a ninguna entidad, sin que haya lugar a responsabilidad alguna en tal caso para con las postuladas o terceros si no estuviera conforme con ninguna de las ofertas presentadas, lo que no generará derecho alguno para las entidades ofertantes.

10.3.- Cruz Roja Española se reserva la facultad de requerir a aquellas entidades que resulten seleccionadas cualquier documentación adicional a efectos de comprobación y verificación del cumplimiento por la destinataria de cuantos requisitos, obligaciones o aptitudes sean exigibles conforme a la naturaleza del contrato o bien conforme a la política de contratación y compromisos anticorrupción y para la prevención de blanqueo de capitales de CRE.

CLÁUSULA 11. DOCUMENTACIÓN A PRESENTAR POR LA EMPRESA SELECCIONADA PARA PRESTAR EL SERVICIO

La entidad que hubiera sido propuesta como seleccionada, tendrá que aceptar la prestación del servicio en el plazo máximo de cinco (5) días a contar desde el momento en que sea formalmente notificada la selección.

Una vez aceptada, la entidad seleccionada queda obligada a registrarse como proveedor de Cruz Roja Española en portal habilitado al efecto, https://proveedores.cruzroja.es, comprometiéndose a aportar, al menos, la siguiente documentación en idéntico plazo:

Documentación acreditativa de la personalidad y capacidad de contratar:

A. Para las personas físicas (empresarios individuales y profesionales), será obligatoria la presentación del documento nacional de identidad (DNI), o documento que lo sustituya, y del número de identificación fiscal (NIF), en caso de que este no conste en el referido DNI.

B. Para las personas jurídicas, será obligatoria la presentación del NIF y de la escritura de constitución o modificación, donde conste expresión de su objeto social; en su caso, debidamente inscrita en el Registro Mercantil, y/o inscripción en otros registros de sociedades profesionales que corresponda, cuando este requisito sea exigible conforme a la legislación que le sea aplicable. Cuando esta inscripción no sea exigida, la acreditación se realizará mediante la aportación de la escritura o documento de constitución, de modificación, estatutos o acta fundacional, en que consten las normas reguladoras de la actividad de la empresa, inscritos, en su caso, en el Registro oficial correspondiente.

C. Si la entidad actúa mediante representante o se trata de una persona jurídica, ha de aportar:

   a. Documento público de apoderamiento, debidamente inscrito en el Registro público correspondiente y acreditando la vigencia del mismo, si fuera el caso, mediante nota del registro mercantil.

   b. DNI y NIF del representante y del firmante de la proposición económica.

D. La capacidad de obrar de las empresas no españolas de Estados miembros de la Comunidad Europea, o signatarios del acuerdo sobre el Espacio Económico Europeo, se tiene que acreditar mediante la inscripción en los registros procedentes de acuerdo con la legislación del Estado donde están establecidos, o mediante la presentación de una declaración jurada, o de una certificación en los términos que se establezcan reglamentariamente, de acuerdo con las disposiciones comunitarias de aplicación.

E. La capacidad de obrar de las empresas extranjeras no comprendidas en el apartado anterior se tiene que acreditar mediante informe de la Misión Diplomática Permanente de España en el estado correspondiente o de la Oficina Consular en el ámbito territorial de la cual, radique el domicilio de la empresa.

F. En estos supuestos, tanto de personas físicas como jurídicas, cada uno de sus componentes acreditará su capacidad, personalidad, representación y solvencia, siendo obligatorio indicar en documento separado los nombres y circunstancias de quienes la subscriben, el porcentaje de participación de cada uno de ellos, y tendrán

que nombrar un representante o apoderado, con facultades suficientes para ejercitar los derechos y cumplir con las obligaciones que se deriven del Contrato hasta su extinción.

G. Copia de la Memoria, Balance, Cuenta de Resultados e informe de los auditores, cuando pudiese ser preceptivo, del último ejercicio.

H. Certificados Negativos de Deuda con la AEAT y con la Seguridad Social y restantes administraciones que competa en su caso.

I. Certificado De Prevención De Riesgos Laborales: declaración de cumplimiento de la Ley de Prevención de Riesgos Laborales emitida por la empresa o por terceros según competa.

J. Cualquier otra documentación adicional o servicios de valor añadido que proponga la entidad como complementarios o relevantes respecto de lo solicitado. Entre otros se tendrá en cuenta positivamente la ostentación de:

   Plan de igualdad. Plan de sostenibilidad, Plan medioambiental. En su caso, indicar motivo, y facilitar información sobre iniciativas respetuosas en dichas materias llevadas a cabo, o comprometidas por la entidad ofertante.

K. Responsabilidad Social Corporativa. Información sobre iniciativas comprometidas, en su caso, por la entidad seleccionada.

CLÁUSULA 12. FORMALIZACIÓN DEL CONTRATO

Aportada la documentación requerida de conformidad con la cláusula precedente, se procederá a formalizar el correspondiente contrato, dentro del plazo de los treinta (30) días siguientes a la fecha de notificación de la selección de la entidad. La fecha tope para esta firma es el 2 de enero de 2026

Si la entidad seleccionada no compareciese a la formalización se podrán declarar nulas todas las actuaciones y disposiciones relacionadas con él, así como dejar sin efecto la selección realizada por CRE para la prestación de los servicios.

CLÁUSULA 13. CUMPLIMIENTO CON LAS OBLIGACIONES LABORALES Y DE PREVENCIÓN DE RIESGOS LABORALES E INEXISTENCIA DE RELACIÓN LABORAL

13.1.- La entidad seleccionada y, en su momento, la contratista será responsable en todo momento del estricto cumplimiento de todas las obligaciones tanto laborales como de la Seguridad Social, Prevención de Riesgos Laborales y de cualquier otra naturaleza en relación con su personal. La entidad seleccionada a la firma del contrato declara que cumplirá con estas obligaciones. El contratista se obliga a estar al corriente del pago de salarios y cotizaciones a la Seguridad Social de su personal afecto a este contrato, reservándose Cruz Roja Española la facultad de requerir cuanta documentación sea acreditativa de este extremo incluso una vez finalizado el contrato.

13.2.- El contratista se compromete a ejercer de modo real, efectivo y continuado el poder de dirección inherente a la misma en su condición de empleador en relación con su plantilla, asumiendo en exclusiva, respecto del personal asignado a la ejecución del contrato, todo lo relacionado con la negociación y pago de retribuciones salariales, afiliaciones y cotizaciones a la seguridad social y pago de prestaciones, permisos, licencias, vacaciones, sustituciones, prevención de riesgos laborales, régimen disciplinario, relaciones sindicales y todos los demás derechos y obligaciones que se deriven de los contratos de trabajos propios.

13.3.- La relación entre las partes tiene carácter exclusivamente mercantil, sin que exista vínculo laboral entre Cruz Roja Española y el personal del Proveedor, aunque tuviese que

realizar tareas en las instalaciones de Cruz Roja. Por lo tanto, amparado en la existencia de la presente Convocatoria y, en su caso, del Contrato que se suscriba, o de su cumplimiento, el personal de la entidad seleccionada no podrá ser considerado, ni de hecho ni de derecho, empleado de Cruz Roja, dado que dependerá únicamente de la dirección de la mencionada empresa a todos los efectos, incluidos, por lo tanto, los aspectos laborales y de Seguridad Social.

Será el contratista quien asuma la dirección y organización de los trabajos, imparta, en su caso, órdenes e instrucciones de trabajo a sus trabajadores, y asuma las obligaciones retributivas y de cotización propias del empresario, no habiendo lugar a responsabilidad alguna para CRE por incumplimientos del adjudicatario por este capítulo.

CLÁUSULA 14. CESIÓN Y SUBCONTRATACIÓN

El contrato derivado de la presente convocatoria no podrá ser cedido a terceros. Las operaciones que la entidad seleccionada subcontrate con sus proveedores externos serán de su exclusiva responsabilidad.

No se permitirá la subcontratación de recursos, ya sea total o parcial, para la ejecución del servicio objeto de este contrato, salvo autorización escrita y explícita previa de Cruz Roja Española.

CLÁUSULA 15. DURACIÓN DEL CONTRATO

15.1.- El contrato tendrá una vigencia inicial de **tres (3) años, con posibilidad de extensión de un (1) año adicional**, siempre que ambas partes estén de acuerdo. Una vez finalizado este periodo, se podrán solicitar prórrogas mensuales, con un máximo de doce (12) meses adicionales, si ambas partes acuerdan la extensión.

15.2.- Los precios serán aplicables durante los tres años de contrato y, en el caso de prórroga, salvo mejora propuesta por la empresa seleccionada, el precio podrá ser revisado de forma anual en función de las variaciones que experimente el último índice anual de precios al consumo publicado, limitándose a un máximo del 2% de incremento.

CLÁUSULA 16. FACTURACIÓN

El contrato establecerá un monto total por los servicios, el cual se facturará mensualmente en partes iguales. Este monto podrá ser objeto de descuentos en caso de que el proveedor incurra en incumplimientos conforme a las penalizaciones definidas en el Acuerdo de Niveles de Servicio (SLA).

