CONTRATO DE SERVICIOS PARA LA OFICINA DE SEGURIDAD DIGITAL DE LOS SERVICIOS CENTRALES Y LA RED EXTERIOR Y TERRITORIAL DE ICEX ESPAÑA EXPORTACIÓN E INVERSIONES, E.P.E.

REUNIDOS

De una parte, Dña. Elisa Carbonell Martín, en su calidad de consejera delegada de **ICEX España Exportación e Inversiones, E.P.E.,** con domicilio en Madrid, Paseo de la Castellana, núm. 278, y provista de NIF Q2891001F, actuando en nombre y representación de esta entidad por delegación expresa del Consejo de Administración mediante acuerdo de 24 de julio de 2024, en adelante **ICEX**.

Y, de otra, D. Alfredo Diez Fernandez, mayor de edad, en su calidad de apoderado de la compañía **Cipherbit, S.L.U**, con NIF B01644558, y domicilio en Rivas Vaciamadrid, Madrid, calle Marie Curie, 19, en virtud de escritura de poder de fecha 28 de junio de 2023, otorgada ante el Notario de Madrid, D. Luis Quiroga Gutiérrez, con el número 1873 de su protocolo, en lo sucesivo el **CONTRATISTA**.

MANIFIESTAN

I. Que, con fecha 29 de enero de 2024 ICEX publicó en la Plataforma de Contratación del Sector Público una licitación para adjudicar la contratación del servicio de oficina de seguridad digital de los servicios centrales y la red exterior y territorial de ICEX, de forma que dichos servicios constituían el Lote 2 del expediente de licitación número 162/2023, habiendo resultado adjudicatario el CONTRATISTA de esta licitación que constaba de tres lotes diferenciados.

II. Que, el CONTRATISTA tiene entre sus fines sociales la realización de estos servicios.

III. Que, para el desarrollo de la actividad que constituye su objeto, el CONTRATISTA cuenta dentro de su organización con los medios técnicos y materiales adecuados y con personal especialmente capacitado para su realización.

IV. Que, el CONTRATISTA ratifica su interés en la prestación de los citados servicios y demás funciones que se le encomiendan en el presente Contrato.

Y teniendo ambas partes capacidad legal suficiente, que mutuamente se reconocen, convienen en otorgar el presente Contrato, el cual formalizan y llevan a efecto de acuerdo con las siguientes:

CLÁUSULAS

PRIMERA. - Objeto del Contrato

El presente Contrato tiene por objeto la contratación del servicio de oficina de seguridad digital para los servicios centrales y la red exterior y territorial de ICEX y la puesta en marcha de una arquitectura SASE de forma completa.

El CONTRATISTA deberá ejecutar el objeto del Contrato con estricta sujeción a su clausulado incluyendo su Anexo 1, por la que se regula la condición de encargado de tratamiento de los datos del CONTRATISTA, y lo establecido en los pliegos reguladores de la licitación nº 162/2023 de fecha 29 de enero de 2024, y a su oferta técnica y económica de fechas 14 y 15 de marzo de 2024 respectivamente, que se adjuntan al presente Contrato como Anexos 2 y 3.

SEGUNDA. - Alcance del Contrato

2.1 Tareas y servicios

El objeto del presente contrato es la contratación de una oficina de seguridad digital y la puesta en marcha de una arquitectura SASE de forma completa con el objetivo de disponer de un alto nivel de ciberseguridad y ciber resiliencia en los activos de ICEX y en los procesos de negocio soportados por dichos activos, abarcando la extensión completa del entorno tecnológico de ICEX y proporcionando servicios de ciberseguridad, adicionales, de valor añadido. Tal y como se detalla en el punto *5.1.1. Alcance del servicio* del Pliego de Prescripciones Técnicas (en adelante, PPT) los servicios que debe ejecutar el CONTRATISTA se dividen en los siguientes subservicios, en línea con el marco de ciberseguridad del NIST:

- Oficina de seguridad digital
- Identificación y prevención
- Protección
- Detección y respuesta
- Gestión de incidencias, peticiones y problemas

El servicio prestado deberá dar cobertura de ciberseguridad a los procesos y activos identificados y ajustarse a los requisitos definidos detalladamente en el PPT y a los acuerdos de nivel de servicio indicados en el mismo. Además de las tareas propias de la oficina de seguridad digital arriba mencionadas cuyos requisitos técnicos y funcionales se detallan en el punto *5.2 Requisitos Técnicos del Servicio* del PPT, el coordinador del Servicio del Lote 2 será el encargado de proporcionar y notificar toda la información relacionada con la prestación de servicios cuando sea solicitada por el Jefe de la Oficina de Gestión y Transformación del Lote 3, ya que es el contratista de ese Lote 3 el que tiene la responsabilidad de coordinar las actividades que deben llevarse a cabo en cada uno de los lotes del presente expediente. Dentro del ámbito de los servicios de gobernanza y soporte se considera la ejecución de, al menos, las siguientes tareas principales inter-lotes:

- Reportar al adjudicatario del Lote 3 respecto al estado de las actividades de puesta en marcha, implantación y prestación de los servicios correspondientes a este Contrato.
- Informar de posibles alertas identificadas, puntos críticos y acciones que puedan impactar en la correcta ejecución de los servicios.
- Participar en reuniones periódicas de seguimiento de los servicios (aspectos técnicos y/o aspectos que puedan afectar al desarrollo de cada proyecto o servicio) organizadas por el adjudicatario del Lote 3, para asegurar la adecuada puesta en marcha y ejecución de los mismos.
- Asistencia a las reuniones periódicas de los Comités de Gestión Operativa.

2.2 Requisitos y Fases de ejecución del servicio

Los requisitos para la correcta prestación del servicio son los descritos en los apartados 5.3.1 a 5.3.12 del PPT, donde se recogen con detalle todas las especificidades para la adecuada ejecución de tareas. En el punto 5.3.13 se desarrollan las fases principales de ejecución que se deben llevar a cabo en función de los servicios a implantar y de los servicios a prestar:

a) Fase 1 Adquisición de conocimiento: Se realiza la transferencia de conocimiento y de toda la documentación disponible al CONTRATISTA sobre la infraestructura tecnológica, procesos y procedimientos de todos los servicios que se prestan en la actualidad en ICEX. El CONTRATISTA deberá adquirir los conocimientos necesarios para la prestación de los servicios requeridos en este contrato. La duración de esta fase será desde la fecha de formalización del contrato hasta el 31 de octubre de 2024.

b) Fase 2 Prestación de servicio: Finalizada la fase 1 de Adquisición de conocimiento dará comienzo la Fase 2 "Prestación de servicio", en la que el CONTRATISTA será plenamente responsable del servicio, cuyo objeto es realizar las actividades necesarias que permitan la continuidad de los servicios y a la vez la evolución y transformación a una arquitectura SASE conforme los requisitos establecidos en el presente procedimiento. En esta fase serán de aplicación los ANS y será facturable de conformidad con lo dispuesto por la cláusula séptima siguiente.- Precio y Forma de pago, del presente Contrato.

c) Fase 3 Devolución del servicio: Esta fase deberá iniciarse sesenta (60) días naturales antes de la finalización del presente Contrato, y contemplará un periodo de transferencia de conocimiento del servicio a quien ICEX determine. Los trabajos a desarrollar necesarios para la devolución del servicio no conllevarán coste económico adicional para ICEX. El CONTRATISTA podrá incurrir en las penalizaciones correspondientes según lo establecido en la cláusula octava siguiente.- Penalidades ante el retraso en el comienzo de la devolución del servicio.

2.3. Mejoras

Tal y como dispuso el CONTRATISTA en su oferta, cumplirá con las mejoras y características respecto al equipo de trabajo. En concreto, cumplirá con las exigencias de especialización y tiempo de experiencia del equipo de trabajo propuesto, por encima de lo dispuesto como obligatorio en el PPT.

2.4 Entregables asociados al servicio

ICEX determinará la documentación que el CONTRATISTA deberá entregar, pudiendo ser, además de la indicada en los apartados 5.2.3 Oficina de Seguridad Digital, 5.2.4 Servicio de Identificación y Prevención, 5.2.5 Servicio de Protección, 5.2.6 Servicio de Detección y Respuesta y 5.2.7 Gestión de Incidencias, Peticiones y Problemas del PPT, por ejemplo:

- Procedimientos.
- Instrucciones Técnicas.
- Políticas.
- Mejoras.
- Análisis.
- Diseño de arquitecturas hardware y software.
- Estudios de viabilidad.
- Consultorías TI.
- Planificaciones de los proyectos.
- Reportes de incidentes.
- Evaluaciones de riesgos y vulnerabilidades.
- Informes de seguimiento y avance de los proyectos y servicios.
- Acuerdos de niveles de servicios (ANS).
- Actas.
- Plan de transferencia.
- Informes de auditoría.
- Manuales de usuario.
- Manuales de procedimientos y resolución de problemas.
- Materiales de concienciación.
- Simulacros.
- Playbooks.
- Tutoriales y manuales de formaciones.
- Mapa de integraciones; así como
- Cualquier otra documentación que ICEX determine.

Sin perjuicio de los demás documentos entregables técnicos y de gestión mencionados por el CONTRATISTA en su oferta vinculados a las distintas fases que integran la prestación del servicio.

2.5. Planificación, dirección y seguimiento de los trabajos

Corresponde a ICEX la supervisión y dirección generales de los trabajos, así como proponer las modificaciones convenientes o, en su caso, proponer la suspensión de los mismos si existiese causa suficiente motivada de conformidad con lo dispuesto en el apartado 5.3.10 del PPT.

ICEX designará una persona que desarrollará las labores de gestor técnico de conformidad con lo dispuesto en el referido apartado 5.3.10 del PPT, por su parte el CONTRATISTA designará a un/a

Coordinador/a del Servicio que actuará como interlocutor con ICEX y será el único empleado del CONTRATISTA al que ICEX dé las instrucciones necesarias. Las funciones de ambos perfiles se definen en el apartado 5.3.10 del PPT. Por su parte, el Coordinador del Servicio del CONTRATISTA deberá asimismo coordinarse con el Coordinador Interlotes del Lote 3 de la licitación de referencia 162/2023. Este perfil será el encargado de proporcionar y notificar toda la información relacionada con la prestación de servicios del presente Contrato, cuando sea solicitada, según solicite el jefe de la Oficina de Gestión y Transformación del Lote 3, que centralizará la comunicación inter-lotes, siguiendo las instrucciones y directrices del Gestor Técnico designado por ICEX. Esto incluye la necesidad de comunicarse, compartir documentos, entregar trabajos o documentación asociada, así como los procesos, procedimientos e instrucciones técnicas específicas del presente Contrato. Las funciones de gobernanza incluirán todos aquellos aspectos detallados en el apartado 5.1.2 del PPT.

2.6. Franja para la realización del servicio

De acuerdo con lo previsto en el PPT, el horario de prestación del servicio se establecerá por el Gestor Técnico de ICEX al comienzo de los trabajos y se podrá revisar en las reuniones periódicas de seguimiento del proyecto. Inicialmente, y con carácter general, el Servicio se prestará de lunes a viernes, excepto festivos nacionales, en un horario comprendido entre las 8:00 y las 18:30 horas. Los perfiles de Analistas de Seguridad (24x7), seguirán prestarse en horario 24x7 para lo cual, el CONTRATISTA deberá establecer un modelo de guardias en el que se siempre se mantengan dos recursos de los perfiles asociados a los servicios indicados en los apartados del PPT 5.2.4 Servicio de Identificación y Prevención, 5.2.5 Servicio de Protección, 5.2.6 Servicio de Detección y Respuesta y 5.2.7 Gestión de Incidencias, Peticiones y Problemas, que realizarán todas las tareas de los niveles mencionados para lo cual, el CONTRATISTA deberá proporcionar un teléfono de guardia a cada recurso. Las guardias, se considerarán carga de trabajo.

El CONTRATISTA debe facilitar un teléfono de guardia, uno para el/la Jefe/a de servicio de la Oficina de Seguridad y otro para el/la Coordinador/a de Seguridad, uno por cada recurso que esté de guardia en horario 24x7 estando obligado a dar continuidad al servicio en aquellos casos que ICEX considere críticos, así como la planificación de actividades fuera del horario definido.

TERCERA. - Medios técnicos y humanos

El CONTRATISTA declara que, cuenta con una organización propia y estable, viabilidad económica, clientela ajena al sector público y medios materiales y personales necesarios para el desarrollo de la actividad contratada. El CONTRATISTA se compromete a asignar al servicio objeto del presente Contrato, como obligación esencial del contrato al menos todos los medios técnicos y personales recogidos en el apartado *5.4 Medios Personales* del PPT, así como los descritos en su oferta técnica. A este respecto, el CONTRATISTA se compromete como mínimo a adscribir, con una dedicación del 100%, hasta la finalización del Contrato a los siguientes perfiles con al menos las cualidades indicadas en su Oferta:

- Jefe/a de Servicio de la Oficina de Seguridad: 1 recurso.
- Consultor/a Oficina de Seguridad: 2 recursos.
- Coordinador/a de Seguridad: 1 recurso.
- Analistas de Seguridad: 2 recursos.
- Analistas de Seguridad (24x7): 2 recursos.