CLÁUSULA 17. PENALIZACIONES POR INCUMPLIMIENTO

El contrato que finalmente se suscriba, determinará las indemnizaciones y/o penalizaciones por incumplimiento.

CLÁUSULA 18. RESOLUCIÓN DEL CONTRATO

18.1.- Podrán motivar la resolución del contrato:

El incumplimiento grave y reiterado del objeto contractual o de los plazos especificados para el suministro.

La manifiesta falta de calidad del suministro/servicio.

La vulneración por parte del proveedor de los derechos de propiedad intelectual o los deberes de confidencialidad establecidos en las presentes Condiciones.

La realización de actos de imitación que comporten aprovechamiento indebido de reputación del esfuerzo ajeno, en beneficio propio o de terceros ajenos al contrato.

CRE se reservará el derecho de anular en cualquier momento el contrato que la vincule con un proveedor en caso de que las actividades de este no respeten los criterios éticos establecidos por Cruz Roja Española o comprometan de alguna forma el respeto y el prestigio debidos a su nombre y emblema.

18.2.- La resolución del contrato por causas imputables al proveedor determinará el valor de los daños y perjuicios que en concepto de indemnización ocasione el incumplimiento a Cruz Roja Española, sin perjuicio de quedar expedita la vía judicial correspondiente en caso de no cubrirse tales responsabilidades.

CLÁUSULA 19. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

19.1. - El contratista estará obligado a respetar el carácter confidencial de toda aquella información a la que tenga acceso para la ejecución del contrato; aquella que así se indique en el mismo, o que así le indique Cruz Roja, o que por su propia naturaleza tenga que ser tratada como tal. Tal compromiso se establece con carácter indefinido, persistiendo así dicha obligación, incluso después de cesar toda relación entre CRE y la entidad seleccionada, de conformidad con la Ley 1/2019, de 20 de febrero, de Secretos Empresariales.

19.2. - El contratista se someterá a la normativa vigente en materia de protección de datos, y en concreto, al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales en adelante, LOPD-GDD).

19.3. - A este respecto, el contratista deberá dar cumplimiento a las siguientes obligaciones:

1. Cumplimiento del principio de *Protección de datos desde el diseño y por defecto* en los desarrollos, conforme a lo establecido en el artículo 25 del RGPD.
2. Realización previa de una Evaluación de Impacto relativa a la protección de datos en los términos recogidos en el artículo 35 del RGPD, presentado el correspondiente informe a CRE.
3. Colaboración con CRE para la elaboración de la Evaluación de Impacto definitiva sobre el proyecto (*si fuese necesario*).

19.4. - Asimismo, toda vez que la presente contratación incluye servicios que conllevan el acceso a datos de carácter personal de responsabilidad de CRE por parte de la entidad seleccionada, ésta deberá ofrecer garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme a la normativa vigente en la materia y garantice la protección de los derechos de los interesados, en particular, deberá acreditar estar en posesión de un certificado en materia de seguridad de la información (ISO 27001, ENS) o de un certificado emitido por tercero auditor que acredite el cumplimiento de la normativa vigente en materia de protección de datos.

19.5. Posteriormente, una vez seleccionada la entidad para la ejecución del contrato, dicha entidad deberá suscribir un contrato de Encargado de Tratamiento, en los términos establecidos en el artículo 28 del RGPD.

CLÁUSULA 20. LEGISLACIÓN Y JURISDICCIÓN COMPETENTE.

El contrato que se formalice derivado de la presente convocatoria tendrá, a todos los efectos, naturaleza y carácter privado, sujeto íntegramente a la legislación civil. Se regirá por

lo establecido en sus propios términos y en los documentos anexos que lo integran que revestirán asimismo idéntico carácter obligacional, y subsidiariamente por lo dispuesto en las presentes Condiciones, junto con los anexos que lo conforman que fuesen de aplicación, y en defecto de prescripción en los anteriores, por el Código Civil y demás legislación civil aplicable.

El desconocimiento de los términos del contrato que pudiera suscribirse, de las instrucciones que se dicten en su ejecución, de las presentes Condiciones o de la regulación que sea aplicable, no eximirá a la entidad seleccionada de la obligación de su cumplimiento.

Para resolver cualquier controversia o litigio derivado de la interpretación o efectos, cumplimiento y extinción de la presente convocatoria, las dos partes se someterán a la jurisdicción civil y competencia de los Juzgados y Tribunales de la ciudad de Madrid, con expresa renuncia a cualquiera otro fuero que les pueda corresponder.

45581260K ASUNCION MONTERO (R: Q2866001G)

Firmado digitalmente por 45581260K ASUNCION MONTERO (R: Q2866001G)
Fecha: 2025.09.24 13:52:42 +02'00'

ANEXO 1. - CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE CIBERSEGURIDAD

CRUZ ROJA ESPAÑOLA

Anexo 1 - CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE CIBERSEGURIDAD.

1. OBJETO DE LA CONTRATACION

Cruz Roja Española (en adelante, “CRUZ ROJA”, "CRE" o la “Institución”) ha iniciado el presente procedimiento de contratación con el objetivo de adjudicar una parte significativa de sus servicios especializados en ciberseguridad, orientados a reforzar la protección de sus sistemas de información y comunicaciones.

Los servicios deberán ser prestado por personal debidamente cualificado, mediante el uso de herramientas adecuadas y conforme a los requisitos técnicos, operativos y de calidad establecidos en el presente pliego.

Este documento, junto al anexo 5 titulado “*Información Técnica de Referencia para la Contratación de Servicios de Ciberseguridad”,* describen los requisitos técnicos mínimos que deben cumplir los servicios a contratar.

A partir de esta información, y de los objetivos establecidos, las empresas interesadas deberán presentar sus propuestas técnicas y económicas más adecuadas.

2. ALCANCE DE LOS SERVICIOS

El presente pliego define el conjunto de servicios que conforman el alcance técnico de la contratación, todos ellos orientados a fortalecer la postura de ciberseguridad de CRE. Con estos servicios se espera cubrir distintas capas de protección, detección, análisis y respuesta ante amenazas que puedan comprometer la seguridad de los sistemas de información y comunicaciones de la organización.

La prestación de los servicios deberá realizarse de forma integrada, coordinada y continua, garantizando su operatividad, calidad y alineación con los requisitos establecidos en este documento.

El alcance incluye el total de las tareas necesarias para la puesta en marcha, gestión y mantenimiento de los elementos que permitan la prestación completa de los servicios.

Cualquier elemento o acción no especificada en este documento, pero que sea imprescindible para que el servicio funcione correctamente, deberá ser incorporado en la propuesta técnica y económica.

Las soluciones a implementar deberán no solo cubrir las necesidades actuales, sino también prever capacidad de crecimiento para atender futuras demandas, garantizando los niveles de disponibilidad requeridos.

Las empresas participantes podrán presentar alternativas técnicas o propuestas de valor añadido que consideren oportunas, siempre que estén debidamente detalladas, justificadas y valoradas, y que representen mejoras técnicas respecto a las condiciones generales del presente pliego.

A continuación, se enumeran los servicios incluidos en el alcance técnico de la contratación:

i. **Centro de Operaciones de Seguridad (Ciber SOC):** CRE tiene como propósito transformar su actual SOC en un modelo más avanzado, eficiente y alineado con las mejores prácticas del sector. Este nuevo enfoque contempla la implantación de un servicio centralizado de monitoreo y defensa digital, cuyo componente principal será un SIEM de última generación. Este sistema estará respaldado por un conjunto de

tecnologías especializadas, incluyendo soluciones de correo electrónico seguro, gestión de vulnerabilidades, protección de endpoints (EDR), seguridad en entornos cloud y capacidades de ciber inteligencia.

Además, se busca incorporar un valor diferencial mediante una gestión experta, la definición de procesos de seguridad sólidos, capacidades de análisis avanzado y una respuesta eficaz ante incidentes. Todo ello con el objetivo de fortalecer significativamente la capacidad de detección, reacción y recuperación frente a cualquier tipo de amenaza o ataque.

ii. **Sistema de Gestion de Eventos e Información de Seguridad de nueva generación (SIEM)**: la iniciativa parte de la necesidad de reemplazar la solución de SIEM actualmente en operación, mediante la adopción de una nueva plataforma completamente basada en el modelo SaaS (Software as a Service).

Esta nueva solución deberá integrar todos sus módulos en una única herramienta con consola de gestión centralizada, garantizando la interoperabilidad entre componentes.

Asimismo, deberá contar con capacidades para integrar múltiples fuentes de logs, realizar análisis de tráfico de red (NTA), aplicar técnicas de análisis de comportamiento de usuarios y entidades (UEBA), y ejecutar procesos de automatización y respuesta mediante tecnologías SOAR.

La empresa adjudicataria será responsable de la instalación, configuración inicial, integración y puesta en marcha de esta solución de SIEM de nueva generación.

iii. **Análisis de vulnerabilidades**: para este servicio se contemplan dos soluciones complementarias, ambas de inclusión obligatoria en la propuesta.

La primera consiste en una solución basada en agente y plataforma EDR, que proporcione capacidades avanzadas de detección, priorización, remediación y monitorización de vulnerabilidades.

La segunda se fundamenta en una solución de escaneo bajo demanda, que permita realizar análisis específicos de seguridad de forma flexible y adaptada a las necesidades operativas.

CRE aceptará soluciones reconocidas en el mercado que cumplan con los requisitos funcionales establecidos en este pliego. Adicionalmente, la empresa adjudicataria será responsable de proporcionar los servicios asociados a la solución propuesta, incluyendo su instalación, despliegue, configuración inicial, formación técnica y operativa, entrega de informes, entre otros.

iv. ***Endpoint Detection and Response* (EDR):** CRE cuenta actualmente con una solución EDR desplegada. En este contexto, se plantea la renovación de dicha solución o, en su defecto, su sustitución por una alternativa equivalente que cumpla con los requisitos técnicos establecidos.

La solución propuesta deberá cumplir, como mínimo, con las funcionalidades establecidas por CRE para plataformas EDR, garantizando así su adecuación técnica y operativa a los requisitos del servicio.

En caso de que la solución ofertada no corresponda al fabricante actualmente en uso por CRE, la empresa adjudicataria será responsable de ejecutar todas las actividades necesarias para una sustitución completa y eficaz. Esto incluye la planificación, instalación, configuración, migración progresiva de agentes, integración con los sistemas actuales y validación final de la solución. Todo el proceso deberá garantizar la continuidad operativa y minimizar cualquier impacto sobre los usuarios finales.

v. **Mantenimiento de hardware (firewalls y balanceadores de carga):** incluye la contratación de los servicios de mantenimiento de hardware para los equipos de firewall y balanceadores de carga ubicados en la sede central de CRE, los cuales forman parte esencial de su infraestructura de seguridad.

El servicio incluirá el mantenimiento oficial del hardware por parte del fabricante, siempre que esté disponible, así como el soporte experto proporcionado por el contratista.

vi. **Despliegue de *Firewalls* por segmento de red**:

- Firewalls para Front End: sustitución de los dispositivos actuales por una nueva solución que garantice mayor capacidad de protección y gestión centralizada.
- Firewalls para red de invitados: renovación de los equipos existentes con una solución que permita segmentar y controlar el tráfico de usuarios externos.
- Firewalls para entorno en la nube: incorporación de dispositivos específicos para proteger servicios alojados en la nube pública, asegurando las comunicaciones internas y externas.
- Firewalls para VPNs de acceso remoto: migración parcial de la infraestructura actual, centrada en los accesos relacionados con la gestión de sistemas y ciberseguridad, excluyendo los accesos de teletrabajo.

vii. ***Attack Surface Management* (ASM)**: incorporación de una solución de gestión de superficie de ataque (ASM) que permita identificar, monitorizar y reducir de forma continua todos los activos digitales expuestos, tanto conocidos como desconocidos, con el objetivo de minimizar el área vulnerable frente a posibles atacantes.

viii. ***Zero Trust Network Access* (ZTNA)**: incorporación de una solución de acceso a red basada en el modelo de Confianza Cero, orientada a transformar el acceso a las aplicaciones de Intranet actualmente expuestas públicamente, en accesos privados, seguros y controlados, bajo los principios de confianza cero y privilegio mínimo.

La solución deberá estar basada en un modelo SaaS, salvo en aquellos casos en los que sea necesario desplegar gateways o proxies para la conexión con entornos on-premise.

Asimismo, la solución deberá garantizar una arquitectura segura, escalable y alineada con las mejores prácticas del sector, asegurando una experiencia de usuario fluida sin comprometer la seguridad. Deberá permitir el acceso tanto con agente como sin agente.

ix. **Seguridad en la Nube**: con el objetivo de ampliar y reforzar las capacidades actuales de la organización, se propone incorporar una plataforma integral de seguridad en la nube, compatible con entornos multicloud, híbridos y DevOps. Esta solución deberá proporcionar visibilidad, detección y protección de riesgos en tiempo real.

La plataforma deberá incluir, como mínimo, funcionalidades de *Cloud Security Posture Management* (CSPM), *Cloud Workload Protection* (CWP) y *Cloud Infrastructure Entitlement Management* (CIEM), alineadas con los estándares del sector y las necesidades específicas de CRE.

En caso de que la solución ofertada no corresponda al fabricante actualmente en uso por CRE, la empresa adjudicataria será responsable de llevar a cabo todas las actividades necesarias para una sustitución completa, garantizando la continuidad operativa y la integración con la infraestructura existente.

x. ***Secure Access Service Edge* (SASE):** se contempla la adquisición e implantación de una solución SASE que permita a la organización unificar, en un servicio centralizado, las funciones de protección de red y seguridad en la nube.

La solución ofertada deberá integrar de forma nativa las siguientes capacidades: Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS) y Data Loss Prevention (DLP).

Dado que esta solución tiene carácter opcional dentro de la oferta global de servicios de ciberseguridad, las empresas interesadas deberán presentar de manera separada y

claramente diferenciada todos los costes asociados a su implantación, licenciamiento, soporte y mantenimiento, sin incluirlos en el presupuesto general de la propuesta.

xi. **Servicio de filtrado de correo electrónico*:*** se incluye la renovación de los servicios de correo limpio con el fabricante actualmente en uso por CRE. La solución deberá contemplar los siguientes módulos: Email Protection, Targeted Attack Protection, Threat Response Auto-Pull, Nexus Risk Explorer, Isolation for VAPs, PSAT Enterprise, Log API Forwarding y Email Fraud Defense**.**

xii. **Servicio de pruebas de penetración (*Pentesting*):** se contempla la contratación de un servicio de seguridad ofensiva, cuyo objetivo será evaluar el nivel de protección de los sistemas de información, redes, aplicaciones y servicios de la organización mediante la simulación controlada de ataques reales.

Esta evaluación permitirá identificar vulnerabilidades y fortalecer la postura de seguridad de forma proactiva.

El servicio se estructurará en base a un número determinado de jornadas de trabajo anuales, acordadas previamente, que serán utilizadas para la ejecución de las distintas actividades.

xiii. **Servicio de respuesta ante incidentes forenses digitales (*DFIR*):** se contempla la contratación de un servicio especializado de respuesta ante incidentes forenses digitales (DFIR), con el objetivo de fortalecer las capacidades de detección, análisis y gestión de incidentes de seguridad informática.

Este servicio estará estructurado en dos componentes diferenciados: Forense Digital (DF – Digital Forensics) y Respuesta a Incidentes (IR – Incident Response).

Su ejecución se organizará en función de un número determinado de jornadas de trabajo anuales previamente acordadas, que serán utilizadas para llevar a cabo las actividades necesarias.

xiv. **Servicio de asesoría y asistencia legal especializada en ciberseguridad:** se contempla la contratación de un servicio especializado capaz de brindar apoyo jurídico experto en la gestión de incidentes de seguridad, cumplimiento normativo y riesgos legales asociados a las tecnologías de la información.

El servicio se estructurará en base a un número determinado de jornadas de trabajo anuales, acordadas previamente, que serán utilizadas para la ejecución de las distintas actividades.

xv. **Incorporación de perfiles profesionales especializados**:

- Responsable de Seguridad de la Información (Security Manager): perfil profesional senior para asumir la coordinación y supervisión de las funciones de ciberseguridad de la Organización. Tendrá una dedicación equivalente al 0.5 FTE, mantenida de forma continua durante toda la vigencia del contrato.
- Analista de ciberseguridad para SIEM: perfil profesional senior para desempeñar funciones de analista, con especialización en el uso de plataformas SIEM de nueva generación para la gestión, correlación y análisis avanzado de eventos de seguridad. Tendrá una dedicación equivalente al 0.5 FTE, mantenida de forma continua durante toda la vigencia del contrato.

xvi. **Servicio de mantenimiento integral de soluciones de Ciberseguridad:** con el objetivo de garantizar la operatividad, disponibilidad y evolución continua de las soluciones y equipamiento de ciberseguridad, CRE requiere la contratación de un servicio de mantenimiento integral.

Este servicio deberá abarcar actividades de mantenimiento preventivo, correctivo y evolutivo, aplicables a todos los componentes contemplados en el presente pliego,

tanto de software como de hardware.

3. INFORMACIÓN TÉCNICA DETALLADA

Dado el carácter sensible de la información técnica relacionada con los servicios de ciberseguridad, esta ha sido incluida en un documento específico: el **ANEXO 5**, titulado "*Información Técnica de Referencia para la Contratación de Servicios de Ciberseguridad*".

Con el fin de proteger dicha información, se establece que las empresas interesadas deberán firmar previamente un **Acuerdo de Confidencialidad** (NDA – Non-Disclosure Agreement) para poder acceder al contenido del anexo.

La solicitud del NDA deberá realizarse mediante correo electrónico a la siguiente dirección: sistemas.informacion@cruzroja.es.