El CONTRATISTA deberá contar con el personal preciso que cubra las posibles bajas o sustituciones de los profesionales que inicialmente ha asignado a la prestación del servicio. Igualmente, durante el periodo de vigencia del contrato, el CONTRATISTA garantizará la estabilidad del equipo asignado. Si durante este periodo se produjeran sustituciones superiores al quince por ciento (15%) del total del equipo, mensualmente se impondrán las penalizaciones previstas a este respecto en la cláusula octava del presente Contrato. La incorporación, sustitución o baja de las personas designadas por el CONTRATISTA requerirá la previa aprobación por parte de ICEX y que las/los sustitutas/os tengan al menos la misma cualificación y experiencia que los perfiles inicialmente asignados al presente Contrato. Asimismo, ICEX se reserva el derecho a solicitar y obtener la baja de las personas asignadas, cuando

concurran circunstancias que así lo aconsejen, entre otras y sin tener carácter exclusivo, la falta de formación y/o experiencia requerida o la falta de competencia para el desarrollo del trabajo objeto del contrato. En caso de que haya incumplimientos en el plazo de incorporación y/o sustitución de recursos se aplicaran las penalizaciones correspondientes de conformidad con lo estipulado en la cláusula octava siguiente. El CONTRATISTA ha designado que los perfiles de Jefe/a de Servicio de Oficina de Seguridad y Coordinador/a de Seguridad formarán parte necesariamente de la propia plantilla del CONTRATISTA. Estas personas tendrán entre sus funciones las indicadas en los pliegos reguladores de la presente contratación y que forman parte del Contrato.

La ejecución del Contrato implicará la dotación de infraestructura suficiente (ordenadores, licencias, software, teléfonos, etc.) a los equipos humanos. Será responsabilidad exclusiva del CONTRATISTA proveer a aquellos de los equipos antedichos, de los gastos asociados al uso de estos, así como la formación necesaria para prestar el Servicio.

CUARTA. - Obligaciones del CONTRATISTA respecto a su personal o colaboradores

Los trabajadores o colaboradores que el CONTRATISTA emplee o contrate para la ejecución del Contrato, aunque éste haya de desarrollarse parcialmente en las instalaciones de ICEX, estarán exclusivamente vinculados al CONTRATISTA, sin vínculo laboral alguno con ICEX, siendo aquél el único y absoluto responsable del cumplimiento de las obligaciones que la legislación vigente le imponga como empleador y ejerciendo plenamente sus facultades directivas y organizativas que como empresario le correspondan en relación con dicho personal, incluido el poder disciplinario y la concesión de permisos y vacaciones. Las relaciones sindicales del personal del CONTRATISTA con éste se sustanciarán igualmente de forma exclusiva entre ambos. No obstante lo anterior, ICEX podrá cursar las instrucciones técnicas necesarias en materia de servicio a los responsables del CONTRATISTA para que, a través de sus coordinadores, se trasladen las órdenes oportunas a su personal, reservándose asimismo ICEX la facultad de supervisar el trabajo efectuado por el CONTRATISTA. El CONTRATISTA deberá estar al corriente, y será de su única responsabilidad, en el pago de tributos, nóminas y cuotas a la Seguridad Social. En caso de incumplimiento de lo dispuesto en esta cláusula, ICEX queda expresamente facultado para reclamar al CONTRATISTA en cuestión la totalidad de las cuantías que pudieran derivarse de las responsabilidades que pretendan hacerse valer frente a ICEX, por cualquiera de los conceptos señalados anteriormente.

QUINTA. - Riesgo y ventura

La ejecución del Contrato se realizará a riesgo y ventura del CONTRATISTA.

SEXTA. – Duración del Contrato

La duración del Contrato será para las fases de prestación del servicio y devolución del servicio de cuarenta y ocho (48) meses desde el día 1 de noviembre de 2024.

,

La fase de adquisición del conocimiento transcurrirá desde la fecha de formalización del presente Contrato hasta el 31 de octubre de 2024.

El Contrato no se podrá prorrogar, sólo podrá prorrogarse excepcionalmente el Contrato en el supuesto contemplado en el último párrafo del artículo 29.4 de la Ley de Contratos de Sector Público.

SÉPTIMA. - Precio y forma de pago

El importe máximo total del Contrato es de tres millones treinta y un mil ochocientos dieciséis euros con sesenta y seis céntimos (3.031.816,66 €) IVA incluido, con el siguiente desglose:

- Base imponible: 2.505.633,60 €
- IVA: 526.183,06 €

El precio estimado como contraprestación a los servicios objeto del presente Contrato viene

determinado por el precio hora ofertado por el CONTRATISTA para cada uno de los perfiles y el número total de horas estimado para cada recurso. Incluidos en el Anexo III- 2 de la oferta económica y de criterios automáticos del CONTRATISTA de fecha 15 de marzo de 2024 y que se desglosan a continuación. El precio por hora a abonar para cada uno de los perfiles del proyecto será el siguiente:

PERFIL	Nº RECURSOS	HORAS RECURSO	PRECIO HORA SIN IMPUESTOS
Jefe/a de Servicio de Oficina de Seguridad	1	[redacted]	
Consultor/a Oficina de Seguridad	2		
Coordinador/a de Seguridad	1		
Analista de Seguridad	2		
Analista de Seguridad Servicio 24x7	2		
TOTAL	8	66.560	2.505.633,60 €

El CONTRATISTA tendrá derecho al abono, con arreglo a los precios convenidos, de los servicios/trabajos efectivamente prestados. El precio será pagadero con carácter mensual, previa presentación de la factura por parte del CONTRATISTA, y aceptación por parte de los responsables de ICEX de los trabajos realizados en dicho periodo. Deberán desglosarse mensualmente las horas dedicadas a cada uno de los servicios con los perfiles correspondientes que lo componen, siendo dichas horas las que serán facturables cada mes:

- Servicio de implantación de arquitectura SASE
- Servicio de Oficina de Seguridad Digital
- Servicio de Identificación y Prevención.
- Servicio de Protección
- Servicio de Detección y Respuesta
- Servicio de Gestión de incidencias, peticiones y problemas

La facturación se efectuará por periodos mensuales en base al precio de las horas dedicadas por cada recurso para la realización los trabajos y aceptadas por ICEX de conformidad con el Informe Mensual entregado por el CONTRATISTA. Las facturas serán atendidas en un plazo no superior a treinta (30) días desde su presentación de forma electrónica a través de la Oficina Virtual de ICEX (https://oficinavirtual.icex.es/facturacion/inicio), una vez descontadas las penalizaciones – si las hubiere – y previa aceptación, por parte de los responsables de ICEX, de los trabajos realizados. Las facturas deberán incluir:

- Número de expediente: 162/2023/Lote 2
- Departamento de facturación: Dirección de Tecnologías de la Información
- Nº propuesta: 202400456
- Posición de gasto: 1

OCTAVA. – Penalizaciones

El servicio se prestará mediante un modelo gestionado, en el que la gestión y la realización de actividades y productos es responsabilidad del CONTRATISTA, y la prestación del servicio está basada en los compromisos adquiridos por éste a través de los Acuerdos de Nivel de Servicio (ANS) detallados en los pliegos, cuyo incumplimiento derivará en la aplicación de las penalidades previstas en esta cláusula. Ante situaciones en las que el CONTRATISTA incurra en demora de forma recurrente o proporcionen servicios de una evidente calidad inferior a lo requerido, ICEX podrá optar indistintamente por la resolución del contrato en cuestión, con pérdida de la fianza en caso de haberse exigido, o por la imposición de las penalizaciones que se especifican a continuación. Los ANS que garantizan la calidad de dichos servicios acordados en el presente Contrato se ejecutan de conformidad con los parámetros e indicadores regulados al efecto en el apartado 5.6 del PPT y se penalizaran de conformidad con las penalidades asociados a cada uno de ellos y regulados a

continuación. El CONTRATISTA asumirá los ANS señalados en el PPT, que forma parte del presente Contrato.

El CONTRATISTA deberá suministrar a ICEX informes que permitan conocer, de forma detallada, unificada o desglosada el cumplimiento de los parámetros contemplados en el ANS. Estos informes deberán poder ser consultados por ICEX en cualquier momento.

Las penalizaciones aplicables y recogidas en los pliegos reguladores son las siguientes:

INDICADOR	MÉTRICA	NIVEL DE CUMPLIMIENTO	INTERVALO DE MEDIDA	PENALI-ZACIONES
Indicadores propios de incidencias				
Tiempo de Respuesta según prioridad: Muy Crítica <= 5 min Crítica <= 15 min Alta <= 30 min Media <= 1 hora Baja <= 2 horas	% de incidencias que no tienen desviación entre el periodo real de tiempo de respuesta y el periodo máximo de tiempo de respuesta establecido según la prioridad en el periodo de medición	> 97%	Mensual	2,00%
Tiempo de Reasignación según prioridad: Muy Crítica <= 3 min Crítica <= 4 min Alta <= 7 min Media <= 15 min Baja <= 20 min	% de incidencias que no tienen desviación entre el periodo real de tiempo de reasignación y el periodo máximo de tiempo de reasignación establecido según la prioridad en el periodo de medición	> 97%	Mensual	2,00%
Tiempo de inicio de resolución según prioridad: Muy Crítica <= 4 min Crítica <= 5 min Alta <= 7 min Media <= 15 min Baja <= 20 min	% de incidencias que no tienen desviación entre el periodo real de tiempo de inicio de resolución y el periodo máximo de tiempo de inicio de resolución establecido según la prioridad en el periodo de medición	> 97%	Mensual	2,00%
Tiempo de Resolución según prioridad: Muy Crítica: 2 horas Crítica <= 4 horas Alta: <= 8 horas Media <= 24 horas Baja <= 48 horas	% de incidencias que no tienen desviación entre el periodo real de tiempo de resolución y el periodo máximo de tiempo de resolución establecido según la prioridad en el periodo de medición	>= 98%	Mensual	2,00%
Resolución por Base de Datos de Conocimiento	% de incidencias que han sido resueltas a partir de información existente en la Base de Datos de Conocimiento	>=50%	Mensual	0,80%
Reapertura de tickets	% incidencias reabiertas frente al total registradas en el periodo de medición	<= 2%	Mensual	0,40%
Indicadores de peticiones de servicio				
Tiempo de Respuesta según prioridad: Muy Crítica <= 10 min Crítica <= 15 min Alta <= 30 min Media <= 1 hora Baja <= 2 horas	% de peticiones que no tienen desviación entre el periodo real de tiempo de respuesta y el periodo máximo de tiempo de respuesta establecido según la prioridad en el periodo de medición	> 97%	Mensual	1,50%
Tiempo de Reasignación según prioridad: Muy Crítica <= 3 min Crítica <= 4 min Alta <= 7 min Media <= 15 min Baja <= 20 min	% de peticiones que no tienen desviación entre el periodo real de tiempo de reasignación y el periodo máximo de tiempo de reasignación establecido según la prioridad en el periodo de medición	> 97%	Mensual	1,50%

Tiempo de inicio de resolución según prioridad: Muy Crítica <= 10 min Crítica <= 20 min Alta <= 30 min Media <= 1 horas Baja <= 2 horas	% de peticiones que no tienen desviación entre el periodo real de tiempo de inicio de resolución y el periodo máximo de tiempo de inicio de resolución establecido según la prioridad en el periodo de medición	> 97%	Mensual	1,50%
Tiempo de Resolución según prioridad: Muy Crítica: 2 horas Crítica <= 4 horas Alta: <= 8 horas Media <= 24 horas Baja <= 72 horas	% de peticiones que no tienen desviación entre el periodo real de tiempo de resolución y el periodo máximo de tiempo de resolución establecido según la prioridad en el periodo de medición	>= 98%	Mensual	1,50%
Resolución por Base de Datos de Conocimiento	% de peticiones que han sido resultas a partir de información existente en la Base de Datos de Conocimiento	>=50%	Mensual	0,80%
Reapertura de tickets	% peticiones reabiertas frente al total registradas en el periodo	<= 2%	Mensual	0,40%
Indicadores de calidad				
Calidad de la documentación entregada	% Entregables que son entregados en forma, entendiéndose como tal la ausencia de No Conformidad según lo establecido en el apartado 5.6.1 Criterios de Medición del PPT	>= 95% de los documentos entregados en forma	Mensual	0,30%
Cumplimiento de plazo de entrega de documentación	% Entregables que son entregados en tiempo, entendiéndose como tal el cumplimiento de la fecha de entrega requerida por ICEX	>= 95% de los documentos entregados en tiempo	Mensual	0,30%
Cumplimiento de la calidad de ejecución y prestación del servicio	% de no conformidades en la ejecución y prestación del servicio	< 10% de no conformidades	Mensual	0,30%
Cumplimiento de la documentación entregada	% de desviación entre el número de Playbooks, informes, análisis y planes periódicos entregados y el número de Playbooks, informes, análisis y planes reales.	<= 2%	Mensual	0,20%
Indicadores de equipo de trabajo				
Rotación equipo de trabajo	% Porcentaje de rotación del equipo	<=15%	Mensual	0,50%
Cumplimiento del plazo de incorporación o sustitución por cada semana natural y por cada medio personal	Diferencia en número de días entre la fecha real de incorporación o sustitución de un medio personal y la fecha acordada con ICEX. Se medirá por cada semana natural y por cada medio personal. En caso de retraso por periodo inferior a una semana o de que existan días que excedan al cómputo semanal que no se puedan contabilizar por semanas, para el cómputo total, se prorrateará por días las penalizaciones que correspondan.	Se requiere que sea < 5 días laborables por recurso	Mensual	1,00%
Indicadores de actividades planificadas				
Cumplimiento de Hito	% desviación, si la hubiere entre la fecha establecida en el plan de trabajo con ICEX para la terminación del hito final de todas aquellas actividades planificadas y la fecha real de terminación del hito	<= 15%	Mensual	0,60%
Indicadores de actividades formativas				
Número de acciones de concienciación	Número mínimo de acciones de concienciación al mes aportando el material asociado a las mismas	>=2	Mensual	0,10%

Número de cursos o seminarios	Número de cursos o seminarios al año aportando el material asociado a los mismos	>=1	Mensual	0,50%
Número de Simulacros de Concienciación	Número de Simulacros de Concienciación al año aportando el material asociado al mismo	>=1	Mensual	0,50%
Indicadores de Infraestructuras/Plataformas				
Disponibilidad	% de disponibilidad mensual de las Infraestructuras, Plataformas, Herramientas	>98%	Mensual	1,00%
Tiempo de recuperación	Tiempo máximo de recuperación de las Infraestructuras, Plataformas, Herramientas	<=1 hora	Mensual	1,00%
Indicadores buzón Oficina de Seguridad				
Tiempo máximo de respuesta a consultas o peticiones en el buzón de OSD	Tiempo máximo de respuesta a consultas o peticiones en el buzón de OSD	<= 2 horas	Mensual	0,10%
Número de Informes de actividad del buzón de OSD	Número de Informes de actividad del buzón de OSD al mes	>=1	Mensual	0,05%
Indicadores de Certificados Digitales				
Renovación Certificados	Tiempo de notificación/preaviso para la renovación de certificados previa caducidad	<= 30 días naturales antes de su caducidad	Mensual	0,60%
Indicadores de Gestión de Activos de Ciberseguridad				
Inventario hardware y software actualizado	% de equipamiento actualizada frente al total auditados	> 99,5%	Mensual	0,50%
Indicadores de Seguridad				
Número de indicadores Sistema de Gestión de Seguridad o Cuadro de Mando	Número mínimo de indicadores definidos para el sistema de gestión de seguridad o Cuadro de Mandos	>= 30	Mensual	0,15%
Indicadores de Riesgo y Cumplimiento				
Número de análisis de riesgos	Número de análisis de riesgos al año	>=1	Mensual	1,50%
Número de planes de mejora o adecuación al ENS en PTR	Número de planes de mejora o adecuación al ENS en PTR al año	>=25	Mensual	0,50%
Indicadores de CiberInteligencia				
Número de controles preventivos	Número mínimo de controles preventivos propuestos/implementados relacionados con los ataques actuales detectados por el HoneyPot u otras fuentes de ciberinteligencia. Al trimestre	>=3	Mensual	0,50%
Número de informes de Ciberinteligencia	Número de informes de Ciberinteligencia al mes	>=1	Mensual	0,60%
Indicadores de Análisis de aplicaciones e infraestructura (caja negra/gris/blanca) y Directorio Activo				
Número de test servicios nuevos	Número mínimo de test de intrusión (caja negra/gris/blanca) por servicio nuevo identificado al mes	>=2	Mensual	1,00%
Número de test ad-hoc	Número mínimo de test de intrusión (caja negra/gris/blanca) ad-hoc al mes	>=3	Mensual	1,00%
Número test Directorio Activo	Número de test de Directorio Activo al semestre	>=2	Mensual	1,00%
Número de test de intrusión	Número de test de intrusión al semestre	>=1	Mensual	1,00%

Tiempo de presentación de los resultados del test de intrusión	Tiempo de presentación de los resultados del test de intrusión transcurrido desde que se realizó el test	<= 15 días	Mensual	0,50%
Indicadores de Vulnerabilidades				
Número de escaneos de red interna	Ejecución escaneos de red interna al semestre (aprox. 3500 IPs)	>= 1	Mensual	1,25%
Número de escaneos de red pública	Ejecución de escaneos de red pública al mes (aprox. 80 IPs)	>= 1	Mensual	1,25%
Número de informes de gestión de vulnerabilidades	Número de informes de gestión de vulnerabilidades al mes	>=1	Mensual	0,50%
Tiempo ejecución escaneos ad-hoc	Tiempo máximo de ejecución de escaneos ad-hoc (limitado a 2 al año)	<= 72 horas	Mensual	0,50%
Tiempo presentación resultados tras escaneos de vulnerabilidades	Tiempo máximo de presentación de resultados tras escaneos de vulnerabilidades (2 al mes)	<= 15 días	Mensual	0,50%
Indicadores de Servicio de Detección y Respuesta				
Número de implantaciones de nuevos casos de uso en los sistemas de detección	Número mínimo mensual de implantación de nuevos casos de uso en los sistemas de detección al mes	>= 2	Mensual	0,50%
Número de informes sobre las herramientas de detección	Número de informes sobre las herramientas de detección al mes	>=1	Mensual	0,40%
Tiempo de diagnóstico inicial incidentes de seguridad Muy Críticos	Tiempo máximo de diagnóstico inicial de incidentes de seguridad catalogados como MUY CRÍTICOS	<= 30 min	Mensual	2,00%
Tiempo de diagnóstico inicial incidentes de seguridad Críticos	Tiempo máximo de diagnóstico inicial de incidentes de seguridad catalogados como CRÍTICOS	<= 2 horas	Mensual	1,70%
Tiempo de diagnóstico inicial incidentes de seguridad Altos	Tiempo máximo de diagnóstico inicial de incidentes de seguridad catalogados como ALTOS	<= 3 horas	Mensual	1,25%
Tiempo de diagnóstico inicial incidentes de seguridad Medios	Tiempo máximo de diagnóstico inicial de incidentes de seguridad catalogados como MEDIOS	<= 3 horas	Mensual	0,75%
Tiempo de diagnóstico inicial incidentes de seguridad No Críticos	Tiempo máximo de diagnóstico inicial de incidentes de seguridad catalogados como NO CRÍTICOS	<= 3 horas	Mensual	0,50%
Tiempo de respuesta incidentes de seguridad Muy Críticos	Tiempo máximo de respuesta de incidentes de seguridad catalogados como MUY CRÍTICOS	<= 1 horas	Mensual	2,00%
Tiempo de respuesta incidentes de seguridad Críticos	Tiempo máximo de respuesta de incidentes de seguridad catalogados como CRÍTICOS	<= 3 horas	Mensual	1,70%
Tiempo de respuesta incidentes de seguridad Alto	Tiempo máximo de respuesta de incidentes de seguridad catalogados como ALTO	<= 5 horas	Mensual	1,25%
Tiempo de respuesta incidentes de seguridad Medio	Tiempo máximo de respuesta de incidentes de seguridad catalogados como MEDIO	<= 6 horas	Mensual	0,50%
Tiempo de respuesta incidentes de seguridad No Críticos	Tiempo máximo de respuesta de incidentes de seguridad catalogados como NO CRÏTICOS	<=8 horas	Mensual	0,25%
Tiempo de resolución incidentes de seguridad Muy Críticos	Tiempo máximo de resolución de incidentes de seguridad catalogados como MUY CRÍTICOS	<= 12 horas	Mensual	2,00%
Tiempo de resolución incidentes de seguridad Críticos	Tiempo máximo de resolución de incidentes de seguridad catalogados como CRÍTICOS	<= 8 horas	Mensual	1,70%
Tiempo de resolución incidentes de seguridad Altos	Tiempo máximo de resolución de incidentes de seguridad catalogados como ALTOS	<=16 horas	Mensual	1,25%

Tiempo de resolución incidentes de seguridad Medios	Tiempo máximo de resolución de incidentes de seguridad catalogados como MEDIOS	<=24 horas	Mensual	0,50%
Tiempo de resolución incidentes de seguridad No Críticos	Tiempo máximo de resolución de incidentes de seguridad catalogados como NO CRÍTICOS	<= 32 horas	Mensual	0,25%
Tiempo de registro incidentes de seguridad herramienta de gestión	Tiempo máximo de registro de incidente de seguridad en la herramienta de gestión de incidentes.	<= 1 hora	Mensual	0,25%
Número mínimo de playbooks propuestos /implementado tras incidente de seguridad potencial	Número mínimo de playbooks propuestos/implementado tras incidente de seguridad potencial	>=1	Mensual	0,20%
Tiempo de presentación informe incidentes de seguridad críticos tras resolución	Tiempo máximo de presentación de informe de incidentes de seguridad críticos tras su resolución	<= 1 día	Mensual	0,50%
Indicadores de Solución de anomalías y no conformidades del servicio				
Tiempo máximo de solución de la anomalía o no conformidad del servicio	Tiempo máximo de solución de la anomalía o no conformidad del servicio	<=30 días	Mensual	0,50%
Indicadores de Cadena de Suministro				
Tiempo máximo de entrega del plan de continuidad del servicio y de protección de la cadena de proveedores/suministros	Tiempo máximo de entrega del plan de continuidad del servicio y de protección de la cadena de proveedores /suministros (apartado 5.3.20 del PPT)) desde el inicio de la fase de prestación del servicio	<=30 días	Mensual	0,15%
Indicadores de Informes Técnicos de incidentes de peligrosidad alta o superios				
Tiempo máximo de entrega de informes técnicos de incidentes de peligrosidad crítica o superior	Tiempo de entrega de informes técnicos de incidentes de peligrosidad alta o superior desde que se produjo el incidente	<=10 días	Mensual	0,80%
Indicadores de Informes forenses en situaciones de crisis o ciberataque exitoso				
Número de informes forenses incidente de ciberseguridad que desencadene la activación del Comité de Crisis de ICEX	Número de informes forenses incidente de ciberseguridad que desencadene la activación del Comité de Crisis de ICEX	>=1	Mensual	0,80%
Indicadores de Gestión de Incidentes de Seguridad				
Plazo máximo de comunicación de actividad que pueda suponer un incidente de ciberseguridad a ICEX	Media de tiempo transcurrido desde que se produce la actividad que pueda suponer un incidente de ciberseguridad hasta su comunicación a ICEX (La media se obtiene entre los tiempos de todas las actividades que puedan suponer un incidente de ciberseguridad que se hayan producido al mes)	<=30 min	Mensual	0,30%
Indicadores de guardias				
Tiempo de atención a las llamadas de guardia	% de desviación entre el tiempo de atención a la llamada de guardia indicado en el apartado (según apartado 5.3.9 Medios técnicos del PPT) y el tiempo real de atención a la llamada de guardia	= 0 %	Mensual	2,00%
Tiempo de inicio de resolución a las actuaciones de guardia Tiempo de atención a las llamadas de guardia	% de desviación entre el tiempo de inicio de resolución a la actuación de guardia indicado en el apartado (según apartado 5.3.9 Medios técnicos del PPT) y el tiempo real de inicio de resolución a la actuación de guardia%	= 0%	Mensual	2,00%

	de desviación entre el tiempo de inicio de resolución a la actuación de guardia indicado en el apartado (según apartado 5.3.9 Medios técnicos) y el tiempo real de inicio de resolución a la actuación de guardia% de desviación entre el tiempo de inicio de resolución a la actuación de guardia indicado en el apartado (según apartado5.3.9 Medios técnicos) y el tiempo real de inicio de resolución a la actuación de guardia			

Las penalidades previstas en el presente apartado se impondrán por acuerdo del órgano de contratación de ICEX, adoptado a propuesta del responsable del contrato y mediante el procedimiento interno de ICEX establecido al efecto, que será inmediatamente ejecutivo, y se harán efectivas mediante deducción de los mismos de los importes pendientes de pago o del aval constituido. En caso de ser necesario, por imposibilidad de deducir en una única factura el importe total de las penalizaciones, se descontarán de las facturas sucesivas hasta su completa extinción. La aplicación y el pago de estas penalizaciones no excluyen la indemnización por daños y perjuicios a que hubiere lugar.

NOVENA. - Condiciones Especiales de Ejecución

El CONTRATISTA quedará obligado a realizar las siguientes condiciones especiales de ejecución:

1) Igualdad de género: Toda la documentación o material que se genere con motivo de la ejecución del presente Contrato tanto de uso interno como para difusión exterior deberá realizar un uso no sexista del lenguaje, evitar cualquier imagen discriminatoria de las personas o estereotipos sexistas y fomentar una imagen con valores de igualdad, presencia equilibrada, diversidad, corresponsabilidad y pluralidad de roles e identidades de género.

   A estos efectos, las comunicaciones efectuadas por el CONTRATISTA cumplirán con las indicaciones recogidas en el Decálogo de Leguaje no Sexista de ICEX que se adjuntó a los pliegos de la licitación con referencia 162/2023 como Anexo VII.

2) Sostenibilidad ambiental: Se exigirá que el CONTRATISTA entregue o implemente a partir de la entrada en vigor del presente Contrato, un programa de sostenibilidad o medioambiente aplicado, en particular, a los servicios que presta y, en general, en su propia empresa, que incluya entre sus compromisos: la digitalización de los procesos, el no uso de papel, el reciclaje de material y los desplazamientos sostenibles.

   Este plan de sostenibilidad tendrá que ser entregado por el CONTRATISTA dentro de los 45 días siguientes a la entrada en vigor del presente Contrato y tendrá que ser aprobado por ICEX.

3) Datos de carácter personal. El CONTRATISTA se someterá a la normativa nacional y de la Unión Europea vigente aplicable en materia de protección de datos. El CONTRATISTA deberá acreditar haber proporcionado una formación básica en materia de protección de datos al equipo de trabajo destinado a la prestación del servicio.

   Esta formación será acreditada mediante la remisión de declaraciones al efecto por parte del CONTRATISTA.

Las circunstancias referidas en los apartados anteriores se acreditarán mediante la declaración responsable o entrega de los documentos acordados sin perjuicio de que dicha declaración pueda ser comprobada, y deba ser posteriormente justificada durante la ejecución del Contrato. En caso de incumplimiento, se valorará la imposición de penalidades entre el 1% y el 3% sobre el importe de la garantía constituida en el caso de que tras el procedimiento establecido al efecto se acrediten incumplimientos por el contratista de las condiciones especiales de ejecución recogidas en la

presente cláusula.