Una vez recibido el acuerdo debidamente firmado, se procederá al envío del ANEXO 5 a la dirección de contacto proporcionada por la empresa solicitante.

4. FASES DEL CONTRATO

Aunque la planificación definitiva de las actividades objeto del contrato se determinará a partir de la reunión de lanzamiento y se irá ajustando paulatinamente durante su ejecución, inicialmente se prevé el siguiente desarrollo por fases:

- Fase I. Transición del Servicio (máximo de 4 meses de duración)
- Fase II. Estabilización del Servicio (máximo de 1 mes de duración)
- Fase III. Operación regular del Servicio
- Fase IV. Devolución o Cierre del Servicio (al menos 1 mes de duración).

Fase I. Transición del Servicio

El objetivo de esta fase, con una duración máxima de cuatro (4) meses, es que el adjudicatario ponga en marcha todos los servicios objeto del contrato en las condiciones definidas en el presente pliego. Durante este periodo:

- No se aplicarán penalizaciones por los Acuerdos de Nivel de Servicio (ANS).
- No se facturarán servicios ni se generarán costes para CRE (CRE).
- El adjudicatario será responsable de organizar y ejecutar la transición, asumiendo los aspectos técnicos y operativos necesarios para garantizar una incorporación efectiva, sin que ello implique costes adicionales para CRE.

Las empresas interesadas deberán presentar en su Memoria Técnica un Plan de Transición del Servicio, detallando el tiempo estimado y la solución técnica para la migración, sin que ello suponga ningún coste adicional para CRE.

El adjudicatario se deberá comprometer expresamente a que, hasta la total implantación y puesta en servicio de las soluciones que él haya ofertado, no exista en ningún momento para CRE pérdida de servicio en las condiciones en las que se venían prestando en el contrato anterior. En cualquier caso, será de responsabilidad del adjudicatario llegar a los acuerdos que sean necesarios que aseguren a CRE la continuidad del servicio, el nivel de calidad de este y una transición transparente.

Todos los gastos necesarios para la puesta en marcha del proyecto objeto de este pliego con plena operatividad, incluyendo los costes de equipamiento, los cambios de titularidad, los traslados y cualquier otro coste derivado de la implantación de los servicios solicitados,

serán por cuenta del adjudicatario.

La fase de transición se considerará cerrada cuando así se constate en la firma del Acta de puesta en marcha por parte del adjudicatario y de CRE, siendo a partir de ese momento cuando el adjudicatario empezará a facturar a CRE los servicios prestados.

Fase II. Estabilización del Servicio

La Fase de Estabilización, con una duración máxima de un (1) mes, comienza inmediatamente después de la transición y tiene como objetivo consolidar la operativa del servicio, asegurando que se cumplan los niveles de calidad, disponibilidad y rendimiento establecidos.

En esta etapa, el adjudicatario deberá definir y acordar con CRE el alcance final del servicio, el modelo de prestación con sus actividades, condiciones y responsabilidades, así como un Plan de Calidad que contemple medidas preventivas y de control, sujeto a aprobación por la Institución.

El servicio deberá ejecutarse conforme a lo acordado, incorporando los ajustes necesarios derivados del proceso de estabilización. En esta etapa no se aplicarán penalizaciones por incumplimiento de los ANS, pero su seguimiento será obligatorio y formará parte del proceso de validación del servicio. En este sentido, el proveedor adjudicatario deberá proporcionar a CRE los valores de los indicadores y niveles de servicio (ANS) definidos en este pliego. Estos datos tendrán carácter informativo y permitirán evaluar el comportamiento del servicio, identificar posibles desviaciones y ajustar los procesos antes del inicio de la fase de prestación plena.

Una vez completadas las actividades previstas en esta fase y verificado el correcto funcionamiento del servicio conforme a los niveles de calidad acordados, se realizará una revisión conjunta entre el adjudicatario y CRE. Esta revisión servirá para validar los resultados obtenidos, documentar posibles incidencias pendientes y, en su caso, aprobar el cierre formal de la Fase de Estabilización.

En caso de que la transición de alguno de los servicios no pudiera completarse dentro del plazo establecido, CRE se reserva el derecho de rescindir total o parcialmente el contrato afectado, sin que ello genere derecho a indemnización para el adjudicatario ni coste adicional alguno para la Institución.

La superación de esta fase será condición necesaria para considerar el servicio plenamente operativo.

Fase III. Operación regular del Servicio

El objetivo principal de esta fase es asegurar la prestación continua de los servicios conforme a lo establecido en el pliego y a lo acordado durante las fases de Transición y de Estabilización.

A partir de este momento, el proveedor se compromete a cumplir con los niveles de servicio definidos en los Acuerdos de Nivel de Servicio (ANS), siendo plenamente aplicables las penalizaciones en caso de incumplimiento.

Durante esta etapa se desarrollarán los procesos y actividades necesarios para la correcta ejecución del servicio, incorporando acciones orientadas a la mejora continua. Además, se generará de forma periódica la documentación e informes que reflejen las tareas realizadas, garantizando la trazabilidad y transparencia del trabajo.

Operación y Continuidad de los Servicios: las entidades participantes deberán incluir en

su Memoria Técnica la Metodología de Operación propuesta para la ejecución de todos los servicios objeto de la contratación, con un nivel de detalle adecuado que permita evaluar la capacidad operativa y organizativa de cada propuesta.

Asimismo, deberán contemplarse jornadas periódicas de transferencia de conocimiento, al menos de carácter semestral, orientadas a la gestión y explotación de las tecnologías involucradas. Estas sesiones estarán dirigidas al personal de CRE, con el objetivo de asegurar la apropiación técnica y operativa de los servicios por parte de la entidad contratante. Cabe destacar que todos los datos generados en el marco de la explotación de los servicios serán propiedad de CRE.

Adicionalmente, las empresas deberán describir las medidas específicas que aplicarán para garantizar la operatividad del servicio durante la Fase de Operación, incluyendo protocolos de actuación ante incidencias que puedan provocar interrupciones. Estas medidas deberán asegurar la continuidad del servicio, minimizando el impacto en los usuarios y manteniendo los niveles de calidad comprometido.

Fase IV. Cierre o Devolución del Servicio

El adjudicatario deberá incluir en su Memoria Técnica un Plan Devolución del Servicio a alto nivel, con una duración mínima de cuatro semanas, que se ejecutará en paralelo al tramo final de la Fase de Ejecución.

Este plan deberá buscar asegurar una transferencia ordenada de la documentación y del conocimiento acumulado a CRE, o a la entidad que esta designe. Aunque su contenido será general en esta fase, el adjudicatario deberá comprometerse a estar plenamente disponible y a colaborar activamente en su ejecución cuando corresponda, asegurando así una transición fluida y sin interrupciones.

Esta fase también incluirá el cierre administrativo de los trabajos, abarcando la finalización y aceptación formal de los servicios prestados, así como la resolución de cualquier pendiente relacionado con el cumplimiento del contrato.

Durante el periodo de devolución del servicio, el adjudicatario deberá cumplir con los Acuerdos de Nivel de Servicio pactados anteriormente. El periodo de devolución no podrá ser en ningún caso causa de ninguna discontinuidad o pérdida de prestaciones o calidad del servicio ofrecido a los usuarios finales.

La devolución del servicio no se considerará finalizada hasta la firma por parte de CRE del Acta de aceptación de la devolución del servicio, condición necesaria para el pago de la última factura.

Acuerdo de prestación provisional ante retrasos en la implantación del nuevo servicio: en caso de que se retrasara la puesta en marcha del servicio por parte del nuevo contratista, por motivos de interés público y con el fin de garantizar la continuidad del servicio, el adjudicatario de este contrato se compromete a continuar dando el servicio hasta la total implantación del siguiente contrato manteniendo los precios de esta oferta y estableciendo, en su caso, los acuerdos necesarios con el siguiente prestatario, asegurando la transición de forma transparente en términos de calidad y continuidad.

5. MODELO DE GOBIERNO DEL SERVICIO

Las empresas interesadas deberán presentar una propuesta detallada sobre el modelo de gobierno que aplicarán para la gestión de los servicios. Este modelo debe incluir los mecanismos formales de control, supervisión y toma de decisiones que aseguren la

correcta prestación de los servicios, su alineación con los objetivos del negocio y su evolución continua.

En particular, se solicita la descripción de la estructura de gobernanza propuesta, incluyendo la conformación y frecuencia de los comités ejecutivos, orientados a la toma de decisiones estratégicas, revisión de resultados globales y definición de acciones de mejora. Asimismo, deberá contemplarse la creación de comités operativos o de seguimiento, que funcionen como espacios periódicos para el análisis de indicadores, revisión de incidentes críticos, evaluación del cumplimiento de los Acuerdos de Nivel de Servicio (ANS) y gestión de problemas recurrentes.

La propuesta deberá especificar los actores involucrados en cada instancia (representantes del proveedor, del cliente, responsables técnicos y funcionales), el tipo de documentación generada (actas, reportes, tableros de control), y el procedimiento para la gestión de los planes de acción derivados de dichas reuniones.

Adicionalmente, se valorará la inclusión de mecanismos de escalamiento formal, tanto técnicos como jerárquicos, que permitan resolver de forma ágil y estructurada situaciones complejas o de alto impacto. La empresa deberá demostrar su capacidad para sostener un modelo de relación basado en la transparencia, colaboración y mejora continua, con foco en la experiencia del usuario y en la evolución del servicio a lo largo del tiempo.

6. PERSONAL ORGANIZATIVO DEL SERVICIO

Las empresas interesadas deberán presentar sus propuestas detalladas sobre la estructura organizativa y técnica que se aplicará para la gestión de los servicios, incluyendo los perfiles profesionales asignados, sus responsabilidades y su dedicación al proyecto. Esta estructura deberá estar alineada con los objetivos del servicio, garantizar una interlocución eficaz y facilitar la coordinación operativa y estratégica con CRE.

A modo de referencia, se espera que la propuesta contemple, al menos, la asignación de los siguientes perfiles clave:

- Interlocutor Único: punto de contacto centralizado entre la empresa adjudicataria y CRE, responsable de coordinar todas las actividades del contrato y asegurar la trazabilidad de las comunicaciones. Responsabilidad compartida con la figura descrita anteriormente en el apartado de Security Manager.
- Jefe de Proyecto: encargado de liderar la implantación del acuerdo durante la vigencia de contrato, gestionando los hitos técnicos, la planificación y la coordinación de los equipos involucrados. Responsabilidad compartida con la figura descrita anteriormente en el apartado de Security Manager.
- Jefe de Servicio: responsable del mantenimiento y operación de todos los elementos instalados, garantizando su disponibilidad, rendimiento y evolución conforme a los niveles de servicio establecidos. Descrito anteriormente en el apartado de Security Manager
- Responsable de Innovación: orientado al desarrollo técnico de las soluciones, proponiendo mejoras continuas, adaptaciones tecnológicas y evolución funcional de los servicios contratados.

Por parte de CRE, se designará un responsable del Contrato, quien supervisará la correcta ejecución del mismo y actuará como interlocutor principal frente a la empresa adjudicataria.

La propuesta deberá incluir la descripción de los perfiles, su experiencia, certificaciones

relevantes y el grado de dedicación previsto, así como los mecanismos de sustitución y continuidad en caso de cambios en el equipo asignado.

7. GESTION DE LA CALIDAD Y MEJORA CONTINUA

Se busca que la empresa que finalmente resulta adjudicada mantenga un enfoque sistemático para la gestión de la calidad y la mejora continua de los servicios prestados. Este enfoque deberá estar alineado con los objetivos del contrato y orientado a garantizar la eficacia, eficiencia y evolución constante de las soluciones implantadas.

A modo orientativo, se espera que la propuesta presentada incluya al menos los siguientes elementos:

- Documentación: la empresa adjudicataria deberá mantener actualizada y ordenada toda la documentación relevante del servicio, incluyendo aspectos técnicos, operativos y administrativos. Esta documentación deberá estar disponible en un plazo máximo de diez días laborables desde su solicitud, salvo excepciones justificadas. Al inicio del contrato se definirá, junto con CRE, el modelo, contenido y periodicidad de los informes, que podrán ajustarse según la actividad. La puntualidad y calidad en la entrega de esta documentación será esencial para el correcto funcionamiento del servicio.
- Informes: se deberá contemplar la elaboración periódica de distintos tipos de informes que permitan el seguimiento integral del servicio. Entre ellos se incluyen:
    - Informes de actividad general. La periodicidad será diaria (informe de buenos días), semanal y mensual de seguimiento y finalmente anual
    - Informes de incidencias y eventos relevantes.
    - Informes mensuales de seguimiento de los Acuerdos de Nivel de Servicio (ANS).
    - Informes de análisis de inventario, tráfico y costes.
    - Informes de instalaciones realizadas.
    - Informes adicionales que puedan ser requeridos por el Responsable del Contrato de CRE.

Asimismo, la empresa adjudicataria deberá estar en disposición de elaborar informes extraordinarios y/o a medida, relacionados con cualquier aspecto de los servicios objeto del presente contrato, cuando así lo solicite CRE.

- Auditorías: las empresas deberán contemplar en sus propuestas la realización de auditorías internas y externas como parte del modelo de gestión de calidad, con el objetivo de evaluar el cumplimiento de los requisitos técnicos, normativos y contractuales, así como identificar oportunidades de mejora. Adicionalmente, CRE se reserva el derecho de llevar a cabo auditorías complementarias sobre el grado de cumplimiento de los parámetros de calidad ofrecidos, ya sea mediante personal propio o a través de empresas externas independientes. Para ello, el adjudicatario deberá facilitar el acceso a toda la información, documentación, sistemas y recursos necesarios, garantizando la colaboración activa y la transparencia durante el proceso de auditoría.
- Formación: las empresas interesadas deberán incluir en sus propuestas un plan de formación dirigido a los usuarios de los servicios y suministros contemplados en el presente pliego. Este plan deberá estar orientado a facilitar la comprensión, el uso adecuado y la explotación eficiente de las soluciones implantadas. Las empresas interesadas deberán detallar en sus ofertas el contenido, formato, frecuencia y destinatarios de las acciones formativas propuestas, incluyendo sesiones presenciales o virtuales, materiales de apoyo, y mecanismos de evaluación del aprendizaje. Se valorará especialmente la capacidad del plan para adaptarse a distintos perfiles de usuario y niveles de conocimiento, así como su alineación con la evolución tecnológica

de los servicios.

La empresa deberá demostrar su compromiso con un modelo de gestión basado en la transparencia, la colaboración y la mejora continua, con foco en la evolución del servicio a lo largo del tiempo. En este sentido, se valorará especialmente la inclusión de portales, cuadros de mando u otras herramientas que faciliten el seguimiento de la prestación; la propuesta de modelos de relación o informes adicionales que puedan aportar valor; y la calidad, alcance y adecuación del plan de formación presentado.

8. CUMPLIMIENTO NORMATIVO

El Esquema Nacional de Seguridad (ENS) tiene como objeto establecer la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información. El adjudicatario (o los adjudicatarios, según corresponda) estará obligado al cumplimiento y a la presentación de los certificados oficiales de la legislación vigente, especialmente:

- Real Decreto 311/2022, de 3 de mayo en **nivel alto**, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- El Real Decreto 311/2022, de 3 de mayo en **nivel alto**, por el que se asigna al Centro Criptológico Nacional el papel de coordinador público a nivel estatal de la respuesta técnica de los equipos de respuesta a incidentes, a través del CCN-CERT; el desarrollo de programas de sensibilización, concienciación y formación dirigidos al personal de las entidades del sector público y la divulgación de buenas prácticas y avisos de ciberseguridad.

En consecuencia, al cumplimiento de la ley vigente del Esquema Nacional de Seguridad (ENS), de carácter específico, se tendrá especial interés en los siguientes aspectos:

- El adjudicatario mantendrá informado al responsable de seguridad de CRE del estado de seguridad de los sistemas. Informará acerca de alteraciones en las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que puedan ser de interés. El adjudicatario deberá reaccionar con diligencia para gestionar el riesgo.
- En caso de incidentes relacionados con la seguridad de la información, el adjudicatario deberá comunicarlos inmediatamente al responsable de Seguridad de CRE, para que este pueda notificarlo a su vez al CCN, de acuerdo a lo indicado en el artículo 36 del ENS. Para la tipificación de los incidentes, el adjudicatario se adaptará a lo indicado en la guía CCN-STIC-817 Gestión de Ciberincidentes, así como las instrucciones técnicas que pudieran afectar.
- El adjudicatario deberá colaborar con el responsable de Seguridad de CRE en la carga de datos del Informe Nacional del Estado de Seguridad de los sistemas TIC (INES), teniendo en cuenta lo indicado en la guía CCN-STIC-824 Información del Estado de Seguridad.

El adjudicatario, informará a su personal, colaboradores y subcontratistas de las obligaciones establecidas en el presente contrato sobre confidencialidad, así como de las obligaciones relativas al tratamiento automatizado de datos de carácter personal. Realizará cuantas advertencias y suscribirá cuantos documentos sean necesarios con su personal y colaboradores, con el fin de asegurar el cumplimiento de tales obligaciones.

Respecto a la gestión, administración y operación de los sistemas de información y de los datos a que se tenga acceso, todo ello dentro de la realización de los trabajos objeto del

presente contrato, se deberán cumplir los requisitos de seguridad recogidos en este clausulado en todas las infraestructuras, servicios y sistemas del adjudicatario que den servicio a CRE en el desarrollo del contrato.

9. ACUERDOS DE NIVELES DE SERVICIO (ANS)

Los Acuerdos de Nivel de Servicio (ANS), definidos por CRE, establecen los estándares mínimos de calidad que deben cumplir los servicios contratados. Su objetivo es permitir una evaluación objetiva del desempeño, mediante parámetros medibles que faciliten el seguimiento tanto puntual como a lo largo del tiempo.