DÉCIMA. - Propiedad Intelectual

Pertenecerán a ICEX, de todo el material (incluyendo cualquier tipo de documento, especificaciones, presentaciones, etc.) que sea elaborado por el CONTRATISTA o sus empleados en ejecución del Contrato, en cualquier modalidad y bajo cualquier formato, incluyendo el derecho de uso, reproducción, transformación, distribución, comunicación pública y puesta a disposición a través de Internet, correspondiendo a los autores materiales del mismo únicamente los derechos morales que les reconoce el artículo 14 del texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril. Dichos derechos se ejercerán a nivel mundial, y durante el máximo periodo de protección de los derechos de autor, para todo tipo de soportes, en cualquier formato, e idioma, y con los efectos que las leyes determinen. El CONTRATISTA cede todos los derechos de Propiedad Intelectual que puedan generarse durante la ejecución contractual sobre todos los desarrollos de software que elabore con ocasión de la ejecución de los servicios comprendidos en el ámbito del contrato, incluyendo esta cesión todos los derechos reconocidos por el Real Decreto Legislativo 1/1996. La titularidad del desarrollo afecta no sólo al producto final de la misma, sino al conjunto de trabajos, bocetos, esquemas, documentos previos, diagramas de flujo y, en conjunto, todos y cada uno de los trabajos susceptibles de ser objeto de propiedad intelectual e industrial realizados para el desarrollo.

El CONTRATISTA garantiza que el desarrollo es absolutamente original y que cuenta con la totalidad de los derechos de propiedad intelectual sobre el mismo, por lo que puede garantizar que todo el software y las herramientas utilizadas no vulneran ninguna normativa, contrato, derecho, interés o propiedad de terceros. El CONTRATISTA se compromete, salvo que medie consentimiento expreso de ICEX, a no utilizar el resultado de su labor, ni reproducirlo, trasmitirlo, modificarlo, adaptarlo, cederlo, alquilarlo, prestarlo ni realizar cualquier otra actividad sin autorización de ICEX, y se comprometen a no divulgarlo, publicarlo, ni ponerlo de ninguna otra manera a disposición de terceros. ICEX adquirirá la titularidad de todo el material (incluyendo cualquier tipo de documento, especificaciones, presentaciones, etc.) que sea elaborado por el CONTRATISTA o sus empleados en ejecución del Contrato, en cualquier modalidad y bajo cualquier formato, para todo el mundo, reservándose ICEX cualquier otra facultad aneja a dichos derechos de explotación. Asimismo, el CONTRATISTA defenderá, a su propio coste, cualquier reclamación o amenaza de reclamación formulada por terceros contra ICEX en la medida que dicha reclamación se fundamente en la pretensión de que los trabajos que hubieran sido desarrollados por el CONTRATISTA en el marco del presente Contrato infrinjan derechos de propiedad intelectual o industrial de terceros, o constituyan una apropiación indebida de secretos comerciales o industriales de terceros o derechos de imagen. Toda la documentación elaborada y los resultados obtenidos por el CONTRATISTA en ejecución del contrato serán propiedad de ICEX, en cuyo poder quedarán cuando así sea requerido por ICEX, no pudiendo el CONTRATISTA utilizarla para otras personas o entidades.

El CONTRATISTA responderá del ejercicio pacífico de ICEX en la utilización del software y demás derechos proporcionados por el CONTRATISTA con motivo del contrato y será responsable de toda reclamación que pueda presentar un tercero por estos conceptos contra ICEX y deberá indemnizar a la entidad pública por todos los daños y perjuicios que ésta pueda sufrir por esta causa. En todo caso, las relaciones jurídicas derivadas del presente Contrato se establecen entre ICEX y el CONTRATISTA. ICEX no estará contractualmente vinculada con personas distintas del CONTRATISTA.

UNDÉCIMA. - Protección de datos personales

La realización del objeto del presente Contrato requiere el acceso por el CONTRATISTA a datos personales de los que es responsable ICEX, teniendo el CONTRATISTA la consideración de encargado del tratamiento conforme a lo establecido en los artículos 28 y 29 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD). Teniendo en cuenta la obligación de cumplir con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, de aplicación a todo el sector público y a los sistemas

de información de las entidades del sector privado el CONTRATISTA debe estar en condiciones de tener sus sistemas adaptados a la categoría BÁSICA de la citada normativa. Por tal motivo, y en cumplimiento de las previsiones legales que se contienen en el RGPD, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, las partes formalizan el Contrato de Acceso a datos por cuenta de terceros como Anexo 1.

DUODÉCIMA. - Lugar de prestación del servicio

La prestación de los servicios objeto del presente Contrato se realizará conjuntamente desde las instalaciones de ICEX y del CONTRATISTA, en atención a la naturaleza de la actividad a realizar, a su posible prestación en remoto o, a las tareas encomendadas a la totalidad o a parte de los recursos asignados. Esto es así, debido a las necesidades específicas del servicio y las características técnicas del mismo y la necesidad de una coordinación rápida de los servicios gestionados que permita que los sistemas principales de ICEX funcionen correctamente. Por eso es necesario que la mayor parte del servicio se pueda prestar desde las instalaciones de ICEX, para su mayor agilidad, seguimiento, control y coordinación con los equipos de negocio y de TI de ICEX. Los servicios centrales de ICEX se ubican en Madrid (Paseo de la Castellana, 278), los servicios para la Red Exterior Territorial de ICEX se prestarán asimismo desde las oficinas del Contratista y los servicios centrales de ICEX, no siendo necesario el desplazamiento de personal a las Oficinas de la RET.

DÉCIMOTERCERA. - Responsabilidades del CONTRATISTA

El CONTRATISTA será responsable de la calidad técnica de los trabajos, prestaciones y servicios que realicen en ejecución del presente Contrato, así como de las consecuencias que se deduzcan para ICEX, o para terceros de las omisiones, errores, métodos inadecuados o conclusiones incorrectas en la ejecución del Contrato. El CONTRATISTA responderá y asumirá las correspondientes indemnizaciones por los daños y perjuicios directos e indirectos causados a ICEX o a terceros, que traigan causa en una conducta negligente o culposa del CONTRATISTA o se deriven del incumplimiento de las obligaciones que le incumben, a tenor de lo señalado en el presente Contrato. Concretamente, el CONTRATISTA se responsabilizará:

- De que, tanto el desarrollo como el resultado final de los servicios/trabajos que le sean encomendados, cumplan las especificaciones de calidad que se hayan acordado por ICEX en su caso.
- Del cumplimiento de los plazos, bien sea el plazo total fijado para la realización del Contrato, o los plazos parciales señalados, en su caso, en los Pliegos o los acordados con ICEX en su caso.
- De las omisiones, errores, conclusiones incorrectas o métodos inadecuados que aconseje y lleve a efecto durante la vigencia del presente Contrato.
- Del personal que forme parte del equipo de trabajo destinado al desarrollo y ejecución del Contrato, siendo el único responsable laboral del comportamiento y funcionamiento del mencionado equipo.
- Del tratamiento de la información y de los datos que se pongan a su disposición, en su caso, responsabilizándose asimismo de la pérdida o corrupción de datos que se puedan producir, especialmente cuando se trate de datos de carácter personal.

Sin perjuicio de cualquier otra indemnización que pudiera corresponderle a ICEX, el CONTRATISTA indemnizará a ICEX por las acciones y reclamaciones derivadas de:

- El daño, pérdida o destrucción de cualquier propiedad o información de ICEX, derivados de actos u omisiones dolosas o negligentes del CONTRATISTA.
- Responsabilidades de todo tipo en que incurra ICEX y sean consecuencia directa del incumplimiento por el CONTRATISTA de sus obligaciones.

El CONTRATISTA quedará exonerado de responsabilidad cuando los incumplimientos sean debidos a causas exclusivamente imputables a ICEX y en los casos de fuerza mayor.

DECIMOCUARTA. - Modificación del Contrato

Las partes podrán acordar las modificaciones al presente Contrato que se consideren necesarias para su correcta ejecución, siempre y cuando las mismas no alteren la naturaleza global del contrato inicial ni supongan una modificación sustancial. A estos efectos, se considerará una modificación sustancial aquellas cuyo coste implique una variación del precio del presente Contrato superior al 20%. Las causas de modificación del Contrato podrán ser:

- Aparición de una nueva legislación sobre materia de Tecnologías de la Información y Comunicaciones, que suponga cambios o modificaciones en la infraestructura o los servicios objeto del Contrato.
- Necesidades de evolución tecnológica en el marco del contrato.
- Todas aquellas derivadas de la disminución o aumento de la plantilla de ICEX, integraciones o traslados organizativos de organismos o entidades del ministerio de adscripción, se hayan producido desde la fecha de publicación de los pliegos reguladores de esta licitación hasta la finalización del presente Contrato y que den lugar a la necesidad de modificar el número de líneas.
- Integración de otros organismos, entes o sociedades en ICEX, incluyendo los ahora adscritos a otros departamentos ministeriales en el caso de que supongan una carga de trabajo inasumible y justificada por parte del equipo previsto.
- En caso de que sea necesario incrementar la capacidad del equipamiento hardware y/o software del sistema de gestión de eventos SIEM, la tecnología de análisis de flujos de la red, y las pantallas de monitorización, por incremento del volumen total de eventos de seguridad a recopilar, correlar y almacenar.
- En caso de que para dar cobertura a los servicios objeto del presente Contrato sea necesaria la dedicación de un mayor número de horas de recursos técnicos al estimado inicialmente, derivado de necesidades de incorporación de nuevas fuentes de eventos de seguridad a monitorizar no previstas, del incremento del número de incidentes de seguridad detectados, analizados y tratados, durante el plazo de ejecución del Contrato.
- Cambios tecnológicos, obsolescencia y mejoras tecnológicas de hardware, software, herramientas o sistemas o de la adaptación a metodologías, buenas prácticas o directrices de seguridad.
- Incremento de la carga de trabajo debido a nuevas necesidades técnicas o funcionales del ámbito de este Contrato, no previstas, en el caso de que supongan una carga de trabajo inasumible y justificada por parte del equipo previsto.
- Aparición de una nueva legislación en materia de Tecnologías de la Información y Comunicaciones y Seguridad.

Asimismo, se podrán llevar a cabo modificaciones cuya necesidad derive de circunstancias sobrevenidas e imprevisibles siempre que su coste no implique una variación del precio del Contrato superior al 50%. En todos los casos, el CONTRATISTA proporcionará por escrito, a petición de ICEX, las condiciones técnicas, económicas y de cualquier otra índole, antes de llevar a cabo cualquier modificación al Contrato. La modificación deberá ser aprobada previamente por ICEX y formalizada en la correspondiente adenda al Contrato.

DECIMOQUINTA. - Resolución del Contrato

Son causas expresas de resolución del Contrato, sin carácter exhaustivo, las siguientes:

- El incumplimiento grave de las obligaciones señaladas en el Contrato o en los Pliegos que lo rigen.
- La pérdida sobrevenida de los requisitos exigidos legalmente en la contratación pública.
- La declaración de concurso o la declaración de insolvencia en cualquier otro procedimiento por parte del CONTRATISTA, en los términos dispuestos en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP) y que resulten de aplicación por el Real Decreto Legislativo 1/2020, de 5 de mayo, por el que se aprueba el texto refundido de la Ley Concursal.
- Las establecidas expresamente en los Pliegos o en este Contrato.
- El incumplimiento por el CONTRATISTA de los perfiles profesionales de personal que, en su

caso, se asigne al servicio.
- La sustitución del equipo asignado en un porcentaje superior al permitido por ICEX.
- El desarrollo de los trabajos de acuerdo con un contenido y metodología sustancialmente distintos a los señalados por ICEX.
- Cualquier causa que imposibilite o retrase la realización del servicio o entrega del objeto del Contrato, o implique una disminución de los niveles de calidad exigibles.
- El incumplimiento de las obligaciones establecidas en materia de subcontratación.
- El incumplimiento de la normativa vigente en materia de protección de datos personales, tanto nacional como de la Unión Europea.
- El mutuo acuerdo de las partes.

En los casos de resolución por incumplimiento culpable del CONTRATISTA, le será incautada la garantía aportada por el CONTRISTA y deberá, además, indemnizar a ICEX por los daños y perjuicios ocasionados en lo que excedan del importe de la garantía incautada. La determinación de los daños y perjuicios que deba indemnizar el CONTRATISTA se llevará a cabo por el Órgano de Contratación en decisión motivada previa audiencia del mismo, atendiendo, entre otros factores, al retraso que implique para la realización de los servicios contratados, y a los mayores gastos que el incumplimiento ocasione a ICEX.

DECIMOSEXTA. – Obligaciones de confidencialidad

El CONTRATISTA está obligado a guardar el secreto profesional respecto a la información y documentación proporcionada por ICEX para la realización de los servicios objeto del presente Contrato. El CONTRATISTA únicamente permitirá el acceso de la información confidencial a aquellas personas que tengan necesidad de conocerla para el desarrollo de las actividades y servicios contratados. El CONTRATISTA será responsable del cumplimiento de las obligaciones de confidencialidad del personal a su servicio y de cualesquiera personas o entidades que sean colaboradoras o subcontratadas por ellas. El CONTRATISTA se obliga a no utilizar la información confidencial de ICEX a la que tenga acceso para fines propios o privados o cualesquiera otros fines. Esta obligación subsistirá tanto durante como después de la terminación de las actividades objeto del Contrato, hasta que transcurran cinco (5) años desde su finalización, salvo que dicha información llegue a ser de dominio público o que, por otras causas legítimas, pierda su consideración de confidencial. El incumplimiento de las obligaciones señaladas anteriormente dará derecho a ICEX a exigir las correspondientes responsabilidades de tipo civil e incluso penal a que hubiere lugar. No quedan comprendidas dentro de la obligación de confidencialidad anterior las informaciones recibidas por una de las partes que:

- Sean conocidas anteriormente por la parte receptora pudiendo ésta justificar la anterior posesión de la información.
- Sean de general o público conocimiento.
- Hayan sido recibidas legítimamente de terceros distintos a las Partes, sin que las informaciones estuvieran sometidas a obligación de confidencialidad.
- Hayan sido desarrolladas independientemente por la parte receptora sin haber utilizado total o parcialmente como base información alguna de la otra Parte.
- Su transmisión a terceros hubiera sido aprobada o consentida previamente y por escrito por aquella Parte de la que procede la información.
- Su transmisión sea requerida por cualquier ley o norma aplicable o por requerimiento de cualquier autoridad administrativa legitimada para ello.

DECIMOSÉPTIMA. - Cesión del Contrato

El CONTRATISTA no podrá ceder o traspasar a terceros, sin autorización previa y expresa de ICEX, obligaciones o derechos dimanantes del presente Contrato.

DECIMOCTAVA. - Garantía

La garantía, presentada bajo la modalidad de seguro de caución, constituida por el CONTRATISTA

por importe equivalente al cinco por ciento (5%) del precio máximo del presente Contrato responderá de los siguientes conceptos:

- De la correcta ejecución de las prestaciones contempladas en el presente Contrato.
- Del resarcimiento de las responsabilidades contempladas en la cláusula decimotercera del presente Contrato.
- De los gastos originados a ICEX por demora del CONTRATISTA en el cumplimiento de sus obligaciones.
- De los daños y perjuicios ocasionados a ICEX con motivo de la ejecución del Contrato o por su incumplimiento.
- De los daños y perjuicios ocasionados por la resolución anticipada del Contrato por causas imputables al CONTRATISTA.
- De las penalizaciones impuestas al CONTRATISTA conforme a la cláusula octava anterior.

En caso de que se hagan efectivas sobre la garantía las penalizaciones o indemnizaciones exigibles al CONTRATISTA, éste deberá reponer o ampliar aquélla, en la cuantía en que corresponda, en el plazo de diez (10) días hábiles desde el día siguiente a la ejecución, incurriendo en caso contrario en causa de resolución. Asimismo, cuando, como consecuencia de una modificación del Contrato, su precio experimente variación, deberá reajustarse la garantía, para que guarde la debida proporción con el nuevo precio modificado, en el plazo de diez (10) días hábiles contados desde el día siguiente la fecha en que se notifique al CONTRATISTA el acuerdo de modificación. La garantía no será devuelta o cancelada hasta que se haya cumplido satisfactoriamente el Contrato o hasta que se declare la resolución de éste sin culpa del CONTRATISTA.

DECIMONOVENA. - Subcontratación

El presente Contrato deberá ser ejecutado directamente por el CONTRATISTA. No obstante, éste podrá concertar con terceros la realización parcial de la prestación, salvo los de los siguientes perfiles Jefe/a de Servicio de Oficina de Seguridad y el de Coordinador/a de Seguridad, que, por su naturaleza crítica, deberán ser ejecutadas directamente por el CONTRATISTA. El CONTRATISTA deberá comunicar anticipadamente y por escrito a ICEX la intención de celebrar los subcontratos, señalando la parte de la prestación que se pretende subcontratar y la identidad del subcontratista, y deberá acreditar las condiciones de solvencia técnica o profesional, de los subcontratistas a los que se vaya a encomendar su realización. En todo caso, el CONTRATISTA será responsable directo frente a ICEX por la actuación de la empresa o empresas subcontratadas en todos los ámbitos, incluyendo el relativo a la calidad de los trabajos/servicios, al cumplimiento de plazos de entrega y finalización, a las obligaciones con relación al tratamiento de datos e informaciones, así como del cumplimiento por parte de la empresa subcontratada de sus obligaciones fiscales y laborales que resultaran de aplicación.

VIGÉSIMA. - Legislación aplicable y jurisdicción competente

La legislación aplicable a este Contrato será la española. El presente Contrato tiene carácter mercantil y se regirá por lo dispuesto en el mismo, así como en los Pliegos reguladores de la presente contratación y en la oferta presentada por el CONTRATISTA, que forman todos ellos parte integrante del Contrato en todo aquello en lo que no contradigan a sus propias cláusulas. Subsidiariamente para todo lo no previsto en éste, se atendrán las partes a las disposiciones del Código de Comercio, usos mercantiles y, en su defecto, a lo dispuesto en el Código Civil y demás legislación específica que le sea de aplicación. Las discrepancias sobre la interpretación o ejecución del presente Contrato serán resueltas por mutuo acuerdo. A falta de este, las Partes con renuncia expresa a su propio fuero, si lo hubiere, se someten expresamente a la jurisdicción y competencia de los Juzgados y Tribunales de Madrid capital.

VIGESIMOPRIMERA. - Cumplimiento del Contrato

El Contrato se entenderá cumplido por el CONTRATISTA cuando éste haya realizado, de acuerdo con los términos del mismo y a satisfacción de ICEX, la totalidad de su objeto.

Y para que conste y en prueba de conformidad, firman el presente Contrato en Madrid, en la fecha indicada en la firma, tomándose como fecha de formalización del presente documento la fecha del último firmante.

ICEX España Exportación e Inversiones, E.P.E.	Cipherbit, S.L.U.
	Firmado digitalmente por [redacted] ALFREDO DIEZ (R: B01644558) Fecha: 2024.09.26 11:01:30 +02'00'
Dña. Elisa Carbonell Martín	D. Alfredo Diez Fernandez

Anexos citados:
Anexo 1: Acceso a Datos por cuenta de tercero
Anexo 2: Oferta Técnica
Anexo 3: Oferta Económica y critérios automáticos

ANEXO nº 1
CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCERO

ANTECEDENTES

(i) Que ICEX ha contratado a la empresa CIPHERBIT S.L.U. (en lo sucesivo, el CONTRATISTA) la prestación del servicio de oficina de seguridad digital de los servicios centrales (SSCC) y la red exterior y territorial de ICEX España Exportación e Inversiones, E.P.E. (ICEX), del que este documento forma parte como anexo (en adelante, el Acuerdo). Para ello resulta necesario que el CONTRATISTA efectúe, por cuenta de ICEX, un tratamiento de los datos de carácter personal de las bases de datos titularidad de ICEX.

(ii) Que en virtud del objeto del citado acuerdo suscrito entre las partes, ICEX tendrá la consideración de responsable del tratamiento y el CONTRATISTA tendrá la consideración de encargado del tratamiento conforme a lo establecido en los artículos 28 y siguientes de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD), y en los artículos 28 y 29 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD).

Así pues, las partes convienen en otorgar el presente contrato de acceso a datos por cuenta de tercero (en lo sucesivo, el Contrato), el cual formalizan en el marco del Acuerdo como anexo al mismo y llevan a efecto de acuerdo con las siguientes:

CLÁUSULAS

PRIMERA. - OBJETO. El presente Contrato tiene por objeto regular el acceso y tratamiento de los datos de carácter personal de los ficheros titularidad de ICEX que el CONTRATISTA realizará con ocasión de la prestación del servicio de oficina de seguridad digital de ICEX SSCC y la red exterior y territorial de ICEX. En consecuencia, el tratamiento de datos personales encargado al CONTRATISTA consistirá en recoger, estructurar, conservar, consultar y modificar los datos personales responsabilidad de ICEX. Para la ejecución de los servicios contratados, el CONTRATISTA tratará las siguientes tipologías de datos personales:

- Datos identificativos y de contacto.
- La IP de los equipos, que permite identificar individualmente a usuarios.
- Los logs generados por los usuarios

SEGUNDA. - DEBER DE SECRETO. El CONTRATISTA se compromete a guardar la máxima reserva y secreto sobre la información clasificada como confidencial. Se considerará información confidencial cualquier dato al que el CONTRATISTA acceda en virtud del presente contrato y/o en el Acuerdo a través del cual se regula los servicios a prestar por parte del CONTRATISTA a ICEX, en especial la información y datos propios de ICEX a los que haya accedido o acceda durante la ejecución del mismo. No tendrán el carácter de confidencial todas aquellas informaciones y datos que fueran de dominio público o que estuvieran en posesión del CONTRATISTA con anterioridad a iniciar la prestación de sus servicios y hubieran sido obtenidas por medios lícitos. Esta obligación de confidencialidad subsistirá tanto durante como después de la terminación de las actividades objeto del Acuerdo, hasta que dicha información llegue a ser de dominio público o que, por otras causas legítimas, pierda su consideración de confidencial estableciéndose un periodo máximo de cinco años desde la finalización del Acuerdo o de la prórroga del mismo en su caso, tal y como se establece en la condición 27.2 del Documento de Condiciones Generales de la licitación. De igual manera, el CONTRATISTA será responsable de que su personal, colaboradores, directivos y en general, todas las personas que tengan acceso a la información confidencial y a los ficheros de ICEX, respeten la confidencialidad de la información, así como las obligaciones relativas al tratamiento de datos de carácter personal. Por tanto, EL CONTRATISTA realizará cuantas advertencias y suscribirá cuantos documentos sean necesarios, con dichas personas, con el fin de asegurar el cumplimiento de tales

obligaciones. Las partes reconocen que el CONTRATISTA podrá tener acceso a ficheros que contienen datos de carácter personal, de los que ICEX es responsable, para la prestación del servicio arriba indicado en el marco del Acuerdo, y que este servicio es necesario para el desarrollo de la actividad del CONTRATISTA. No obstante lo anterior, ICEX es, con carácter único, quien decidirá sobre la finalidad, contenido y uso de los ficheros de datos existentes o que puedan ser creados y a los que pueda tener acceso el CONTRATISTA, como resultado de las actividades realizadas por éste.

TERCERA. - OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO. El CONTRATISTA, en su calidad de Encargada del Tratamiento asume las obligaciones siguientes:

- Acceder a los ficheros o bases de datos de carácter personal de ICEX, únicamente, cuando el mismo sea imprescindible para el buen desarrollo de los servicios para los que ha sido contratado.
- Tratar los datos conforme a las instrucciones que reciba de ICEX.
- En caso de que el tratamiento incluya la recogida de datos personales en nombre y por cuenta de ICEX, el CONTRATISTA deberá seguir los procedimientos e instrucciones que reciba de ICEX, especialmente en lo relativo al deber de información y, en su caso, la obtención del consentimiento de los afectados.
- Si el CONTRATISTA considera que alguna de las instrucciones de ICEX infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, informará inmediatamente a ICEX.
- No destinar, aplicar o utilizar los datos personales responsabilidad de ICEX con fin distinto del indicado en el presente contrato o de cualquier otra forma que suponga un incumplimiento de las instrucciones de ICEX.
- Asumir la condición de responsable del tratamiento en caso de que destine los datos a otra finalidad distinta del cumplimiento del objeto del Contrato, los comunique o los utilice incumpliendo las estipulaciones del mismo o las obligaciones de la normativa vigente, respondiendo de las infracciones en que hubiera incurrido personalmente.
- No permitir el acceso a los datos personales responsabilidad de ICEX a ningún empleado de su responsabilidad que no tenga la necesidad de conocerlos para la prestación de los servicios contratados.
- No revelar, transferir, ceder o de otra forma comunicar los datos personales responsabilidad de ICEX, ya sea verbalmente o por escrito, por medios electrónicos, papel o mediante acceso informático, ni siquiera para su conservación, a ningún tercero, salvo que exista autorización o instrucción previa de ICEX.
- En caso de estar obligado a ello por el artículo 30 del RGPD, el CONTRATISTA mantendrá un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de ICEX, que contenga la información exigida por el artículo 30.2 del RGPD.
- Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- Dar apoyo a ICEX en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- Dar apoyo a ICEX en la realización de las consultas previas a la Autoridad de Control, cuando proceda.
- Poner a disposición de ICEX toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen ICEX u otro auditor autorizado por este.
- Adoptar y aplicar las medidas de seguridad estipuladas en el presente Contrato, conforme lo previsto en el artículo 32 del RGPD, que garanticen la seguridad de los datos personales responsabilidad de ICEX y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.
- En caso de estar obligado a ello por el artículo 37.1 del RGPD, designar un delegado de protección de datos y comunicar su identidad y datos de contacto a ICEX, así como cumplir con todo lo dispuesto en los artículos 37, 38 y 39 del RGPD.
- Respetar todas las obligaciones que pudieran corresponderle como encargado del tratamiento con arreglo al RGPD, o de cualquier otra disposición o regulación complementaria

que le fuera igualmente aplicable.

- En caso de que el CONTRATISTA deba transferir o permitir acceso a datos personales responsabilidad de ICEX a un tercero en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará a ICEX de esa exigencia legal de manera previa, salvo que estuviese prohibido por razones de interés público.

CUARTA. - OBLIGACIONES DEL RESPONSABLE DEL FICHERO. ICEX manifiesta y hace constar, a los efectos legales oportunos que:

- Los datos a los que accederá el CONTRATISTA se hallan debidamente legalizados, legitimados y cumplen con todas las prescripciones legales y reglamentarias que exige la normativa vigente en materia de protección de datos.
- Los términos del presente Contrato en nada alteran ni sustituyen las obligaciones y responsabilidades que sean atribuibles a ICEX, como responsable del registro, en virtud de la vigente legislación en materia de protección de datos.

QUINTA. - MEDIDAS DE SEGURIDAD Y VIOLACIÓN DE LA SEGURIDAD. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el CONTRATISTA aplicará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- La seudonimización y el cifrado de datos personales.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, así como la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
- Un catálogo de medidas de seguridad reconocido en normativas o estándares de seguridad de la información, tales como el Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad), el estándar internacional ISO/IEC 29151:2017, o el estándar internacional ISO/IEC 27002:2013.

Al evaluar la adecuación del nivel de seguridad, el CONTRATISTA tendrá en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. el CONTRATISTA permitirá y contribuirá a la realización de auditorías, incluidas inspecciones, por parte de ICEX o de otro auditor autorizado por el mismo. Asimismo, en caso de modificación de la normativa vigente en materia de protección de datos o de otra normativa relacionada y que resultase aplicable al tratamiento objeto del presente Contrato, el CONTRATISTA garantiza la implantación y mantenimiento de cualesquiera otras medidas de seguridad que le fueran exigibles, sin que ello suponga una modificación de los términos del presente Contrato. En caso de violación de la seguridad de los datos personales en los sistemas de información utilizados por el CONTRATISTA para la prestación de los servicios objeto del Acuerdo y regulado bajo el presente Contrato, el CONTRATISTA deberá notificar a ICEX, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas hábiles, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia conforme a lo dispuesto en el artículo 33.3 del RGPD. En tal caso, corresponderá a ICEX comunicar las violaciones de seguridad de los datos a la Autoridad de Protección de Datos y/o a los interesados conforme a lo establecido en la normativa vigente.