La empresa adjudicataria será responsable de cumplir con estos acuerdos, de medir los niveles de servicio y de presentar los informes correspondientes al Responsable del Contrato, quien podrá aplicar penalizaciones en caso de detectarse incumplimientos. Los informes deberán ser periódicos —inicialmente mensuales, salvo que CRE indique otra frecuencia— y se deberá mantener un histórico de actividad durante toda la vigencia del contrato.

CRE se reserva el derecho de auditar los ANS, directamente o a través de terceros, y la empresa adjudicataria deberá facilitar los medios necesarios para ello.

a. Consideraciones para el establecimiento de los ANS

La definición de los Acuerdos de Nivel de Servicio (ANS) se basará en una serie de conceptos operativos y técnicos que permiten establecer criterios claros para la gestión, seguimiento y evaluación de los servicios contratados. A continuación, se detallan dichos conceptos:

Conceptos de seguridad

- Amenaza de seguridad: Evento o circunstancia con potencial de comprometer la seguridad de los activos de información.
- Vulnerabilidad de seguridad: Debilidad en un sistema que puede ser explotada por una amenaza.
- Evento o alerta de seguridad: Notificación generada por sistemas de monitorización que indica una posible actividad anómala.
- Incidente de seguridad: Evento confirmado que afecta negativamente la seguridad de los sistemas o la información.

Clasificación de incidentes

- Incidente grave: Incidente clasificado con nivel de peligrosidad ALTO, MUY ALTO o CRÍTICO, según la guía CCN-STIC-817 del Esquema Nacional de Seguridad.
- Incidente normal: Incidente clasificado con nivel de peligrosidad BAJO o MEDIO, conforme a la misma guía.

Gestión de incidencias

- Incidencia: Interrupción o degradación del servicio que afecta su funcionamiento.
- Incidencia grave: Pérdida total del servicio o afectación crítica que impide su uso.
- Incidencia normal: Degradación parcial del servicio sin pérdida total de funcionalidad.

Se establecen también los siguientes **parámetros de gestión**:

- Tiempo de respuesta: Intervalo desde la detección o notificación hasta el inicio de la atención.
- Tiempo de escalado: Intervalo hasta la transferencia del caso a un nivel superior de

soporte.

- Tiempo de resolución: Intervalo hasta la solución efectiva del incidente o incidencia.
- Tiempo de cierre: Intervalo hasta la formalización del cierre del caso.
- Tiempo de entrega del informe de resolución: Intervalo hasta la entrega del informe técnico correspondiente.

Todos los tiempos se contabilizarán en régimen 24x7, en coherencia con el horario de prestación del servicio.

Para los ANS relacionados con la disponibilidad, se considerará como referencia el porcentaje de tiempo mensual en que cada plataforma esté operativa, incluyendo el acceso a consolas de gestión y su funcionalidad básica, una vez en fase de explotación.

b. Indicadores de Nivel de Servicios

Esta sección detalla los indicadores que permiten medir el cumplimiento de los ANS establecidos. Cada indicador incluye su definición, fórmula de cálculo, valor objetivo, frecuencia de medición y nivel de criticidad.

Estos indicadores son fundamentales para el seguimiento del desempeño del proveedor y la mejora continua del servicio.

Centro de Operaciones de Seguridad (Ciber SOC):

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad del servicio SOC	(Horas operativas / Horas totales del periodo) × 100	≥ 99.9%	Mensual	Alto
Tiempo de respuesta ante incidente grave	Tiempo desde la detección o notificación hasta el inicio de atención	≤ 30 minutos	Por Incidente	Alto
Tiempo de respuesta ante incidente normal	Tiempo desde la detección o notificación hasta el inicio de atención	≤ 2 horas	Por incidente	Medio
Tiempo de resolución de incidente grave	Tiempo desde la detección hasta la resolución efectiva	≤ 4 horas	Por incidente	Alto
Tiempo de resolución de incidente normal	Tiempo desde la detección hasta la resolución efectiva	≤ 24 horas	Por incidente	Medio
Tiempo de escalado	Tiempo desde la detección hasta la transferencia a nivel superior de soporte	≤ 1 hora (grave)	Por incidente	Medio
Tiempo de entrega de informe	Tiempo desde el cierre del incidente hasta la entrega del informe técnico	≤ 3 días hábiles	Por incidente	Bajo
Frecuencia de informes de actividad	Entrega de informe consolidado de actividad del SOC	1 informe mensual	Mensual	Alto
Monitorización continua	Verificación de que el servicio está activo 24x7 sin interrupciones	100% cobertura 24x7	Mensual	Medio

Sistema de Gestion de Eventos e Información de Seguridad de nueva generación (SIEM):

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad del sistema	(Horas disponibles / Horas totales) × 100	≥ 99,5%	Mensual	Alto
Tiempo medio de integración de nuevas fuentes de logs	Σ (Tiempo de integración por fuente) / N° de fuentes integradas	≤ 5 días por fte.	Mensual	Medio
Tiempo de detección de eventos críticos	Tiempo desde la generación del evento hasta su detección por el SIEM	≤ 5 minutos	Mensual	Alto
Tiempo de respuesta ante alertas generadas por el SIEM	Tiempo desde la alerta hasta la primera acción registrada	≤ 15 minutos	Mensual	Alto
Porcentaje de falsos positivos	(N° alertas falsas / N° total alertas) × 100	≤ 5%	Mensual	Medio
Porcentaje de cobertura de logs críticos	(N° fuentes críticas integradas / N° total de fuentes críticas identificadas) × 100	≥ 95%	Trimestral	Alto

Análisis de vulnerabilidades: Solución basada en el agente y plataforma de EDR

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad del sistema	(Horas disponibles / Horas totales) × 100	≥ 99,5%	Mensual	Alto
Cobertura de agentes desplegados	(N° de endpoints con agente activo / N° total de endpoints) × 100	≥ 98%	Mensual	Alto
Frecuencia de escaneo automático	N° de escaneos realizados por agente / N° de endpoints	≥ 1 escaneo diario por endpoint	Mensual	Alto
Tiempo medio de detección de vulnerabilidades críticas	Σ (Tiempo desde aparición hasta detección) / N° de vulnerabilidades críticas detectadas	≤ 24 horas	Mensual	Alto

Análisis de vulnerabilidades: Solución basada en escaneos bajo demanda

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad del motor de escaneo bajo demanda	(Horas disponibles / Horas totales) × 100	≥ 99,5%	Mensual	Alto
Tiempo de ejecución de escaneo bajo demanda	Tiempo desde solicitud hasta finalización del escaneo	≤ 4 horas	Por escaneo	Medio
Cobertura de activos escaneados	(N° de activos escaneados / N° total de activos solicitados) × 100	≥ 100%	Por escaneo	Alto
Tiempo medio de generación de informe post-escaneo	Σ (Tiempo desde fin del escaneo hasta entrega del informe) / N° de escaneos	≤ 24 horas	Mensual	Medio
Porcentaje de escaneos exitosos	(N° de escaneos completados sin error / N° total de escaneos solicitados) × 100	≥ 99%	Por escaneo	Alto

Endpoint Detection *and Response* (EDR):

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad de la plataforma EDR	(Horas disponibles / Horas totales del periodo) × 100	≥ 99,5%	Mensual	Alto
Cobertura de agentes EDR desplegados	(N° de endpoints con agente activo / N° total de endpoints) × 100	≥ 98%	Mensual	Alto
Tiempo medio de detección de amenazas críticas	Σ (Tiempo desde aparición hasta detección) / N° de amenazas críticas detectadas	≤ 5 minutos	Mensual	Alto
Tiempo medio de respuesta ante incidentes detectados por EDR	Σ (Tiempo desde alerta hasta primera acción registrada) / N° de incidentes	≤ 15 minutos	Mensual	Alto
Porcentaje de amenazas contenidas automáticamente por el EDR	(N° de amenazas contenidas automáticamente / N° total de amenazas detectadas) × 100	≥ 90%	Mensual	Medio
Porcentaje de falsos positivos	(N° de alertas falsas / N° total de alertas generadas) × 100	≤ 5%	Mensual	Medio
Tiempo de despliegue de agente en nuevos endpoints	Σ (Tiempo desde solicitud hasta instalación) / N° de endpoints nuevos	≤ 2 días	Mensual	Medio

Mantenimiento de hardware (firewalls y balanceadores de carga):

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad de los dispositivos gestionados (Firewalls y Balanceadores)	(Horas disponibles / Horas totales del periodo) × 100	≥ 99.95% mensual	Mensual	Alto
Tiempo medio de resolución de incidencias hardware	Σ (Tiempo desde apertura hasta cierre de incidencia) / N° de incidencias	≤ 4 horas	Mensual	Alto
Tiempo de respuesta ante fallo crítico	Tiempo desde detección del fallo hasta inicio de intervención	≤ 30 minutos	Mensual	Alto
Porcentaje de mantenimiento preventivo ejecutado según plan	(N° de mantenimientos realizados / N° de mantenimientos planificados) × 100	≥ 100%	Trimestral	Medio
Porcentaje de actualizaciones de firmware aplicadas en plazo	(N° de actualizaciones aplicadas / N° de actualizaciones planificadas) × 100	≥ 95%	Trimestral	Medio
Porcentaje de disponibilidad de backups de configuración	(N° de backups disponibles / N° de dispositivos gestionados) × 100	≥ 100%	Mensual	Alto