SEXTA. - DESTINO DE LOS DATOS AL FINALIZAR LA RELACIÓN CONTRACTUAL. Una vez cumplida o resuelta la prestación contractual acordada entre ICEX y el CONTRATISTA a través del Acuerdo, y que justifica el acceso a los datos personales respecto de los cuales es responsable ICEX, los datos personales serán destruidos o devueltos a ICEX, al igual que cualquier soporte o

documentos en que conste algún dato de carácter personal objeto del tratamiento. La destrucción no procederá en el caso de que una previsión legal exija la conservación de los datos, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación. En cualquier caso, los datos permanecerán convenientemente bloqueados.

SÉPTIMA. - EJERCICIO DE DERECHOS. Si los afectados ejercitan sus derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de los datos y a no ser objeto de decisiones individualizadas automatizadas ante el CONTRATISTA y solicitan el ejercicio de tales derechos ante la misma, el CONTRATISTA deberá dar traslado de la mencionada solicitud, en el plazo máximo de tres (3) días, a ICEX a fin de que por el mismo se resuelva, en los plazos establecidos por la normativa vigente. Asimismo, el CONTRATISTA deberá tramitar cualquier instrucción relativa a los derechos que reciba a través de ICEX, a la mayor celeridad posible, y siempre dentro del plazo máximo de dos (2) días hábiles a contar desde la recepción de la solicitud, confirmando por escrito tanto la recepción de la solicitud como la ejecución de la tarea encomendada. Estas comunicaciones serán remitidas al buzón del delegado de protección de datos de ICEX (delegadoprotecciondatos@icex.es)

OCTAVA. - DEBER DE INFORMACIÓN MUTUO. Las partes se informan mutuamente de que los datos de las personas de contacto que figuran en el encabezamiento del Acuerdo, así como los datos personales de cualquier empleado que se proporcionen entre sí como consecuencia de la relación negocial objeto del citado acuerdo serán incorporados a los registros de actividad de tratamiento titularidad de cada una de las partes con la finalidad de gestionar dicha relación. La base jurídica que legitima el tratamiento de los datos de los interesados es la necesidad para la celebración y ejecución del Acuerdo. Los datos serán conservados durante la vigencia del Acuerdo y, posteriormente, durante el plazo legal necesario con la finalidad de atender a las posibles responsabilidades derivadas de la relación contractual. En todo caso, los afectados podrán ejercer sus derechos de acceso, rectificación, cancelación/supresión, oposición, limitación y portabilidad ante la parte que corresponda a través de comunicación por escrito al domicilio social que consta al comienzo del presente documento o al buzón del delegado de protección de datos de ICEX (delegadoprotecciondatos@icex.es), aportando fotocopia de su DNI o documento equivalente e identificando el derecho que se solicita. Asimismo, en caso de considerar vulnerado su derecho a la protección de datos personales, podrán interponer una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es).

NOVENA. - CONFIDENCIALIDAD. La totalidad de los términos y condiciones del presente documento tienen carácter confidencial, estando sujetos a las obligaciones expuestas a lo largo del mismo y del Acuerdo del que trae causa.

DÉCIMA. - SUBCONTRATACIÓN. El CONTRATISTA no podrá subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato y que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios. Sin perjuicio de lo anterior, en caso de que el CONTRATISTA necesitara subcontratar todo o parte de los servicios contratados por ICEX en los que intervenga el tratamiento de datos personales, deberá comunicarlo previamente y por escrito a ICEX, con una antelación de 1 mes, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si ICEX no manifiesta su oposición en el plazo establecido. En este último caso, el subencargado, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para EL CONTRATISTA y las instrucciones que dicte ICEX. Corresponde al CONTRATISTA exigir por contrato al subencargado el cumplimiento de las mismas obligaciones asumidas por él a través del presente documento. El CONTRATISTA seguirá siendo plenamente responsable ante ICEX en lo referente al cumplimiento de las obligaciones. El CONTRATISTA está obligado a informar a ICEX de cualquier cambio en la incorporación o sustitución de otros subencargados con una antelación de un (1) mes, dando así a ICEX la oportunidad de oponerse a dichos cambios.

UNDÉCIMA. - RESPONSABILIDAD. El CONTRATISTA se compromete a cumplir con las

obligaciones establecidas en el presente Contrato y en la normativa vigente, en relación con el presente encargo de tratamiento. El CONTRATISTA será considerado responsable del tratamiento en el caso de que destine los datos a otras finalidades, los comunique o los utilice incumpliendo las estipulaciones del presente Contrato, respondiendo de las infracciones en que hubiera incurrido personalmente.

DUODÉCIMA. - UBICACIÓN DE LOS SERVIDORES Y DE LOS SERVICIOS ASOCIADOS AL MISMO. De conformidad con lo señalado en el Real Decreto-ley 14/2019, de 31 de octubre, el CONTRATISTA declara que los servidores en los que se alojarán los datos personales de ICEX objeto de tratamiento están ubicados en los propios de ICEX para la prestación del servicio.

---

y que la ubicación desde dónde se van a prestar los servicios asociados a los mismos es en las instalaciones del ICEX en Madrid y en su caso y previa autorización de ICEX, en las instalaciones principales de CIPHERBIT ubicadas en C/ Marie Curie, 17-19 28521, Rivas-Vaciamadrid, España, y/o cualquier otra ubicación del ICEX, CIPHERBIT o Terceros que se acuerde por las partes.

El CONTRATISTA se obliga a comunicar durante la vigencia del contrato, cualquier cambio que se produzca de la información facilitada en esta cláusula.

Anexo 2: Oferta Técnica
Anexo 3: Oferta Económica y de Criterios Automáticos

ANEXO II. MODELO DE PRESENTACION DEL PROYECTO TECNICO
LOTE 2

(A incluir en el sobre nº 2)

DATOS DE IDENTIFICACIÓN DEL EXPEDIENTE

Expediente nº: 162/2023
Objeto: Suministro, administración, gestión y operación de la infraestructura tecnológica de ICEX y de la Red Exterior y Territorial:
- Lote 2: Servicio de Oficina de Seguridad Digital de ICEX Servicios Centrales y la Red Exterior y Territorial.

Presupuesto base de licitación: 4.159.883,20 €, IVA incluido.

DATOS DE IDENTIFICACIÓN DEL FIRMANTE DE LA PROPOSICIÓN Y DEL LICITADOR

Apellidos y nombre del firmante de la proposición: DIEZ FERNANDEZ, ALFREDO
Relación que une al firmante con el licitador[1]: Representante legal, (Apoderado)
Razón Social del Licitador: CIPHERBIT, S.L.U.
NIF del licitador: B01644558
Domicilio del licitador Calle Marie Curie, 19, Rivas Vaciamadrid, 28521
Teléfono [redacted]

DATOS DE LA DIRECCIÓN DE CORREO HABILITADA PARA RECIBIR NOTIFICACIONES ELECTRÓNICAS:

concursos@oesia.com

PROPOSICIÓN TÉCNICA

El abajo firmante, en virtud de la representación que ostenta presenta Proyecto Técnico para la licitación convocada por ICEX para la contratación del servicio Oficina de Seguridad Digital de ICEX Servicios Centrales y la Red Exterior y Territorial (Lote 2).

De acuerdo con las condiciones contenidas en los pliegos que rigen esta licitación, aceptando expresamente el contenido de los mismos y se compromete, caso de resultar adjudicatario, a tomar a su cargo la realización de los servicios relativos a esta licitación, ofertando las condiciones técnicas especificadas en el caso práctico que acompaña al presente Anexo II** siendo las mismas vinculantes para la ejecucion de los servicios objeto de este lote:

[1] A cumplimentar por el licitador: "Apoderado, Gerente o Administrador". Si el licitador actúa en su propio nombre, dejará en blanco este apartado

* La empresa licitante declara expresamente conocer y aceptar los formatos requeridos por ICEX para la presentación de su proyecto técnico. Cualquier desviación u omisión de los datos y formatos solicitados podrá suponer la desestimación automática de toda la proposición.

* La empresa licitante declara expresamente conocer y aceptar los formatos requeridos por ICEX para

La oferta técnica deberá contemplar específicamente los siguientes apartados:

- **Caso Práctico:** Se valorará un caso práctico para la gestión de un incidente de ciberseguridad relacionado con una posible alerta de una cuenta comprometida de un usuario, tal como se indica en los apartados *5.2 Requisitos técnicos del servicio, 5.3 Requisitos de Ejecución del Servicio y 5.4 Medios Personales, respectivamente,* del Pliego de Prescripciones Técnicas.

En Rivas Vaciamadrid, a fecha firma.

Fdo.: D. ALFREDO DIEZ FERNANDEZ
APODERADO

IMPORTANTE
NOTAS PARA LA PRESENTACION DE LA OFERTA TÉCNICA:

- La oferta técnica tendrá una extensión máxima de 15 páginas incluyendo la portada e índice, con margen superior e inferior de 2,5 cm e izquierdo y derecho de 3 cm, redactadas con tipo de letra Arial, salto de 6 puntos entre párrafos, tamaño 11 puntos e interlineado de 1,5 y no podrán incluirse otros anexos diferentes a los citados en el pliego.
- Las ofertas que se excedan de esta extensión no respeten este formato, o que no incluyan todos los apartados dentro del proyecto tal y como se solicita en los apartados anteriores podrán ser excluidas. Cualquier propuesta que supere el límite de páginas indicado, incluyendo portada e índice, no será objeto de valoración el contenido del exceso.
- En ningún caso la oferta técnica podrá tener contenido económico ni ninguna información que permita deducir la puntuación de los criterios valorables de forma automática.

---

la presentación de su proyecto técnico. Cualquier desviación u omisión de los datos y formatos solicitados podrá suponer la desestimación automática de toda la proposición.

CIPHERBIT – SOLUCIÓN CASO PRÁCTICO LOTE 2

Adjunto ANEXO II. MODELO DE PRESENTACION DEL PROYECTO TECNICO LOTE2

ÍNDICE

1 Solución al Caso Práctico

CONTEXTO: se recibe una alerta de una cuenta comprometida de un usuario que puede derivar en un posible incidente de seguridad.

METODOLOGÍA PROPUESTA: para los procesos de gestión de incidentes, CIPHERBIT propone utilizar un nuestro modelo de desarrollo interno, Ciberseguridad 360º, basado en las siguientes guías y recomendaciones de autoridades relevantes, contemplando asimismo las particularidades del contexto ICEX (en base a la información disponible en los pliegos):

- *GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES del Consejo Nacional de Ciberseguridad Guia-Nacional-de-Notificacion-y-Gestion-de-Ciberincidentes.pdf (interior.gob.es)*
- *Guía de Seguridad de las TIC CCN-STIC 817_ ENS Gestión de ciberincidentes file (cni.es)*
- *Guía de GESTIÓN DE CIBERCRISIS: BUENAS PRÁCTICAS EN LA GESTIÓN DE CRISIS DE CIBERSEGURIDAD_CCN CERT file (cni.es)*
- *ITIL V4 Gestión de Servicios de TI*

Para ello se propone la respuesta al caso práctico en un ciclo completo de gestión de incidentes estructurado en cuatro fases (*1.Preparación 2.Identificación. 3.Contención, Mitigación y Recuperación 4.Actividades Post-incidente*)

ORGANIZACIÓN DEL EQUIPO DE TRABAJO: se describen a continuación (en base a la información disponible en el PPT) los equipos/perfiles involucrados para la gestión del incidente

- **CIPHERBIT:** *Coordinador de Seguridad (Lote 2), Analista de Seguridad (Lote 2), Servicio de Gestión de incidentes de Ciberseguridad (Lote 2), Servicio Repuesta a incidentes de Ciberseguridad - CSIRT (Lote 2) y Oficina de Seguridad Digital (Lote 2).*
- **ICEX/TERCEROS:** *Servicio de Comunicaciones (Lote 1), Servicios de Monitorización, Operación y Soporte (Lote 1), Servicio explotación de sistemas (Lote 1), Coordinador de Servicio (Lote 1), Jefe de Servicio de la Oficina de Gestión y Transformación (Lote 3), Gestor/es Técnico/s ICEX, Comité de Seguridad (Áreas de Calidad y Procesos y Asesoría Jurídica), Comité Operativo y Otros responsables del servicio, seguridad y/o que se determinen.*

MATRIZ PROPUESTA DE ROLES Y RESPONSABILIDADES **X:** Responsables de realizar alguna gestión del proceso **I:** Informados **C**: Consultados	Equipo CIPHERBIT					Equipos ICEX/TERCEROS										
	Oficina de Seguridad Digital	Coordinador de Seguridad	Analista de Seguridad	Servicio de Gestión de incidentes	Servicio de Respuesta CSIRT	Servicio Comunicaciones (Lote1)	Servicio Monitorización, (Lote 1)	Servicio explotación (Lote 1)	Coordinador de servicio (Lote 1)	Jefe Oficina (Lote 3)	Gestor/es técnico/s ICEX	Comité de Seguridad	Comité Operativo	Área de Calidad y Procesos	Asesoría Jurídica	ICEX (otros responsable seg/serv)
IDENTIFICACIÓN																
A. Detección, Categorización y Registro		X	X	I						I	I					
B. Solicitud de información adicional y diagnostico		X		X	I	X	X		I	I	C					I
CONTENCIÓN, MITIGACIÓN Y RECUPERACIÓN																
C. Medidas de contención		X			X			X	I	I	C					I
D. Medidas de Mitigación, Remediación y Notificación		X			X			X	I	I	C	C		X	X	I
E. Medidas Recuperación y vuelta a la normalidad		X	X		X			X	I	I	C	C				I
POST-INCIDENTE																
F. Análisis final e informe	X	X	C	C	C				I	I	I	I	I			I
G. Lecciones aprendidas	X	X	C	C	C				C	C	C	C	C	C		C

Fase 1. Preparación

OBJETIVOS: La fase de Preparación contempla todas las acciones de *prevención, anticipación y preparación* para la orquestación de la respuesta de incidentes. Si bien esta fase *no es objeto de desarrollo para la respuesta al caso práctico,* destacar sus principales características, a ejecutar por parte del equipo CIPHERBIT con el soporte y directrices del ICEX al inicio del servicio: *Designación y organización de los Equipo de Gestión y Respue sta a Inci dentes y otras par tes involucradas . Desarrollo de los*

procedimientos de respuesta ante incidentes, flujogramas de escalado, comunicación y notificación de incidentes de a autoridades y terceros. Puesta a punto de Recursos, Mecanismos y Herramientas necesarias. Formación, Capacitación de los Equipos y ejercicios de Simulación de Incidentes. Mantenimiento, Revisión y Actualización Periódica.

Fase 2. Identificación

OBJETIVOS: En la fase de identificación, desde el mismo momento que se detecta la alerta, el equipo de respuesta llevará a cabo un análisis para verificar, con la información disponible, si es posible confirmará que no se trata de un falso positivo y comenzará con las tareas de análisis, categorización, registro y escalado del incidente, buscando conocer la naturaleza, impacto potencial, activos afectados y causa.

A. Detección, Categorización y Registro	
Tareas	**Subtareas**
1. Detección de alerta en el SIEM	• El analista de Seguridad (Lote 2) realizará un análisis preliminar con los datos proporcionados en la alerta. • Se descartarán falsos positivos tras la comprobación de actividad sospechosa.
2. Categorización de la alerta	• Tras el análisis preliminar se categorizará la alerta como posible incidente de nivel ALTO.
3. Comunicación al ICEX	• En analista informará al coordinador de seguridad (Lote 2) para que notifique al Gestor Técnico del ICEX y, en su caso, al Jefe de Servicio de la Oficina de Gestión y Transformación (Lote 3), informando que se está investigando un posible incidente de seguridad.
4. Registro y escalado en la herramienta de gestión de incidentes.	• El analista registrará y escalará el posible incidente en la herramienta de gestión de incidentes con los primeros datos, para su evaluación por parte del "Servicio de Gestión de incidentes de Ciberseguridad (Lote 2)"

Ficha Registro de incidente	
1	***Código/ID del incidente**: Automático, generado por la herramienta*
2	***Responsable Registro:** Identificación Analista de Seguridad (Lote 2)*
3	**Fuentes de detección**: *Microsoft Office 365*
4	**Sistemas de Información, IPs/Dominios:** *Cuenta de correo afectada: xx@icex.com*

	IP de conexión: xx.xx.xx.xx *Lugar de conexión: xx* *Dispositivo que realiza la conexión: xx (no corporativo)*
4	**Análisis preliminar** *"Se ha detectado una alerta sobre inicios de sesión irregulares de la cuenta de correo electrónico del usuario X"*
5	**Clasificación preliminar y justificación***: Incidente ALTO: En base a la información disponible y a los ANS del apartado 5.6 del PPT, en concreto, a la matriz de tipología de incidentes, se catalogará el presente incidente en la categoría de "Acceso no autorizado a información en el que confirma capacidad para exfiltrar, o dañar información clasificada como RESTRINGIDA" para el que se estipula el nivel ALTO. Dicha categoría también se encuentra alineada a las recomendaciones del CCN e INCIBE con respecto a incidentes vinculados al "compromiso de cuentas de correo", salvo situaciones especiales (por ejemplo, pueda derivarse impacto legal o reputacional muy alto por la categoría de profesional y/o información tratada en dicha cuenta, descartada en el presente supuesto)*
6	**Hipótesis.** *Compromiso de credenciales*
	Riesgos y posible impacto. *Acceso no autorizado a información de uso interno y/o* *Restringido (Información que únicamente debería estar accesible para determinado personal del ICEX), potencial impacto en seguridad, legal y reputación.*
7	**Información relativa al ámbito de las comunicaciones.** *Se indicarán las IPs, dominios y cuentas de correo involucradas.*
8	**Análisis de las IP/Dominios implicados.** *En el caso de llevar a cabo un análisis preliminar y que no se detectasen IP/Dominios catalogados como maliciosos, quedará pendiente de confirmación por el servicio de vigilancia digital.*
9	**Relaciones.** *Pendiente de determinar relaciones con incidentes previos.*
10	**Roles y equipos a notificar:** *Servicio de Gestión de incidentes de Ciberseguridad (Lote 2)*
11	**Nivel Prioridad.** *ALTO (Reevaluación por análisis Nivel 2)*
12	**Prescripciones preliminares.** *Bloqueo de la cuenta y cambio de contraseña.*

Recursos involucrados en la GESTIÓN y resultados del proceso	
Organización del equipo CIPHERBIT	• Analista de Seguridad (Lote 2) • Coordinador de Seguridad (Lote 2)

Necesidades equipos ICEX y/o terceros	N/A
Registros solicitados y revisados	N/A
Tiempo /ANS del proceso	• Comunicación a ICEX (por parte del Coordinador (Lote 2) y Jefe de Servicio de la Oficina de Gestión y Transformación (Lote 3) de actividad sospechosa (correo electrónico y/o Telf.): < 30 minutos • Registro en la Plataforma de Gestión de Incidentes (por parte del Analista): < 1 hora
Salida del proceso	• Escalado de la alerta al "Servicio de Gestión de incidentes de Ciberseguridad (Lote 2)" como posible incidente.

B. Solicitud de información adicional para evaluación en detalle del incidente, diagnóstico final y determinar la estrategia de respuesta	
Tareas	**Subtareas**
1. Revisión de la actividad de la cuenta de correo del usuario afectado.	• Solicitar al servicio de protección del correo o logs de inicio de sesión en Office 365 del usuario afectado: *Revisión de los logs. Se confirman varios accesos no autorizados.* o los logs del servicio SaaS de filtrado Antispam y gestión de cuarentena del usuario afectado: *Revisión de los logs. Se observan correos enviados a direcciones desconocidas.* o correos enviados desde la cuenta del usuario afectado al servicio SaaS de filtrado Antispam y gestión de cuarentena: *Revisión de los correos. Se confirma exfiltración de información por correo electrónico.*
2. Revisión de actividad adicional del usuario afectado	• Solicitar al Servicio de Comunicaciones los logs de inicio de sesión y actividad en la VPN corporativa: *Revisión de los logs. No se detecta actividad sospechosa.* • Solicitar al servicio de protección de aplicaciones (WAF/DAM) los logs de actividad en las aplicaciones corporativas que están accesibles desde internet. *Revisión de los logs. No se detecta actividad sospechosa.*

3. Revisión de los dispositivos del usuario afectado	• Solicitar al servicio de protección del dispositivo final los logs, eventos, telemetría y detecciones ocurridas en el equipo final y en el dispositivo móvil a través del EDR y del MDM: *Revisión de los logs, eventos, telemetría y detecciones. No se detecta evidencia de que algún dispositivo haya sido comprometido.*
4. Realizar un análisis del tráfico de red	• Solicitar a los Servicios de Monitorización, Operación y Soporte los logs del tráfico de red: r*evisión de logs, e ventos, tel emetría y detecciones. No se detecta actividad sospechosa.*
5. Vigilancia digital	• Solicitar al servicio de Vigilancia Digital: a*nálisis reputacional de las IPs, dominios y cuentas de correo que intervienen en el incidente. Búsqueda de evidencias de filtración de credenciales corporativas en Deep o da rk web. Búsqueda de la información filtrada en foros o webs de venta.*
6. Actualización de la información del incidente en la herramienta de gestión de incidentes	• Actualizar Ficha Registro de incidente con la confirmación de categorización ALTO. • Registrar nueva información indicando que se detecta exfiltración de información, registrar datos de la información exfiltrada, cuentas de correo a las que se ha exfiltrado y peticiones subsidiarias que se han abierto solicitando registros.
7. Informar y actualizar estado al ICEX	• Notificar por parte del Coordinador de Seguridad (Lote 2) al ICEX de los avances en la investigación del incidente, para la consulta y toma de decisiones de próximos pasos con el soporte del Coordinador de Seguridad (Lote 2). • Involucración en esta fase al Coordinador de servicio (Lote 1) dentro del ciclo de parte interesada a informar, como responsable de los equipos de gestión Lote 1 a su cargo, así como otros Responsables que determine el ICEX.
8. Escalado	• Escalar el incidente, por parte del "Servicio de Gestión de incidentes de Ciberseguridad (Lote 2)" al "Servicio de respuesta ante incidentes – CSIRT (Lote 2)".
Recursos involucrados en la GESTIÓN y resultados del proceso	
Organización	• Servicio de Gestión de incidentes de Ciberseguridad (Lote 2). • Coordinador de Seguridad (Lote 2).

del equipo CIPHERBIT	
Necesidades equipos ICEX y/o terceros	• Servicio de Comunicaciones (Lote 1). • Servicios de Monitorización, Operación y Soporte (Lote 1).
Registros solicitados y revisados	• Logs de inicio de sesión en Office 365 (Lote 2). • Logs del servicio SaaS de filtrado Antispam y gestión de cuarentena (Lote 2). • Correos enviados desde la cuenta del usuario (Lote 2). • Logs de inicio de sesión y actividad VPN corporativa (Lote 1). • Logs de actividad en las aplicaciones corporativas que están accesibles desde internet (Lote 2). • Logs, eventos, telemetría y detecciones ocurridas en el equipo final y en el dispositivo móvil a través del EDR y del MDM (Lote 2). • Logs del tráfico de red (Lote 1).
Tiempo /ANS del proceso	• Tiempo de diagnóstico final del incidente categorizado Alto: < 3 horas.

Salida del proceso	• Peticiones en el Sistema de Gestión de Incidencias y Peticiones (Gestión de Tickets).
	• Actualización del Registro de Incidentes y actualización de estado a ICEX y partes interesadas.
	• Escalado al “Servicio de respuesta ante incidentes – CSIRT (Lote 2)” para determinar las medidas de tratamiento.
	• Creación de 2 grupos/equipos de seguimiento, ambos liderados y coordinados por el Coordinador de seguridad (Lote 2):
	  ○ Grupo técnico con las diferentes áreas involucradas en la respuesta al incidente para compartir información de interés del incidente y trabajar en las tareas de contención, mitigación y recuperación de los servicios.
	  ○ Grupo ejecutivo en el que se comunicará el estado del incidente con los altos cargos, el grado de avance y se trataran las acciones necesarias para la comunicación interna y externa, si procede.

Fase 3. Contención, mitigación y recuperación

OBJETIVOS: Tratamiento del Incidente, desde el mismo momento que se confirme la materialización del incidente, la principal prioridad de respuesta consistirá en contener el incidente con la mayor brevedad posible con el objetivo de limitar el daño que éste pueda causar y prevenir la extensión del impacto. Inmediatamente a continuación (o paralelamente si es posible) se trabajará en la remediación y vuelta a la normalidad. Para la respuesta se usarán como norma general los playbooks/runbooks definidos previamente y se mantendrá en todo momento una comunicación fluida con los equipos del ICEX y terceros, para realizar una respuesta ágil, teniendo además en consideración la necesidad/idoneidad de notificación a autoridades u otras partes interesadas.

C. Medidas de contención	
Tareas	**Subtareas**
1. Deshabilitar la cuenta comprometida.	• Solicitar y proceder a la deshabilitación temporal de la cuenta de correo comprometida para prevenir el acceso no autorizado. • Solicitar y proceder a la deshabilitación temporal de otras cuentas corporativas asociadas al usuario.
2. Revocación de Sesiones Activas	• Solicitar y proceder al cierre de todas las sesiones activas de la cuenta comprometida, si existiesen, para prevenir un acceso continuo no autorizado.
3. Cambio de credenciales	• Solicitar y proceder al cambio de contraseña de la cuenta de correo electrónico. • Solicitar y proceder el cambio de contraseña en el resto de servicio y/o aplicaciones en las que, el usuario utilice el mismo nombre de usuario, pero no son SSO (Single Sign-On).
Recursos involucrados en la GESTIÓN y resultados del proceso	
Organización del equipo CIPHERBIT	• Servicio de respuesta a incidentes de ciberseguridad – CSIRT (Lote 2). • Coordinador de Seguridad (Lote 2).
Necesidades equipos ICEX y/o terceros	• Servicio explotación de Sistemas (Lote 1): o Deshabilitación de las cuentas del usuario afectado. o Gestión cambio de credenciales.
Registros solicitados y revisados	• Evidencia de cambio contraseña, cierres de sesiones y deshabilitación cuentas (Lote 1).
Tiempo /ANS	• Tiempo de respuesta incidente de seguridad Alto: < 5 horas

del proceso	
Salida del proceso	• Peticiones en el Sistema de Gestión de Incidencias y Peticiones (Gestión de Tickets). • Actualización del Registro de Incidentes y actualización de estado a ICEX y partes interesadas. • Prescripción y aplicación de medidas de contención y continuación de la fase de tratamiento con la determinación de medidas de mitigación y recuperación.