Despliegue de Firewalls por segmento de red:

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Tiempo máximo de despliegue por pareja de firewalls	Días desde inicio del despliegue hasta puesta en producción	≤ 15 días hábiles	Por despliegue	Alta
Disponibilidad de los firewalls desplegados	(Horas disponibles / Horas totales del periodo) × 100	≥ 99.95%	Mensual	Alta
Porcentaje de validación funcional post-despliegue	(N° de pruebas superadas / N° total de pruebas planificadas) × 100	100%	Por despliegue	Alta
Porcentaje de entrega de documentación técnica completa	(N° de entregas completas / N° total de despliegues) × 100	100%	Por despliegue	Media
Tiempo medio de aplicación de cambios solicitados durante el despliegue	Σ (Tiempo desde solicitud hasta aplicación) / N° de cambios	≤ 3 días hábiles	Mensual	Media

Attack Surface *Management* (ASM):

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad de la plataforma ASM	(Horas disponibles / Horas totales del periodo) × 100	≥ 99.9% mensual	Mensual	Alto
Cobertura de activos monitorizados	(N° de activos monitorizados / N° total de activos identificados) × 100	≥ 98%	Mensual	Alto
Tiempo medio de detección de exposición crítica	Σ (Tiempo desde aparición hasta detección) / N° de exposiciones críticas	≤ 1 día	Mensual	Alto
Tiempo medio de notificación de exposición	Σ (Tiempo desde detección hasta notificación al cliente) / N° de exposiciones	≤ 30 minutos	Mensual	Alto
Porcentaje de falsos positivos en exposiciones	(N° de exposiciones falsas / N° total de exposiciones reportadas) × 100	≤ 5%	Mensual	Medio

Zero Trust Network Access (ZTNA):

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad de la plataforma ZTNA	(Horas disponibles / Horas totales del periodo) × 100	≥ 99.9% mensual	Mensual	Medio
Tiempo medio de autenticación de usuarios	Σ (Tiempo desde solicitud de acceso hasta validación) / N° de accesos	≤ 5 segundos	Mensual	Medio
Porcentaje de accesos bloqueados por políticas ZTNA	(N° de accesos bloqueados / N° total de intentos de acceso) × 100	≥ 98% (cuando corresponda)	Mensual	Alto

Tiempo medio de aplicación de cambios en políticas de acceso	Σ (Tiempo desde solicitud hasta aplicación efectiva) / N° de cambios	≤ 2 horas	Mensual	Medio
Porcentaje de dispositivos evaluados antes de conceder acceso	(N° de accesos con evaluación de dispositivo / N° total de accesos) × 100	≥ 100%	Mensual	Alto
Porcentaje de accesos seguros (cumplen requisitos de contexto)	(N° de accesos que cumplen requisitos / N° total de accesos concedidos) × 100	≥ 99%	Mensual	Alto

Seguridad en la Nube:

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad de las plataformas de seguridad en la nube (CSPM, CWP, CIEM)	(Horas disponibles / Horas totales del periodo) × 100	≥ 99.9% mensual	Mensual	Alto
Cobertura de activos cloud monitorizados	(N° de activos monitorizados / N° total de activos en la nube) × 100	≥ 98%	Mensual	Alto
Tiempo medio de detección de desviaciones de configuración (CSPM)	Σ (Tiempo desde aparición hasta detección) / N° de desviaciones	≤ 1 hora	Mensual	Alto
Tiempo medio de respuesta ante alertas de carga de trabajo (CWP)	Σ (Tiempo desde alerta hasta primera acción) / N° de alertas	≤ 15 minutos	Mensual	Alto
Porcentaje de privilegios excesivos detectados (CIEM)	(N° de identidades con privilegios excesivos / N° total de identidades evaluadas) × 100	≤ 5%	Mensual	Medio

Secure Access Service *Edge* (SASE):

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad global de la solución SASE	(Horas disponibles / Horas totales del periodo) × 100	≥ 99,5%	Mensual	Alto
Disponibilidad del componente SWG	(Horas disponibles / Horas totales del periodo) × 100	≥ 99,5%	Mensual	Alto
Disponibilidad del componente CASB	(Horas disponibles / Horas totales del periodo) × 100	≥ 99,5%	Mensual	Alto
Disponibilidad del componente FWaaS	(Horas disponibles / Horas totales del periodo) × 100	≥ 99,5%	Mensual	Alto
Disponibilidad del componente DLP	(Horas disponibles / Horas totales del periodo) × 100	≥ 99,5%	Mensual	Alto
Tiempo medio de aplicación de políticas de acceso (CASB / FWaaS)	Σ (Tiempo desde solicitud hasta aplicación efectiva) / N° de cambios	≤ 2 horas	Mensual	Medio
Porcentaje de tráfico	(N° de sesiones inspeccionadas / N°	≥ 99%	Mensual	Alto

inspeccionado por SWG	total de sesiones web) × 100			
Porcentaje de detección de fuga de datos (DLP)	(N° de intentos de fuga detectados / N° total de intentos) × 100	≥ 98%	Mensual	Alto
Porcentaje de accesos bloqueados por políticas CASB	(N° de accesos bloqueados / N° total de intentos de acceso a apps cloud) × 100	≥ 98%	Mensual	Alto
Tiempo medio de respuesta ante incidentes detectados por SASE	Σ (Tiempo desde alerta hasta primera acción) / N° de incidentes	≤ 15 minutos	Mensual	Alto

Servicio de filtrado de correo electrónico:

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad del servicio de filtrado	(Horas disponibles / Horas totales del periodo) × 100	≥ 99,5%	Mensual	Alto
Porcentaje de correos maliciosos detectados	(N° de correos maliciosos bloqueados / N° total de correos maliciosos recibidos) × 100	≥ 99%	Mensual	Alto
Tasa de detección de spam	(Correos spam detectados / Total correos spam recibidos) × 100	≥ 98%	Mensual	Alto
Porcentaje de falsos positivos	(N° de correos legítimos bloqueados / N° total de correos legítimos) × 100	≤ 0.5%	Mensual	Medio
Tiempo medio de entrega de correos legítimos	Σ (Tiempo desde recepción hasta entrega) / N° de correos legítimos	≤ 30 segundos	Mensual	Alto
Tiempo medio de actualización de reglas de filtrado	Σ (Tiempo desde publicación de nueva amenaza hasta actualización de reglas) / N° de actualizaciones	≤ 4 horas	Mensual	Alto
Porcentaje de cumplimiento de políticas de filtrado definidas	(N° de correos filtrados según política / N° total de correos procesados) × 100	≥ 98%	Mensual	Alto

Servicio de pruebas de penetración (Pentesting):

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Tiempo máximo de inicio de prueba desde solicitud	Días desde solicitud formal hasta inicio de la prueba	≤ 10 días hábiles	Por evento	Medio
Porcentaje de cobertura de activos definidos en el alcance	(N° de activos evaluados / N° total de activos definidos) × 100	≥ 100%	Por prueba	Medio
Tiempo máximo de entrega del informe técnico	Días desde finalización de la prueba hasta entrega del informe	≤ 5 días hábiles	Por prueba	Medio

Servicio de respuesta ante incidentes forenses digitales (*DFIR*):

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Tiempo de respuesta inicial ante incidente crítico (IR)	Tiempo desde notificación del incidente hasta inicio de intervención	≤ 1 hora	Por incidente	Alto
Tiempo medio de contención de incidentes	Σ (Tiempo desde detección hasta contención) / N° de incidentes	≤ 4 horas	Mensual	Alto
Tiempo medio de entrega de informe forense (DF)	Σ (Tiempo desde finalización del análisis hasta entrega del informe) / N° de informes	≤ 5 días	Mensual	Medio
Porcentaje de incidentes con análisis forense completo	(N° de incidentes con informe completo / N° total de incidentes gestionados) × 100	≥ 95%	Mensual	Alto
Porcentaje de cumplimiento de procedimientos de cadena de custodia	(N° de casos con cadena de custodia documentada / N° total de casos forenses) × 100	≥ 100%	Mensual	Alto
Porcentaje de incidentes cerrados dentro del plazo acordado	(N° de incidentes cerrados en plazo / N° total de incidentes) × 100	≥ 90%	Mensual	Alto

Servicio de asesoría y asistencia legal especializada en ciberseguridad:

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Tiempo máximo de respuesta a solicitud de asesoría	Días desde la solicitud formal hasta la primera reunión o entrega de orientación	≤ 3 días hábiles	Por evento	Alto
Porcentaje de cumplimiento de plazos de entrega de informes o dictámenes	(N° de entregas en plazo / N° total de entregas) × 100	≥ 95%	Trimestral	Medio