D. Medidas de Mitigación, Remediación y Notificación	
Tareas	**Subtareas**
1. Aislamiento de la amenaza	• Solicitar la custodia y cuarentena preventiva de los dispositivos asociados con la cuenta del usuario afectado (en determinados casos, por la ubicación del usuario u horario de realización de esta fase, no se podrá disponer de los los dispositivos hasta más adelante) y proceder con: o Aislamiento del equipo portátil y el dispositivo móvil del usuario de la red para evitar una posible comunicación con sistemas no autorizados. o Análisis forense informático para recopilar y analizar registros de eventos y la integridad de los archivos del sistema en busca de malware o software malicioso. • Solicitar y proceder al bloqueo de las direcciones IP maliciosas o rangos de direcciones asociados con la amenaza en los firewalls y sistemas de detección de intrusiones • Solicitar y proceder al bloqueo de los destinatarios de los correos filtrados en el servicio de protección del correo.
2. Implementación de Medidas de Control Adicionales	• Solicitar y proceder la actualización de las políticas de seguridad, incluyendo las políticas de acceso y autenticación y la política de contraseñas. • Solicitar y proceder a la implementación de restricciones adicionales de acceso y autenticación, como la autenticación multifactor (MFA). • Solicitar y proceder a la creación una política para que la cuenta del usuario afectado no pueda iniciar sesión en ninguna ubicación geográfica que no sea España y/o autorizada.

	• Solicitar y proceder a la aplicación de parches de seguridad disponibles para los sistemas y aplicaciones afectados. • Solicitar y proceder a la realización de escaneos de vulnerabilidades para identificar posibles puntos débiles en la infraestructura de TI y aplicar medidas correctivas.
3. Monitorización Continua y Respuesta Inmediata	• Solicitar y proceder a la configuración los sistemas de monitoreo de seguridad para detectar actividades maliciosas en tiempo real en base a los nuevos IOC e indicadores de ataque obtenidos, definiendo nuevos casos de uso en base al patrón del ataque del incidente y de los indicadores obtenidos, configurando alertas automáticas.
4. Valoración de impacto normativo y necesidad de notificación a autoridades	• Se solicitará colaboración del Comité de Seguridad, en concreto: o Se solicitará y prestará soporte al área de Asesoría Jurídica en la determinación de posible vulneración del RGPD/LOPDGDD por exfiltración de datos personales y, en su caso, necesidad de notificar a la AEPD. o Se solicitará y prestará soporte al área de Calidad y Procesos en la determinación de la necesidad de notificación del incidente al CCN en cumplimiento del ENS. o Se determinará en conjunto que no se han materializado las condiciones que determinan la obligatoriedad de notificación del incidente a las autoridades.
Recursos involucrados en la GESTIÓN y resultados del proceso	
Organización del equipo CIPHERBIT	• Servicio de respuesta ante incidentes de ciberseguridad – CSIRT (Lote 2): o Aislamiento de endpoints, escaneos de vulnerabilidades, introducción de IOC/IOA, alertas automáticas y casos de uso.
Necesidades equipos ICEX y/o terceros	• Servicio explotación de sistemas (Lote 1): o Bloqueo de comunicaciones e introducción de IOC/IOA. o Aplicación de parches. • Comité de Seguridad (Calidad y Procesos, Asesoría Jurídica).
Registros solicitados y revisados	• Evidencia de aislamiento de los equipos del usuario (Lote 1). • Evidencia de bloqueo de las direcciones IP o rangos de direcciones maliciosas (Lote 1). • Evidencia del bloqueo de los destinatarios de los correos filtrados

	(Lote 1). • Evidencia de la actualización de las políticas de seguridad, incluyendo las políticas de acceso y autenticación, MFA y la política de contraseñas (Lote 1). • Evidencia de la creación de una política para que la cuenta del usuario no pueda iniciar sesión según su ubicación geográfica (Lote 1).
Tiempo /ANS del proceso	• Tiempo de respuesta incidentes de seguridad Alto < 5 horas.
Salida del proceso	• Peticiones en el Sistema de Gestión de Incidencias y Peticiones (Gestión de Tickets). • Actualización del Registro de Incidentes y actualización de estado a ICEX y partes interesadas. • Prescripción y aplicación de medidas de mitigación y remediación y, continuación de la fase de tratamiento con la determinación de medidas de recuperación.

E. Medidas Recuperación y vuelta a la normalidad	
Tareas	**Subtareas**
1. Restauración de Servicios y comprobación de eliminación del riesgo	• Seguimiento y verificación de que las medidas implantadas han conseguido erradicar el daño y asegurar que el incidente no se reproduce. • Se restaurará la cuenta de correo electrónico desde una copia de seguridad reciente o desde el punto en el que se detectó el compromiso. Así como el resto de los servicios deshabilitados de forma segura. • El analista de seguridad verifica que la cuenta y servicios restaurados esté funcionando correctamente y que no hay rastros de actividad maliciosa. Se confirmará el cierre de todos los tickets y peticiones de servicio. Se actualizará la Ficha de Registro de incidentes para proceder a su cierre. Se confirmará que el incidente está controlado y la vuelta a la normalidad.
2. Notificación de cierre del incidente a partes interesadas	• Se informará al ICEX y a todas las partes interesadas de las acciones de tratamiento llevadas a cabo, la confirmación de resolución del mismo y la puesta en marcha del Informe detallado del Incidente para su posterior revisión.

Recursos involucrados en la GESTIÓN y resultados del proceso	
Organización del equipo CIPHERBIT	• Servicio de respuesta ante incidentes de ciberseguridad – CSIRT (Lote 2). • Coordinador de Seguridad (Lote 2). • Analista de Seguridad (Lote 2).
Necesidades equipos ICEX y/o terceros	• Servicio explotación de sistemas (Lote 1): o Administrador dominio. • Comité de Seguridad (Calidad y Procesos, Asesoría Jurídica).
Registros solicitados y revisados	• Evidencia de la restauración de cuenta de usuario (Lote 1)
Tiempo /ANS del proceso	• Tiempo de resolución incidentes de seguridad Alto < 16 horas.
Salida del proceso	• Peticiones en el Sistema de Gestión de Incidencias y Peticiones (Gestión de Tickets). • Actualización del Registro de Incidentes y actualización de estado a ICEX y partes interesadas. • Restauración y verificación de la cuenta comprometida.

Fase 4. Actividades post-incidente

OBJETIVOS: durante la fase post-incidente, se llevará a cabo una revisión detallada y reflexiva del incidente, con el objetivo de extraer lecciones valiosas y mejorar continuamente las capacidades de ciberseguridad.

F. Análisis final e informe del incidente	
Tareas	**Subtareas**
1. Documentación de hallazgos	• Analizar todos los datos obtenidos durante el análisis del incidente y se organizan los hallazgos de manera clara y concisa para facilitar la comprensión en el informe.
2. Análisis de causas raíz	• Identificar y analizar las causas del incidente, cómo y por qué ocurrió el incidente, fallos en los controles de seguridad, errores humanos, vulnerabilidades del sistema, etc.
3. Análisis de las acciones tomadas	• Analizar las estrategias de las respuesta, métodos de comunicación, roles y responsabilidades involucrados, flujos de trabajo, condiciones de gestión y tiempos de respuesta.
4. Impacto del	• Describir el alcance del daño: impacto operativo, reputacional,

incidente	legal y coste (especialmente, en términos de compromiso de información y servicios degradados durante la gestión).
5. Desarrollo de Informe	• La Oficina de Seguridad Digital (Lote 2), con el soporte del Coordinador, desarrollarán el Informe final que consta de un Informe Técnico y un Informe Ejecutivo.
6. Entrega y presentación de los informes	• Hacer entrega del Informe a las partes interesadas y programación de una reunión para la presentación formal de los informes. • Presentar al Comité Operativo mensual el informe ejecutivo.
Recursos involucrados en la GESTIÓN y resultados del proceso	
Organización del equipo CIPHERBIT	• Coordinador de Seguridad (Lote 2). • Analista de Seguridad (Lote 2). • Oficina de Seguridad Digital (Lote 2).
Necesidades equipos ICEX y/o terceros	• NA
Registros solicitados y revisados	• Toda la información obtenida durante la gestión del incidente.
Tiempo /ANS del proceso	• Tiempo de entrega de informes técnicos y ejecutivos desde que se produjo el incidente: < 10 días.
Salida del proceso	• Informes del Incidente para: Comité de Seguridad y Comité Operativo, Gestores Técnicos de los 3 Lotes, Coordinador de Servicio (Lote 1), Jefe de Servicio de la Oficina de Gestión (Lote 3) y otros interesados.

G. Lecciones aprendidas, medidas correctivas y mejoras proactivas	
Tareas	**Subtareas**
1. Lecciones aprendidas	• Con la colaboración y feedback de todas las partes interesadas, se consagra un know-how de lecciones aprendidas para minimizar la probabilidad de materialización de futuros incidentes similares. • Análisis reposado de las causas del problema y cómo se ha desarrollado la actividad durante la gestión y problemas asociados. • Determinar áreas de mejora en políticas, procedimientos y controles de seguridad, mecanismo de comunicación, notificación y coordinación, así como en tecnologías de prevención, detección, comunicación y gestión de incidentes.

2. Medidas correctivas	• Proporcionar recomendaciones de protección de cuentas de usuario y correo electrónico. • Identificar acciones correctivas a corto y largo plazo para prevenir y, en su caso, gestionar de forma más eficiente y ágil incidentes similares. • Actualizar las métricas e indicadores de implantación, eficacia, eficiencia y gestión de incidentes. • Revisar la adecuación de los ANS e idoneidad de la taxonomía de incidentes y criterios de clasificación. • Desarrollar y documentar, siguiendo las indicaciones del Área de Calidad y Procesos, playbooks específicos para este incidente (o revisan y actualizan, en caso de ya disponerse) y otros que puedan cubrir escenarios relacionados o similares.
3. Preparación proactiva	• Se capacitará al personal y se realizarán ejercicios de simulación del incidente, siguiendo las indicaciones del Área de Calidad y Procesos, para comprobar los cambios realizados en los planes de respuesta y playbooks y verificar si las medidas implementadas son suficientes.
Recursos involucrados en la GESTIÓN y resultados del proceso	
Organización del equipo CIPHERBIT	• Coordinador de Seguridad (Lote 2). • Analista de Seguridad (Lote 2). • Oficina de Seguridad Digital (Lote 2).
Necesidades equipos ICEX y/o terceros	• Gestores Técnicos de los 3 Lotes • Coordinador de Servicio (Lote 1). • Jefe de Servicio de la Oficina de Gestión (Lote 3). • Área de Calidad y Procesos. • Comité Operativo y Comité de Seguridad.
Registros solicitados y revisados	• N/A.
Tiempo /ANS del proceso	• Número mínimo de playbooks propuestos/implementado. tras incidente de seguridad potencial > 1.
Salida del proceso	• Informe Post-incidentes de lecciones aprendidas. • Playbooks específicos y simulación de incidentes. • Evoluciones del plan de respuesta y gestión de incidentes.

ANEXO III. MODELO DE PROPOSICIÓN ECONÓMICA Y CRITERIOS DE VALORACIÓN AUTOMÁTICA
LOTE 2

(A incluir en el sobre nº 3)

DATOS DE IDENTIFICACIÓN DEL EXPEDIENTE

Expediente nº: 162/2023
Objeto: Suministro, administración, gestión y operación de la infraestructura tecnológica de ICEX y de la Red Exterior y Territorial:
- Lote 2: Servicio de Oficina de Seguridad Digital de ICEX Servicios Centrales y la Red Exterior y Territorial.

Presupuesto base de licitación: 4.159.883,20 €, IVA incluido.

DATOS DE IDENTIFICACIÓN DEL FIRMANTE DE LA PROPOSICIÓN Y DEL LICITADOR

Apellidos y nombre del firmante de la proposición: DIEZ FERNANDEZ, ALFREDO
Relación que une al firmante con el licitador[1]: Representante legal, (Apoderado)
Razón Social del Licitador: CIPHERBIT, S.L.U.
NIF del licitador: B01644558
Domicilio del licitador Calle Marie Curie, 19, Rivas Vaciamadrid, 28521
Teléfono [redacted]

DATOS DE LA DIRECCIÓN DE CORREO HABILITADA PARA RECIBIR NOTIFICACIONES ELECTRÓNICAS:

concursos@oesia.com

PROPOSICIÓN ECONÓMICA

El abajo firmante, en virtud de la representación que ostenta se compromete, en nombre de su representado, a la ejecución del contrato para la contratación del Servicio de Oficina de Seguridad Digital de ICEX Servicios Centrales y la Red Exterior y Territorial (Lote 2) en la cifra de TRES MILLONES TREINTA Y UN MIL OCHOCIENTOS DIECISEIS EUROS CON SESENTA Y SEIS CÉNTIMOS (3.031.816,66 €) IVA incluido, con el siguiente desglose:

Importe IVA excluido: **2.505.633,60 €**
IVA: **526.183,06 €**

El importe no podrá superar la cifra de CUATRO MILLONES CIENTO CINCUENTA Y NUEVE MIL OCHOCIENTOS OCHENTA Y TRES EUROS CON VEINTE CÉNTIMOS (4.159.883,20 €), IVA incluido.

De acuerdo con las estipulaciones contenidas en los pliegos que rigen la referida licitación, aceptando expresamente el contenido de los mismos por la mera presentación de esta oferta.

[1] A cumplimentar por el licitador: "Apoderado, Gerente o Administrador". Si el licitador actúa en su propio nombre, dejará en blanco este apartado

En el precio ofertado se consideran y aceptan como incluidos cualquier otro tributo o gasto que se derive de la ejecución del contrato y que no figure excluido expresamente en Cuadro de Condiciones Particulares o en el cualquier otro documento integrante de los pliegos.

El desglose del precio ofertado se completará a través del ***Anexo III-2. Modelo de Oferta Económica Lote 2.***

CRITERIOS AUTOMÁTICOS (EQUIPO DE TRABAJO)

El desglose y el detalle de los criterios automáticos se completará a través del ***Anexo III-3. Requisitos valorables del Equipo de Trabajo Pliego Infraestructuras Lote 2.***

En Rivas Vaciamadrid, a fecha firma.

Fdo.: D. ALFREDO DIEZ FERNANDEZ
APODERADO