Incorporación de perfiles profesionales especializados:

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Tasa de rotación del personal asignado	N° de cambios de perfil durante el contrato	≤ 1 cambio total	Anual / Final de contrato	Alto
Tiempo máximo de sustitución de perfil clave	Días desde la baja del recurso hasta incorporación del reemplazo	≤ 10 días hábiles	Por evento	Alto
Porcentaje de continuidad operativa en cambios de personal	(N° de cambios con transición documentada y sin impacto / N° total de cambios) × 100	≥ 100%	Trimestral	Alto
Porcentaje de cumplimiento de dedicación acordada	(Horas efectivas / Horas planificadas) × 100	≥ 95%	Mensual	Alto

Servicio de mantenimiento integral de soluciones de Ciberseguridad:

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Porcentaje de mantenimiento preventivo ejecutado según plan	(N° de mantenimientos realizados / N° planificados) × 100	≥ 100%	Trimestral	Alto
Porcentaje de actualizaciones aplicadas en plazo	(N° de actualizaciones aplicadas / N° planificadas) × 100	≥ 95%	Trimestral	Medio
Porcentaje de cumplimiento en la custodia de credenciales privilegiadas	(N° de accesos registrados / N° total de accesos a credenciales) × 100	100%	Mensual	Alto
Porcentaje de componentes con documentación técnica actualizada	(N° de componentes con documentación vigente / N° total de componentes gestionados) × 100	100%	Trimestral	Medio

Otros Indicadores:

Indicador	Fórmula de Cálculo	Valor Objetivo	Freq. Medición	Nivel de Crit.
Disponibilidad del Interlocutor Único	(Días disponibles / Días hábiles) × 100	≥ 95%	Mensual	Medio
Tiempo máximo de respuesta del Interlocutor Único	Tiempo desde la consulta hasta la primera respuesta efectiva	≤ 1 día hábil	Mensual	Medio
Entrega de informes solicitados	N° de informes entregados en plazo / Total informes solicitados	100% en plazo	Mensual	Medio
Calidad de la documentación técnica	N° de documentos rechazados por deficiencias / Total documentos entregados	≤ 5%	Trimestral	Bajo
Porcentaje de cumplimiento de entregables contractuales	(N° de entregables cumplidos / N° total de entregables comprometidos) × 100	≥ 98%	Trimestral	Medio

c. Penalizaciones válidas para todos los apartados.

Con el objetivo de garantizar la calidad del servicio prestado, se establece un sistema de penalizaciones asociado al incumplimiento de los indicadores definidos en el presente pliego. Dichos indicadores se agrupan en función de su nivel de criticidad, conforme al impacto que su incumplimiento pueda tener sobre la continuidad del servicio, la satisfacción del usuario o la eficiencia operativa.

Es así, que las penalizaciones se aplicarán mensualmente, en función del grado de desviación respecto al valor objetivo (ANS) de cada indicador, según el siguiente esquema:

Nivel de Criticidad	Penalización por desviación	Máximo mensual por nivel
Alto	0.5% por cada 5 puntos de desviación respecto al valor objetivo	Hasta 4% del total mensual
Medio	0.25% por cada 5 puntos de desviación	Hasta 1.5% del total mensual
Bajo	0.1% por cada 5 puntos de desviación	Hasta 0.5% del total mensual
Monitorización	Sin penalización económica	-

El importe total de penalizaciones aplicables en un mismo mes no podrá superar, en ningún caso, el **5% del importe total facturado** en dicho periodo.

De acuerdo con lo establecido, las penalizaciones no serán de aplicación hasta que el servicio haya concluido la fase de estabilización y se encuentre en régimen de operación regular. Esta fase será definida y acordada entre las partes, y su finalización deberá constar por escrito.

d. Informe periódico de seguimiento de los ANS

Durante los primeros días de cada mes, el adjudicatario deberá entregar a CRE un informe mensual de seguimiento, correspondiente al mes natural anterior. Este informe tendrá como finalidad evaluar el grado de cumplimiento de los ANS acordados.

El informe deberá incluir, como mínimo, la siguiente información para cada ticket gestionado:

- Identificador y descripción del ticket.
- Persona que generó la solicitud.
- Fecha y hora de comunicación del ticket al adjudicatario.
- Nivel de criticidad del servicio afectado.
- Nivel de impacto del ticket.
- Nivel de prioridad asignado.
- Tiempos registrados: atención, respuesta y resolución.
- Relación de tickets pendientes de resolución al cierre del período.

Con base en esta información, y conforme a los procedimientos definidos, se calculará el grado de cumplimiento de los ANS correspondientes al período reportado.

e. Evolución y mejora de los ANS

CRE evaluará positivamente la incorporación de indicadores adicionales propuestos por el proveedor, siempre que dichos indicadores sean medibles utilizando las herramientas de las que dispone CRE, o que el proveedor demuestre un sistema claro y válido para su medición.

Asimismo, CRE valorará de forma positiva la presentación de una planificación detallada y una metodología de evolución para los Acuerdos de Nivel de Servicio (ANS). Esta planificación debe permitir un mayor grado de especificación en el dimensionamiento del servicio, asegurando así su continua mejora.

El Acuerdo de Nivel de Servicio será objeto de revisión anual, o en cualquier momento que alguna de las partes lo solicite, para evaluar su efectividad y realizar las modificaciones necesarias en función de los cambios en las necesidades o en el entorno de la institución.

Anexo 2 DATOS DE IDENTIFICACIÓN

RAZÓN SOCIAL	NIF	
Domicilio Social	**CP**	**Población / Provincia**

PERSONA DE CONTACTO: nombre y apellidos	Teléfonos de contacto
Cargo que ocupa	**Dirección de correo electrónico**

PERSONAS DE CONTACTO ALTERNATIVAS: Nombre y Apellidos	Teléfonos de contacto
Cargo que ocupa	**Dirección de correo electrónico**

REFERENCIAS EN SERVICIOS SIMILARES	

Facturación anual (miles de €)	2022	2023	2024
Perdidas/Ganancias (miles de €)	**2022**	**2023**	**2024**

Anexo 3 DECLARACIÓN RESPONSABLE

Don/Dña. ....., con DNI ....., actuando en nombre y representación de ....., con NIF....., en su condición de ..... y con poderes suficientes para subscribir la presente Declaración Responsable, enterado de la convocatoria del procedimiento de contratación para la selección del contrato,

DECLARA RESPONSABLEMENTE QUE:

1. La empresa que representa no incurre en prohibición de contratar o de recibir subvenciones con/de las entidades del sector público.
2. El órgano de gobierno o administración de la empresa que representa no está compuesto por alguna persona directiva, empleada o voluntaria de Cruz Roja.
3. La empresa que representa cumple con los requisitos de capacidad y solvencia necesarios para garantizar el contrato de referencia.
4. Se encuentra al corriente de obligaciones tributarias con el Estado y CCAA.
5. Se encuentra al corriente de obligaciones con sus trabajadores y con la Seguridad Social.
6. Está dado de alta al Impuesto sobre Actividades Económicas y al corriente de su pago, cuando se ejerzan actividades sujetas en este impuesto.
7. Declara responsablemente no haber participado en la elaboración de las condiciones técnicas o en los documentos preparatorios del contrato objeto de este suministro.
8. Se compromete, en el momento que sea requerido por Cruz Roja, a aportar la documentación acreditativa de todos los requisitos exigidos por CRE para la contratación y que Declara responsablemente cumplir mediante la presente.
9. Que respeta los DIEZ PRINCIPIOS DEL PACTO MUNDIAL DE NACIONES UNIDAS, al que se refiere el presente documento.
10. Que dispondrá de un teléfono de atención y resolución de incidencias y/o medio de comunicación análogo mediante el que responderá ante Cruz Roja en un plazo máximo de 24 horas desde que Cruz Roja comunique la referida incidencia.
11. Que acepta que la documentación y condiciones mencionadas en el presente documento se incluirán en el contrato de referencia con carácter contractual.

Y a los efectos oportunos, se firma la presente, a ..... de ..... del 2025.

Firma:

Anexo 4 PROPOSICIÓN ECONÓMICA Y CRITERIOS AUTOMÁTICOS

D/Dña ....., con DNI ....., y con domicilio a efecto de notificaciones en ....., actuando en nombre propio o de la empresa ..... NIF ....., en calidad de ....., manifiesta que, aceptando de forma expresa todas las cláusulas, requisitos y condiciones que constan en el documento de requerimientos para la contratación de los **SERVICIOS DE CIBERSEGURIDAD.** se compromete a asumir el cumplimiento del contrato que del mismo se derive formulando la siguiente

PROPOSICION ECONÓMICA

SERVICIO	Importe Máximo	Importe Ofertado
IMPORTE ECONÓMICO (SIN IVA)	n/a	€
IVA	n/a	€
IMPORTE ECONÓMICO (IVA INCLUIDO)	n/a	€

La oferta se presenta con todos los gastos e impuestos incluidos.

Y a los efectos oportunos, se firma la presente, a ..... de ..... del 2025.

Firma: