

Pliego de Cláusulas Técnicas que han de regir el contrato de servicio denominado **“SERVICIO DE DESARROLLO, IMPLANTACIÓN Y EJECUCIÓN DE UN PROGRAMA DE FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD PARA PERSONAL SANITARIO Y DE LAS ENTIDADES LOCALES”** a adjudicar mediante procedimiento abierto con pluralidad de criterios, bajo el marco del Proyecto RETECH, alineado con la Agenda España Digital 2026 y el Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea – NEXT GENERATION EU

Expediente: ACR-037-2025



INDICE:

CLÁUSULA 1.- INTRODUCCIÓN.....	4
1.1 Finalidad del contrato.....	4
1.2 Contexto estratégico y marco del proyecto RESEDA	4
1.3 Naturaleza del servicio y enfoque	5
CLÁUSULA 2.- OBJETO Y ALCANCE DEL CONTRATO	6
2.1 Objeto y alcance del contrato.....	6
2.2 Duración del contrato y calendario de ejecución.....	7
2.3 Exclusiones del contrato	8
2.4 Resultados esperados e impacto previsto	8
2.4.1 Impacto previsto.....	9
CLÁUSULA 3.- REQUISITOS GENERALES	10
3.1 Condiciones generales de ejecución	10
3.2 Enfoque metodológico y principios pedagógicos	11
3.3 Segmentación y adaptación al público destinatario	11
3.4 Accesibilidad, inclusión y formatos multicanal	12
CLÁUSULA 4.- CAPACIDADES, FUNCIONES Y SERVICIOS A PRESTAR	13
4.1 Ámbito operativo de proyecto	13
4.1.1 Planificación, diseño y validación de los eventos formativos	13
4.1.2 Organización técnica y soporte logístico	17
4.1.3 Materiales, evaluación y dinamización	18
4.1.4 Entregables principales.....	19
4.2 Ámbito de gestión y coordinación	20
4.2.1 Entregables transversales.....	21
CLÁUSULA 5.- EQUIPO Y LUGAR DE TRABAJO	22
5.1 Composición orientativa del equipo	22
5.2 Perfiles profesionales y dedicación.....	22
5.3 Lugar de trabajo.....	24
CLÁUSULA 6.- TECNOLOGÍAS Y HERRAMIENTAS A UTILIZAR	25
6.1 Entornos de simulación, virtualización y despliegue de ejercicios	25
6.2 Herramientas de dinamización, puntuación y evaluación	26
6.2.1 Requisitos de conectividad e infraestructura.....	27
6.2.2 Requisitos de ciberseguridad para entornos prácticos y de simulación	27
6.2.3 Herramientas de apoyo para campañas de entrenamiento de phishing	28
6.3 Requisitos transversales de soporte y mantenimiento.....	29
CLÁUSULA 7.- MODELO DE GESTIÓN DEL SERVICIO.....	29
7.1 Gobernanza y actores clave	29
7.2 Planificación, cronograma y fases	30
7.3 Comunicación y reporte	31
CLÁUSULA 8.- GESTIÓN DE LA SEGURIDAD	31
8.1 Confidencialidad y uso de la información.....	31

8.2	Cumplimiento del ENS y normativa de protección de datos	31
8.3	Obligaciones del personal del contratista	31
8.4	Medidas específicas de protección de la documentación	32
8.5	Notificación de incidentes de seguridad.....	32
CLÁUSULA 9.- DERECHOS Y OBLIGACIONES		32
9.1	Obligaciones del contratista	32
9.2	Derechos del órgano de contratación	33
9.3	Propiedad de los resultados y derechos de uso	33
9.4	Licenciamiento, formatos y reutilización institucional	33
9.5	Responsabilidad frente a terceros	33
CLÁUSULA 10.- CALIDAD DEL SERVICIO.....		33
10.1	Criterios de calidad de los entregables	33
10.2	Validación técnica de resultados.....	34
10.3	Indicadores de calidad y mejora continua	34
CLÁUSULA 11.- PLAZOS, DURACIÓN Y ETAPAS		34
11.1	Duración total del contrato	34
11.2	Hitos técnicos.....	34
11.3	Plazos de revisión y validación de entregables.....	35
CLÁUSULA 12.- GARANTÍA DE LOS TRABAJOS		35
12.1	Compromisos de garantía.....	35
12.2	Corrección de deficiencias	35
12.3	Alcance del compromiso de garantía	35
CLÁUSULA 13.- CUMPLIMIENTO NORMATIVO ADICIONAL.....		35
13.1	Principio DNSH (Art. 5 Orden HFP/1030/2021)	35
13.2	Etiquetado verde y etiquetado digital (Art. 4 Orden HFP/1030/2021)	35
13.3	Comunicación y publicidad	36
CLÁUSULA 14.- CONSULTAS SOBRE EL PLIEGO TÉCNICO		37

CLÁUSULA 1.- INTRODUCCIÓN

1.1 Finalidad del contrato

El objeto del presente contrato es la prestación de un servicio integral para el diseño, desarrollo, ejecución y evaluación de un programa de formación, concienciación y entrenamiento práctico en ciberseguridad, dirigido al personal del sector sanitario de la Comunidad de Madrid y del ámbito local, en el marco de la iniciativa RESEDA.

El servicio comprende el diseño, preparación, dinamización y evaluación de un plan formativo de actividades de carácter especializado en ciberseguridad, incluyendo:

- **Dos hackathones**, orientados al aprendizaje colaborativo mediante retos sectoriales de innovación.
- **Nueve ciberejercicios**, centrados en la simulación de incidentes reales y el entrenamiento operativo de respuesta técnica y organizativa.
- **Doce sesiones presenciales de formación dirigidas a la alta dirección** de los organismos del sector sanitario y de las entidades locales de la Comunidad de Madrid, con enfoque estratégico, de gobernanza y gestión de crisis.
- **Seis campañas de sensibilización frente a phishing**, diseñadas para reforzar la capacidad de detección y respuesta de empleados, frente a intentos de ingeniería social (phishing, smishing y vishing).
- **Diez sesiones formativas temáticas especializadas**, centradas en materias normativas (ENS, NIS2, CER, RGPD, etc.) y en tecnologías emergentes (IA, IoT sanitario, cloud, ciberseguridad en entorno sanitario y smartcities, entre otras), con un alcance abierto y adaptable a las necesidades detectadas.

Con esta contratación se persigue alcanzar los siguientes objetivos estratégicos:

- a) Reforzar las competencias en ciberseguridad del personal mediante actividades prácticas, sesiones especializadas y métricas de aprendizaje que permitan medir su impacto, con acciones de cercanía y adaptadas a sus necesidades, tanto en el ámbito sanitario como en las entidades locales.
- b) Desarrollar una cultura de ciberseguridad, implicando activamente a profesionales y directivos en dinámicas de entrenamiento y sensibilización frente a amenazas reales.
- c) Sensibilizar a los órganos de dirección sobre los riesgos, decisiones y responsabilidades en materia de ciberseguridad, facilitando la adopción de una visión estratégica y proactiva.
- d) Evaluar de forma estructurada el impacto del programa, mediante indicadores clave de rendimiento (KPIs), informes técnicos e instrumentos de análisis comparativo, que permitan la mejora continua de las capacidades organizativas.

1.2 Contexto estratégico y marco del proyecto RESEDA

El presente contrato se enmarca en el Proyecto RESEDA (Resiliencia de los Datos en el Sector Salud y en la Administración Local), una iniciativa estratégica incluida en el Plan de Recuperación, Transformación y Resiliencia (PRTR) del Gobierno de España y financiada con cargo al Mecanismo de Recuperación y Resiliencia de la Unión Europea (NextGenerationEU).

Las actuaciones objeto de este contrato forman parte de la Línea 4 del Proyecto RESEDA, orientada al sector sanitario, y de la Línea 5, dirigida al ámbito de las entidades locales. Ambas líneas están alineadas con los objetivos del Componente 15, Inversión 7, que refuerzan la ciberseguridad en sectores esenciales de prestación de servicios públicos y de protección de derechos fundamentales.

El sector salud, clasificado como infraestructura crítica de acuerdo con el marco legal vigente, enfrenta un riesgo creciente de ciberamenazas que comprometen la seguridad de la información, la continuidad asistencial y la confianza ciudadana. Del mismo modo, las entidades locales, como administraciones de proximidad responsables de servicios básicos y de la gestión de datos personales de la ciudadanía, presentan una alta exposición a incidentes de ciberseguridad que pueden afectar de forma directa a la prestación de servicios públicos esenciales.

En este contexto, la Agencia de Ciberseguridad de la Comunidad de Madrid, creada mediante la Ley 14/2023, asume la competencia y liderazgo en la coordinación e impulso de actuaciones destinadas a fortalecer la ciberresiliencia de estos sectores estratégicos.

La iniciativa se apoya en un marco normativo robusto, que establece obligaciones concretas para los operadores del sector sanitario y de las entidades locales en materia de ciberseguridad y protección de datos:

- **Reglamento General de Protección de Datos (RGPD) y Ley Orgánica 3/2018 (LOPDGDD)**, en relación con la protección de datos personales.
- **Directiva (UE) 2022/2555 (NIS2) y Directiva (UE) 2022/2557 (CER)**, sobre medidas de ciberseguridad y resiliencia de entidades críticas.
- **Esquema Nacional de Seguridad (ENS)**, regulado por el Real Decreto 311/2022, como marco de referencia para la protección de los sistemas de información en el sector público.

Todas estas disposiciones subrayan la necesidad de adoptar medidas organizativas, técnicas y formativas que refuercen la preparación del sector sanitario y de las administraciones locales frente a las amenazas digitales.

En este marco, el componente humano se considera un factor crítico de éxito. La sensibilización y capacitación del personal de los sectores sanitario y local resultan indispensables para minimizar vulnerabilidades, mejorar la capacidad de respuesta institucional y consolidar una cultura organizativa de seguridad como eje transversal del funcionamiento de los servicios públicos, reforzando especialmente la capacidad de reconocer y responder a intentos de ingeniería social, una de las principales amenazas actuales.

1.3 Naturaleza del servicio y enfoque

El contrato se caracteriza por su naturaleza de servicio integral, que combina consultoría especializada, desarrollo de materiales formativos, prestación de servicios de capacitación y ejecución práctica. Todo ello se articula con un enfoque específicamente diseñado para el sector sanitario y el ámbito de las entidades locales, atendiendo a su exposición a riesgos digitales, sensibilidad de los datos, criticidad de los servicios y diversidad de perfiles profesionales implicados.

El servicio incluye un conjunto de actuaciones de carácter práctico, formativo y de sensibilización, entre las que destacan:

- **Ciberejercicios:** nueve (9) sesiones prácticas orientadas al entrenamiento ante incidentes de ciberseguridad y a la mejora de la respuesta técnica y organizativa. Deben ser altamente prácticas y plenamente adaptadas al público objetivo y a sus necesidades.
- **Hackathones:** dos (2) eventos colaborativos dirigidos a profesionales y estudiantes del ámbito tecnológico, en los que se desarrollan soluciones innovadoras ante retos vinculados a la ciberseguridad.
- **Formación presencial para alta dirección:** doce (12) sesiones específicamente diseñadas para perfiles de alta responsabilidad en la Comunidad de Madrid, centradas en la gobernanza, la toma de decisiones estratégicas, la gestión de crisis y la continuidad operativa en ciberseguridad.

- **Campañas de sensibilización frente a phishing:** seis (6) campañas prácticas y progresivas que permitan medir la exposición y mejorar la capacidad de detección y respuesta del personal sanitario y los empleados de entidades locales frente a intentos de ingeniería social.
- **Sesiones formativas sobre temáticas especializadas:** diez (10) sesiones de carácter diverso, centradas en materias normativas (ENS, NIS2, CER, RGPD, etc.) y en tecnologías emergentes (IA, IoT sanitario, cloud, ciberseguridad en entorno sanitario, ciberseguridad en entorno local, entre otras).

Todas estas actuaciones comparten un **enfoque metodológico y operativo común**, orientado a garantizar la alineación con el marco estratégico y regulatorio vigente, la adaptación a las necesidades reales de la Agencia de Ciberseguridad de la Comunidad de Madrid y la sostenibilidad de los resultados obtenidos. Dicho enfoque se basa en principios de **accesibilidad, inclusión, calidad pedagógica, innovación tecnológica y mejora continua**, asegurando la coherencia entre acciones formativas, de sensibilización y de simulación práctica, así como la continuidad operativa del servicio en el tiempo.

CLÁUSULA 2.- OBJETO Y ALCANCE DEL CONTRATO

2.1 Objeto y alcance del contrato

El presente contrato tiene por objeto la prestación de un servicio integral de formación, concienciación y entrenamiento práctico en ciberseguridad, dirigido al personal del sector sanitario y entidades locales de la Comunidad de Madrid, en el marco del proyecto RESEDA. Su finalidad es fortalecer las capacidades humanas y organizativas frente a ciberamenazas, combinando actividades colaborativas de simulación práctica, campañas de sensibilización, sesiones formativas temáticas y sesiones presenciales dirigidas a los equipos directivos.

El contrato se articula bajo principios de reutilización, sostenibilidad y aprovechamiento institucional de los resultados. Todas las actuaciones deberán ejecutarse con un enfoque modular, escalable, interoperable y alineado con los objetivos de continuidad y generalización en el sector público, conforme a lo establecido en la cláusula 9 del presente pliego.

El servicio comprende el diseño, ejecución y evaluación de un conjunto de actividades prácticas y formativas, destinadas tanto al entrenamiento colaborativo como a la formación directa y a la sensibilización frente a riesgos de ingeniería social. Todas estas actividades estarán plenamente adaptadas para cubrir las necesidades específicas del entorno y del público al que se dirigen.

Se desarrollarán las siguientes acciones:

- **Nueve (9) ciberejercicios**, centrados en la simulación de incidentes de ciberseguridad y la evaluación de la capacidad organizativa y técnica de respuesta. Soportados por una herramienta de simulación, que servirá de guía para la ejecución de la actividad.
- **Dos (2) hackathones**, dirigidos a profesionales y estudiantes del ámbito tecnológico, donde se abordarán diferentes retos, con participación del personal de la Agencia en roles de observación o dinamización. La temática será consensuada con la Agencia, así como los niveles de los retos y el uso de reutilización de contenidos o desarrollo nuevo.
- **Doce (12) sesiones presenciales de formación para la alta dirección**, diseñadas específicamente para responsables de dirección general, gerencia, sistemas de información, contratación, asuntos legales, control interno y ciberseguridad del organismo en cuestión. Estas sesiones estarán orientadas a reforzar la comprensión institucional del riesgo digital y a facilitar la toma de decisiones estratégicas informadas en materia de seguridad. Cada formación se llevará a cabo tras un ejercicio de consultoría de cada organismo, para analizar y asesorar con una base fundamentada de la casuística de cada organismo.

- **Seis (6) campañas de sensibilización frente a phishing**, progresivas y segmentadas, orientadas a reforzar las capacidades de detección y respuesta del personal frente a intentos de ingeniería social (phishing, smishing y vishing).
- **Diez (10) sesiones formativas temáticas especializadas**, de dos horas de duración, centradas en materias normativas (ENS, NIS2, CER, RGPD, etc.) y en tecnologías emergentes (IA, IoT sanitario, cloud, ciberseguridad en entorno sanitario, ciberseguridad en entorno local, entre otras), con un alcance abierto y adaptable a las necesidades detectadas.

Cada evento incluirá:

- Gestión del calendario de las acciones y de las invitaciones de los participantes.
- Diseño técnico y pedagógico de los contenidos, adaptados a su tipología.
- Validación por parte de expertos en ciberseguridad, TI del sector salud y de la administración local, y en gestión institucional.
- Fichas técnicas detalladas, incluyendo objetivos, roles, tiempos, requisitos y criterios de éxito.
- Configuración de entornos virtuales cuando proceda (sandbox, cyber-range o simuladores específicos).
- Gestión de inscripciones, canales de comunicación y soporte logístico.
- Observación estructurada de la dinámica de los participantes o asistentes.
- Evaluación individualizada de los resultados y elaboración de informes por evento.

Al cierre del servicio se entregará un informe consolidado de resultados, que incluya:

- Métricas de participación y desempeño.
- Análisis de impacto y calidad percibida.
- Propuestas de mejora y plan de continuidad.
- Repositorio de materiales reutilizables, buenas prácticas y fichas técnicas.

2.2 Duración del contrato y calendario de ejecución

La duración del contrato será de **seis (6) meses** a contar desde la fecha de formalización, con posibilidad de **dos (2) prórrogas adicionales**, cada una por un periodo de seis (6) meses, en las mismas condiciones del periodo inicial.

El servicio se desarrollará de forma progresiva a lo largo de cada periodo contractual, iniciando con una fase de preparación intensiva y seguida de la ejecución escalonada de los distintos eventos formativos y de sensibilización planificados.

Meses 1 a 2: Fases 1 y 2 – Planificación y preparación

- **Fase 1:** Planificación estratégica de las actividades.
- **Fase 2:** Preparación técnica y logística de los ejercicios y sesiones.

Durante este periodo se procederá a:

- Validar los retos técnicos y pedagógicos.
- Configurar los entornos virtuales (sandbox, cyber-range o simuladores específicos).
- Definir los sistemas de evaluación y criterios de éxito.
- Coordinar los aspectos logísticos y comunicativos esenciales.

Meses 3 a 6: Fases 3 y 4 – Ejecución y evaluación

- **Fase 3:** Realización de todas las actividades previstas, distribuidas del siguiente modo:

- 9 ciberejercicios
- 2 hackathones
- 12 sesiones de formación para alta dirección
- 6 campañas de sensibilización frente a phishing
- 10 sesiones formativas temáticas especializadas

- **Fase 4:** Evaluación de impacto, consolidación de resultados y elaboración del informe final.

Cada actividad requerirá una preparación previa específica y su correspondiente evaluación posterior, integrándose en un informe consolidado que recoja métricas de participación, calidad percibida y propuestas de mejora.

2.3 Exclusiones del contrato

Quedan excluidas del presente contrato las siguientes actividades, servicios o suministros:

- El desarrollo de software a medida o la creación/adaptación de plataformas tecnológicas propietarias, así como la evolución de soluciones distintas de las estrictamente necesarias para la ejecución de las actividades contratadas. (Se exceptúa la configuración básica y uso, durante la vigencia del contrato, de herramientas de soporte para los eventos, p. ej., videoconferencia, registro de hackathones, guiado y evaluación de ciberejercicios, y de simulación de phishing para campañas de concienciación)
- La adquisición de licencias o derechos de uso con vigencia que exceda el periodo contractual, salvo las expresamente incluidas como parte del servicio en los plazos establecidos en este pliego.
- La provisión de equipamiento físico, dispositivos o infraestructura tecnológica individualizada para el acceso o uso por parte de los usuarios finales.
- La contratación de espacios físicos, servicios de restauración, transporte u otros recursos logísticos, salvo el suministro de refrigerios ligeros previstos en el diseño y desarrollo de los eventos contemplados en el contrato, que se entienden incluidos en el alcance del servicio.
- La actualización, revisión o modificación de materiales y contenidos formativos una vez hayan sido aceptados por la Agencia, aceptación que deberá producirse dentro del periodo de vigencia de cada actividad. El alcance se limita a la entrega y conservación de dichos materiales durante el periodo contractual, sin incluir paquetes de mantenimiento pedagógico ni adaptaciones derivadas de cambios normativos, técnicos o de amenazas posteriores.

2.4 Resultados esperados e impacto previsto

El presente contrato tiene como finalidad generar un impacto tangible y medible en la cultura de ciberseguridad del sector sanitario y local de la Comunidad de Madrid, promoviendo una transformación progresiva en las competencias digitales de los profesionales y en la capacidad organizativa frente a ciberamenazas.

Los resultados esperados se estructuran en torno a los siguientes ejes:

- Ejecución completa de las actividades previstas, que comprenden:
 - 2 hackathones.
 - 9 ciberejercicios.
 - 12 sesiones de formación dirigidas a la alta dirección.

- 6 campañas de sensibilización frente a phishing.
- 10 sesiones formativas temáticas especializadas.
- Diseño técnico y pedagógico adaptado a cada tipología de evento, con despliegue de entornos virtuales específicos (sandbox o cyber-range) cuando proceda.
- Medición estructurada de resultados, incluyendo:
 - Nivel de participación efectiva y diversidad de perfiles.
 - Desempeño observado en pruebas y simulaciones.
 - Capacidad de trabajo en equipo y coordinación interprofesional.
 - Calidad, aplicabilidad y grado de innovación de los productos generados en los hackathones.
 - Satisfacción de participantes y transferencia de conocimiento en sesiones temáticas y de alta dirección.
- Documentación sistemática del proceso, mediante la generación de un repositorio reutilizable que incluya materiales, retos técnicos, fichas metodológicas y buenas prácticas transferibles.
- Entrega de un informe final consolidado, con análisis comparativo entre eventos, indicadores clave de rendimiento (KPIs), identificación de factores de éxito y propuestas de continuidad o escalabilidad.

2.4.1 Impacto previsto

Los resultados anteriores deberán traducirse en los siguientes impactos concretos y verificables:

- Incremento significativo de la concienciación en ciberseguridad entre el personal sanitario, con una mayor capacidad para identificar amenazas comunes y aplicar buenas prácticas en su actividad diaria.
- Incremento de la concienciación y de la madurez en ciberseguridad entre el personal de las entidades locales, con mayor capacidad para identificar amenazas y aplicar buenas prácticas en su actividad.
- Refuerzo de la preparación organizativa ante ciberincidentes, gracias al entrenamiento práctico, la simulación de escenarios realistas y la mejora de los protocolos de actuación conjunta.
- Mayor implicación de la alta dirección en la gobernanza de la ciberseguridad, facilitando la integración de estos aspectos en la planificación estratégica y en la gestión del riesgo institucional.
- Consolidación de una cultura digital de seguridad, que promueva la coordinación entre funciones clínicas, administrativas y técnicas en la gestión del riesgo cibernético.
- Disponibilidad de recursos reutilizables, incluyendo materiales, fichas metodológicas, retos técnicos y guías de buenas prácticas, que faciliten la extensión del programa a otros ámbitos y su replicación en futuras ediciones dentro de la Comunidad de Madrid.
- Refuerzo de la coordinación y respuesta en las entidades locales ante ciberincidentes, mediante simulaciones y mejora de protocolos interfuncionales.

CLÁUSULA 3.- REQUISITOS GENERALES

3.1 Condiciones generales de ejecución

La ejecución del contrato se regirá por principios de calidad, cumplimiento de plazos, orientación a resultados y coordinación efectiva con la Agencia de Ciberseguridad.

Condiciones generales

- Se deberá cumplir rigurosamente el calendario y los hitos establecidos en la planificación del contrato. Toda desviación significativa deberá comunicarse con antelación suficiente a la Agencia, acompañada de una propuesta de medidas correctoras.
- Se deberá asignar personal cualificado, con experiencia acreditada en las materias objeto del contrato, y disponer de los medios técnicos y logísticos necesarios para garantizar la correcta ejecución de las actividades.
- Cada fase del servicio deberá planificarse en detalle, incluyendo cronogramas, responsables, entregables previstos y métricas de seguimiento.
- El adjudicatario implantará mecanismos internos de control, revisión y mejora continua de la calidad de los entregables.
- Se deberá mantener un registro sistemático de evidencias que respalden la ejecución: actas, informes, estadísticas de participación, materiales desarrollados y documentación técnica o pedagógica de soporte.
- Se deberá garantizar la capacidad de adaptación ante nuevas necesidades operativas que puedan surgir durante la ejecución, siempre que no supongan una modificación del objeto ni del alcance contractual.
- Se deberá asegurar la continuidad en la prestación del servicio hasta su finalización en los términos establecidos en este pliego, incluyendo cobertura de ausencias, recuperación de retrasos, resolución de incidencias y mantenimiento sin interrupciones injustificadas.
- Se deberá cumplir estrictamente con la normativa vigente en materia de ciberseguridad, protección de datos personales, accesibilidad digital, neutralidad tecnológica, imagen institucional y uso responsable de recursos públicos.

Condiciones específicas para las actividades previstas

- La ejecución de las actividades formativas y de sensibilización previstas deberá desarrollarse de manera escalonada durante el periodo contractual, una vez aprobada la planificación semestral y completada la preparación técnica y logística realizada en los dos meses iniciales.
- Cada actividad deberá contar con un plan específico de coordinación, ejecución y evaluación, que será validado previamente por la Agencia.
- En el caso de las sesiones de formación dirigidas a la alta dirección, se deberá prestar especial atención a su adecuación a las agendas institucionales, a su coherencia metodológica y a la calidad pedagógica de los materiales y ponentes.
- En el caso de las sesiones temáticas especializadas, los contenidos deberán ser actualizados y diversos, abarcando tanto ámbitos normativos (ENS, NIS2, CER, RGPD) como tecnológicos (IA, IoT sanitario, cloud, ciberseguridad en dispositivos médicos, entre otros).
- En el caso de las campañas de concienciación frente a phishing, las herramientas utilizadas deberán permitir su ejecución en modalidad SaaS, garantizando trazabilidad, confidencialidad de resultados y cumplimiento de la normativa aplicable en materia de protección de datos.

3.2 Enfoque metodológico y principios pedagógicos

El servicio deberá regirse por un enfoque metodológico centrado en la persona usuaria, adaptado a la diversidad de perfiles del sector sanitario y a los diferentes tipos de actividades previstas (hackathones, ciberejercicios, sesiones temáticas, formación de alta dirección y campañas de sensibilización).

Principios comunes

- Se aplicará un aprendizaje centrado en la persona, con contenidos y dinámicas adaptados al perfil profesional, al nivel competencial y al contexto específico del sector trabajado.
- Se garantizará la segmentación y personalización de las actividades en función del rol desempeñado, del nivel de madurez digital y de las necesidades operativas de cada colectivo.
- Los contenidos y dinámicas se diseñarán en unidades breves y modulares, para facilitar la comprensión inmediata y permitir una asimilación progresiva y flexible (principios de microaprendizaje).
- Se garantizará un diseño accesible, inclusivo y visualmente claro, conforme a los principios de accesibilidad universal, experiencia de usuario y usabilidad.
- Las metodologías y materiales deberán estar validados por especialistas, actualizados frente a amenazas emergentes y alineados con buenas prácticas de ciberseguridad en el ámbito sanitario y local.
- Se incorporará un sistema de evaluación continua, orientado a reforzar la comprensión, consolidar aprendizajes y facilitar la mejora del desempeño.
- Se establecerá un proceso de iteración y mejora continua de contenidos, recursos y dinámicas, basado en la retroalimentación sistemática obtenida durante la ejecución.

Condiciones específicas para las actividades

- En los ciberejercicios y hackathones, se aplicarán metodologías de aprendizaje experiencial mediante simulaciones, dinámicas grupales, resolución colaborativa de retos y entrenamiento operativo en un entorno seguro y controlado.
- Las sesiones temáticas especializadas se diseñarán como espacios dinámicos y participativos, con exposición clara, análisis de casos prácticos, debate estructurado y materiales de referencia, fomentando la aplicabilidad inmediata en el entorno laboral.
- Las sesiones de formación para alta dirección se plantearán como espacios de aprendizaje estratégico, con enfoque inspiracional, discusión sobre riesgos reales, participación activa y facilitación por parte de expertos reconocidos en gobernanza, gestión de crisis y ciberseguridad.
- Las campañas de sensibilización frente a phishing (smishing y vishing incluidos) se diseñarán como experiencias breves, realistas y seguras, que combinen la exposición práctica a intentos simulados con retroalimentación inmediata y materiales explicativos. Estas campañas deberán fomentar la capacidad de detección, la adopción de conductas preventivas y la mejora progresiva del comportamiento de los participantes, garantizando siempre la anonimización o pseudonimización de los resultados individuales.

3.3 Segmentación y adaptación al público destinatario

La segmentación constituye un principio estructural en el diseño metodológico y en la planificación de las actividades formativas, prácticas y de sensibilización. Su finalidad es asegurar que las acciones se ajusten a la diversidad de perfiles y maximicen su eficacia.

- Se aplicará una segmentación doble y complementaria:
 - Por grupo funcional:

- En el sector sanitario, incluyendo como mínimo: personal asistencial especializado, personal de enfermería, auxiliares y técnicos clínicos, personal administrativo, servicios generales, cargos directivos, responsables de seguridad de la información y delegados de protección de datos.
- En el ámbito de las entidades locales, incluyendo como mínimo: personal TIC, responsables de seguridad de la información, personal directivo, personal administrativo y delegados de protección de datos.
- Por nivel de progresión, definido en tres categorías (básico, intermedio y avanzado), en función de la complejidad técnica, la profundidad conceptual y el grado de implicación práctica requerida.
- Se garantizará un enfoque inclusivo y representativo, evitando sesgos de género, jerarquía o rol, e incorporando ejemplos y narrativas que reflejen la diversidad de cada entorno.
- Como parte del proceso de segmentación, se deberá realizar una evaluación diagnóstica previa de las capacidades digitales y de ciberseguridad de los colectivos destinatarios. Los resultados se emplearán para orientar la adecuación del grado de dificultad de las dinámicas prácticas (ciberejercicios, hackathons), de las sesiones temáticas y de las sesiones dirigidas a la alta dirección.
- Los contenidos formativos y las dinámicas de aprendizaje deberán adaptarse al grupo funcional y al nivel de progresión asignado, ajustando el lenguaje, la extensión, el nivel de detalle técnico, el grado de interactividad y los ejemplos prácticos a las características de cada destinatario, de manera que la acción resulte pertinente, comprensible y aplicable al contexto real de su actividad.

3.4 Accesibilidad, inclusión y formatos multicanal

El cumplimiento de criterios de accesibilidad universal, inclusión y disponibilidad multicanal constituye una obligación transversal aplicable a todas las actividades y materiales desarrollados en el marco del contrato.

Disposiciones comunes

- Se deberá garantizar el cumplimiento, como mínimo, del nivel AA de las Pautas WCAG 2.1, así como de lo establecido en el Real Decreto 1112/2018, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.
- Se deberá emplear un lenguaje claro, directo y comprensible, evitando tecnicismos innecesarios y ajustando el discurso al perfil de los destinatarios.
- Se deberá asegurar la subtítulos de todos los contenidos audiovisuales y la disponibilidad de transcripciones textuales, de modo que puedan ser comprendidos por personas con discapacidad auditiva.
- Se deberá garantizar la compatibilidad con tecnologías de asistencia (lectores de pantalla, navegación por teclado u otras herramientas de apoyo).
- Se deberá implementar un diseño responsive y multicanal, que asegure el acceso desde navegadores web y dispositivos móviles, así como la posibilidad de descargar materiales en formatos imprimibles accesibles (por ejemplo, documentos PDF estructurados).
- Se deberá incorporar de forma explícita la perspectiva de género y diversidad en ejemplos, imágenes, casos y dinámicas, fomentando la representatividad y evitando estereotipos.
- Se deberá realizar una validación previa de accesibilidad y usabilidad de los entornos digitales y de los materiales de apoyo, antes de su publicación o puesta a disposición de los usuarios finales.

Aplicación a las actividades previstas

- En los ciberejercicios y hackathones, los materiales de apoyo (briefings, instrucciones, fichas técnicas, informes) deberán elaborarse siguiendo principios de claridad, accesibilidad y diseño inclusivo, de forma que resulten comprensibles para todos los perfiles participantes, independientemente de su nivel técnico.
- En las sesiones formativas temáticas y las sesiones para alta dirección, se garantizará la accesibilidad de presentaciones, casos prácticos y materiales de referencia, asegurando que estén disponibles en formatos digitales accesibles e imprimibles.
- En las campañas de sensibilización frente a phishing, smishing y vishing, se deberá asegurar que los mensajes y simulaciones sean claros, inclusivos y comprensibles, evitando sesgos de género, culturales o jerárquicos, y garantizando la accesibilidad de las herramientas digitales utilizadas.

CLÁUSULA 4.- CAPACIDADES, FUNCIONES Y SERVICIOS A PRESTAR

4.1 Ámbito operativo de proyecto

4.1.1 Planificación, diseño y validación de los eventos formativos

El adjudicatario será responsable de la preparación, ejecución y cierre de las 39 actividades previstas, orientadas a reforzar las capacidades de ciberseguridad tanto en el entorno sanitario como en las entidades locales de la Comunidad de Madrid.

Las funciones y requisitos operativos se estructuran en los siguientes apartados:

a) Definición inicial de alcance y planificación estratégica

- Se deberán establecer los objetivos estratégicos, los públicos destinatarios y la planificación preliminar de las actividades.
- Se deberán distribuir las 39 actividades en función de prioridades temáticas, ventanas temporales y perfiles participantes.
- Se deberá obtener la aprobación de la Agencia sobre principios metodológicos, segmentos de usuarios y tipologías de retos.

b) Definición de eventos

- Se deberán clasificar las actividades en cinco categorías:
 - Hackathones: retos técnicos, resolución de incidentes, pruebas de concepto o análisis forense.
 - Ciberejercicios: simulaciones organizativas, gestión de crisis, trabajo colaborativo y respuesta coordinada.
 - Sesiones de formación a alta dirección: espacios presenciales enfocados a decisiones estratégicas y gestión ejecutiva de la ciberseguridad.
 - Campañas de entrenamiento de phishing (phishing, smishing y vishing): simulaciones de ingeniería social seguras, orientadas a la sensibilización y el entrenamiento.
 - Sesiones temáticas especializadas: sesiones de dos horas centradas en materias normativas (ENS, NIS2, CER, RGPD, etc.) y tecnologías emergentes (IA, IoT sanitario, cloud, ciberseguridad en entorno sanitario, ciberseguridad en entorno local).
- Se deberán definir las características clave de cada actividad: duración, formato, número de participantes, niveles de dificultad, nivel de preparación requerido y fundamentos educativos.

- Cada hackathon deberá contar con al menos 20 participantes, organizados en equipos de 4 a 6 personas.
- Cada ciberejercicio deberá contar con un mínimo de 8 participantes, representando al menos tres roles diferenciados: técnico, organizativo y de dirección.
- Las sesiones de alta dirección deberán tener entre 5 y 20 asistentes.
- En las campañas de phishing, la Agencia definirá la población objetivo y las exclusiones aplicables.
- Las sesiones temáticas deberán garantizar diversidad de temas, evitando repeticiones y cubriendo tanto aspectos normativos como tecnológicos.

c) Elaboración del programa de actividades

- Se deberán distribuir cronológicamente las 39 actividades, garantizando cobertura territorial, diversidad de públicos y progresión en dificultad.
- Se deberán asignar fechas preliminares, ubicaciones (físicas o híbridas) y plataformas de simulación en el caso de las campañas de phishing.
- Se deberá notificar cualquier reprogramación por causas no imputables a la Agencia con al menos diez (10) días laborables de antelación y ejecutarla en un plazo máximo de treinta (30) días naturales.

d) Diseño pedagógico y técnico de los retos y sesiones

- Se deberán desarrollar retos prácticos ajustados a los perfiles participantes.
- Se deberán elaborar fichas técnicas con briefing, objetivos, roles, reglas, cronograma, criterios de éxito, indicadores de evaluación y requerimientos logísticos o de plataforma.
- Se deberán incluir escenarios realistas inspirados en amenazas actuales del sector sanitario y en la administración local.
- Se deberán diseñar sesiones temáticas y de dirección con materiales ejecutivos y aplicables.

e) Validación de actividades

- Se deberán someter las actividades a revisión y validación por parte de expertos sectoriales y perfiles representativos de cada sector.
- Se deberán ajustar los diseños en base a la validación, garantizando aplicabilidad, realismo y alineamiento con los objetivos.
- Se deberá verificar el cumplimiento normativo (protección de datos, confidencialidad, anonimización/pseudonimización en campañas de phishing).
- Se deberá obtener la aprobación final de cada actividad al menos un mes antes de su ejecución.
- En campañas de phishing, se deberá garantizar la seguridad por diseño (enlaces inofensivos, dominios controlados, sin recolección de credenciales reales ni ejecución de binarios).
- Se deberá proporcionar información previa corporativa sobre la campaña (sin revelar fechas exactas), con canal de dudas y opción de exclusión por causas justificadas.
- Se deberá realizar, cuando proceda, una Evaluación de Impacto relativa a la Protección de Datos (DPIA/IAE) específica para la campaña.
- En simulaciones de phishing, se deberá emplear un guion aprobado previamente, sin solicitar nunca datos sensibles (clínicos, financieros o de pacientes).

f) Identificación y prevalidación de ubicaciones o entornos

- Se deberán seleccionar espacios físicos y/o entornos virtuales adecuados, en coordinación con personal de la Agencia.
- Se deberá coordinar con antelación la viabilidad logística, conectividad, accesibilidad y recursos necesarios.

g) Definición de indicadores de resultado

- Se deberán establecer indicadores cualitativos y cuantitativos para medir eficacia e impacto.
- En campañas de phishing, se deberán definir métricas específicas como tasa de apertura, clic, reporte, tiempo de respuesta, interacción en vishing y evolución tras retroalimentación.
- Se deberán someter a aprobación de la Agencia todas las métricas de rendimiento, participación y satisfacción.

h) Requisitos adicionales específicos por tipología de actividad

- Hackathones:
 - Se deberá garantizar una duración mínima de dos jornadas completas, con fases claramente diferenciadas de presentación de retos, trabajo en equipos y exposición final.
 - Se deberán incluir criterios de evaluación transparentes y publicados previamente, que contemplen innovación, aplicabilidad al sector sanitario, calidad técnica y claridad en la presentación de resultados.
 - Cada equipo deberá contar con mentores multidisciplinares (al menos un perfil técnico y un perfil sanitario) para asegurar la transferencia de conocimientos.
 - Los resultados deberán entregarse en un repositorio controlado por la Agencia, en formato editable, con documentación técnica que permita su reutilización.
 - Se deberá organizar una sesión final de cierre y difusión de resultados, incluyendo la entrega de reconocimientos simbólicos a los equipos participantes.
- Ciberejercicios:
 - Se deberán plantear con niveles progresivos de dificultad (básico, intermedio y avanzado), garantizando un aprendizaje escalonado de las competencias de respuesta.
 - Cada ejercicio deberá contemplar una fase de preparación previa, con distribución de roles, guion de incidentes y materiales de referencia.
 - Se deberá garantizar la participación de al menos tres roles diferenciados en cada ejercicio: técnico, organizativo y de dirección.
 - Cada ciberejercicio deberá incluir una sesión de retroalimentación inmediata (“hot wash-up”), con recogida estructurada de observaciones y lecciones aprendidas.
 - Se deberán aplicar mecanismos de evaluación del desempeño colectivo, que complementen las métricas técnicas con indicadores de coordinación, comunicación y toma de decisiones.
 - Se deberá elaborar un informe individualizado por ejercicio, con recomendaciones prácticas de mejora y propuestas de continuidad.
- Sesiones de formación a alta dirección:
 - Cada sesión deberá tener una duración mínima de dos horas, con un formato orientado a la discusión estratégica y la toma de decisiones.
 - Se deberán incorporar casos prácticos contextualizados al sector sanitario español, preferiblemente basados en incidentes reales o simulaciones de alto impacto.

- Se deberá incluir al menos una dinámica de simulación de decisiones estratégicas, en la que los participantes deban valorar alternativas bajo presión.
- Se deberá aportar un material ejecutivo breve (“policy brief”), de un máximo de 5 páginas, con los puntos clave tratados, riesgos principales y recomendaciones prácticas.
- Adicionalmente, los materiales de apoyo deberán incluir guías prácticas, mapas de riesgos y cuestionarios de autoevaluación, adaptados a un enfoque ejecutivo.
- Los ponentes deberán ser expertos reconocidos en gobernanza, gestión de crisis y ciberseguridad, con experiencia acreditada en el ámbito sanitario.
- Se deberá garantizar la participación activa de los asistentes, evitando formatos unidireccionales exclusivamente expositivos.
- Campañas de phishing (phishing, smishing y vishing):
 - Se deberá garantizar que las campañas se diseñen con escenarios verosímiles y contextualizados al entorno objetivo, diferenciando claramente entre las modalidades de phishing, smishing y vishing.
 - La muestra de usuarios deberá ser representativa de los distintos colectivos destinatarios (personal asistencial, administrativo y directivo), de forma proporcional y equilibrada.
 - Se deberá asegurar una retroalimentación inmediata personalizada para los usuarios que interactúen con las simulaciones, mediante mensajes educativos claros o páginas de aterrizaje formativas específicas.
 - Se deberán definir y medir métricas clave (tasa de apertura, clic, reporte, tiempo de respuesta, interacción en llamadas de vishing, evolución tras retroalimentación).
 - Se deberá garantizar en todo momento la anonimización o pseudonimización de los resultados individuales, entregando a la Agencia únicamente datos agregados.
 - Se deberá elaborar un informe comparativo de tendencias al finalizar las seis campañas, mostrando la evolución de los resultados y las mejoras en la concienciación.
 - En las simulaciones de vishing, se deberá utilizar un guion previamente aprobado, sin solicitar nunca datos sensibles de carácter clínico, financiero o personal.
- Sesiones temáticas especializadas:
 - Se deberá establecer una duración estándar de dos (2) horas por sesión, incluyendo un mínimo del 25% de tiempo destinado a dinámicas participativas (debate, estudio de caso, ejercicios prácticos).
 - Los temas a tratar deberán ser consensuados previamente con la Agencia, de acuerdo con las necesidades detectadas y las prioridades estratégicas. Los alcances posibles de las sesiones incluirán, al menos:
 - a. Marco normativo y regulatorio aplicable (ENS, NIS2, CER, RGPD).
 - b. Tecnologías emergentes con impacto en el sector sanitario (IA, IoT sanitario, cloud, ciberseguridad en dispositivos médicos).
 - c. Tecnologías emergentes con impacto en el sector de ámbito local (IA, smartcities, cloud, ciberseguridad entorno local).
 - d. Buenas prácticas y estándares internacionales de ciberseguridad (ISO 27001, ISO 22301, HITRUST, etc.).

- e. Experiencias y casos prácticos de ciberincidentes en entornos de salud o de entidades locales.
- Al menos un 30% de las sesiones deberá incluir dinámicas participativas que permitan aplicar los contenidos en contextos reales.
 - Se deberá entregar un dossier digital con referencias actualizadas (normativas, guías CCN-STIC, bibliografía técnica).
 - Las sesiones deberán ser impartidas por expertos acreditados en la materia, con experiencia contrastada en la temática correspondiente y, preferiblemente, con certificaciones reconocidas (p. ej., ENS Auditor, ISO 27001 LA, CISSP, CISM).

Finalmente, el adjudicatario deberá entregar un **Plan Integral de Actividades Formativas**, que recoja todas las acciones anteriores, y que será validado por la Agencia como referencia obligatoria para la ejecución.

4.1.2 Organización técnica y soporte logístico

El adjudicatario deberá planificar y ejecutar todos los aspectos técnicos y logísticos necesarios para garantizar la correcta celebración de las treinta y nueve (39) actividades previstas, que podrán desarrollarse en modalidad presencial o híbrida, y que, en su caso, podrán apoyarse en el uso de plataformas de simulación.

Las tareas y requisitos mínimos que se deberán atender son:

a) Preparación y despliegue de entornos virtuales y plataformas de simulación:

- Se deberán diseñar, provisionar y poner en marcha los entornos técnicos necesarios (sandbox, cyber range, simuladores, etc.).
- Se deberán preparar plataformas específicas de simulación para phishing (correo, SMS y llamadas de voz).
- Se deberá garantizar la disponibilidad, rendimiento, seguridad y trazabilidad de los entornos.
- Se deberán configurar sistemas de evaluación automática y/o manual con registro de interacciones y resultados.

b) Coordinación de espacios físicos proporcionados por la Administración:

- Se deberá coordinar con la Consejería de Digitalización y con los centros participantes la preparación de los espacios físicos.
- Se deberán identificar necesidades técnicas (red, conectividad, audiovisuales, mobiliario).
- Se deberán verificar las condiciones del entorno físico y establecer planes de contingencia.

c) Gestión de inscripciones y atención a participantes en hackathones, ciberejercicios y sesiones formativas:

- Se deberán desarrollar formularios de inscripción y confirmar la participación de los asistentes.
- Se deberá enviar documentación previa (instrucciones, horarios, requerimientos técnicos).
- Se deberá controlar la asistencia y emitir certificados cuando corresponda.

d) Soporte funcional y técnico durante los eventos:

- Se deberá disponer de personal técnico de apoyo en cada actividad.
- Se deberá coordinar con dinamizadores y tutores para asegurar una ejecución fluida.

e) Comunicación previa y acompañamiento informativo:

- Se deberán elaborar y difundir materiales de convocatoria (landing pages, infografías, boletines, etc.).
- Se deberán gestionar canales de consulta previos a la actividad.

f) Provisión de refrigerios ligeros:

- En las actividades presenciales se deberá incluir la organización de pausas breves con provisión de refrigerios ligeros (café, infusiones, agua, zumos, galletas u otros elementos equivalentes), sin carácter de servicio de restauración.
- Estos refrigerios deberán estar disponibles al inicio de la jornada y/o en pausas intermedias, adecuadamente organizados para no interferir con el desarrollo de las actividades técnicas.

g) Registro, documentación y cierre:

- Se deberá documentar cada actividad (participantes, incidencias, resultados, observaciones).
- Se deberá elaborar un dossier post-actividad, incluyendo indicadores de calidad y satisfacción, en formato editable y compatible con los sistemas de análisis de la Agencia.
- En campañas de phishing, se deberán incluir métricas específicas y análisis agregado con datos anonimizados.

h) Protección de la imagen y registros:

- En las actividades con participación presencial se deberá gestionar el consentimiento de los participantes en relación con el uso de su imagen y las grabaciones realizadas.
- La publicación de fotografías, vídeos o extractos quedará restringida a fines internos, salvo autorización expresa por escrito de los interesados.

4.1.3 Materiales, evaluación y dinamización

El adjudicatario deberá proporcionar todos los materiales técnicos, herramientas de evaluación y recursos comunicativos necesarios para la correcta ejecución de las 39 actividades previstas, garantizando su adecuación pedagógica, técnica y normativa.

Las tareas y requisitos mínimos que se deberán atender son:

a) Entornos simulados seguros y soporte técnico:

- Se deberán proveer entornos virtuales seguros (cloud, redes simuladas, máquinas virtuales, sandboxes, etc.), diseñados bajo criterios de seguridad por defecto y por diseño.
- Se deberán gestionar las licencias temporales necesarias para el uso de software, plataformas y servicios asociados.
- Se deberá garantizar soporte técnico durante todo el desarrollo de cada actividad, incluyendo resolución de incidencias y monitorización de rendimiento de los entornos.

b) Herramientas de evaluación y puntuación automatizada:

- Se deberán integrar herramientas de scoring y paneles visuales de progreso en tiempo real, cuando proceda según la naturaleza de la actividad.
- En campañas de phishing, se deberán proporcionar métricas clave estandarizadas (tasa de apertura, clic, reporte, tiempo de respuesta, interacción en llamadas de phishing) y elaborar informes comparativos de evolución.
- Se deberá garantizar que los informes sean anonimizados o pseudonimizados, evitando en todo caso la identificación individual de participantes.

c) Materiales de difusión y canales de comunicación:

- Se deberán elaborar materiales de captación de participantes, incluyendo landing pages específicas por actividad, infografías explicativas, banners promocionales y mensajes adaptados al canal de difusión (boletines, intranet, redes sociales, etc.).
- Se deberán gestionar los canales de comunicación previos a las actividades, incluyendo atención a consultas, resolución de dudas técnicas, envío de instrucciones previas y mensajes de motivación.

d) Apoyo audiovisual y soporte remoto:

- Se deberá proveer soporte audiovisual profesional en hackathones y ciberejercicios híbridos, incluyendo grabación, retransmisión y apoyo técnico remoto cuando proceda.
- Se deberán garantizar mecanismos de accesibilidad y compatibilidad con los sistemas corporativos de la Administración.

e) Premios y estímulos a la participación:

- En los hackathones se deberán proporcionar premios simbólicos no monetarios (ej. reconocimientos, diplomas, kits técnicos o formativos).
- Se deberán organizar ceremonias de cierre con entrega simbólica de reconocimientos a los equipos participantes.

f) Dossier post-evento:

- Se deberá elaborar un dossier individualizado por cada actividad, que incluya al menos:
 - Descripción del escenario simulado y dinámica aplicada, cuando proceda.
 - Participación efectiva (número, perfiles, distribución por centro sanitario o entidad local).
 - Resultados agregados y análisis de desempeño, cuando proceda.
 - En campañas de phishing, métricas específicas y análisis comparativo de evolución, con resultados anonimizados o pseudonimizados.
 - Evaluación global del evento (dimensión técnica, logística y formativa).
 - Recomendaciones de mejora para futuras ediciones.
- El dossier deberá entregarse en formato editable y compatible con los sistemas de análisis de la Agencia.

Todas estas acciones deberán estar alineadas con los objetivos del programa y deberán contar con la aprobación previa de la Agencia.

4.1.4 Entregables principales

Con el objetivo de facilitar el seguimiento, control y validación del cumplimiento contractual, se establecen los siguientes entregables principales vinculados al servicio.

Todos deberán:

- Presentarse en formato editable y compatible con los sistemas ofimáticos de la Agencia de Ciberseguridad.
- Ser validados formalmente por la Agencia para considerarse aceptados.
- Respetar los plazos máximos definidos.

Entregable		Plazo de entrega	Requisitos y observaciones
E1	Plan Integral de Eventos Formativos	Mes 1	Recogerá la planificación estratégica, la tipología de actividades, el diseño metodológico y el cronograma detallado. Incluirá la distribución de las 39 actividades (hackathons, ciberejercicios, sesiones de alta dirección, campañas de phishing y sesiones temáticas especializadas), los objetivos estratégicos y las métricas de evaluación propuestas.
E2	Fichas técnicas de evento (uno por cada evento)	Mes 2	Incluirán briefing, objetivos, roles, cronograma, requerimientos técnicos, criterios de éxito, niveles de dificultad, perfil de destinatarios y fundamentos pedagógicos. Se elaborarán para cada hackathon, ciberejercicio, sesión de alta dirección, campaña de phishing y sesión temática especializada.
E3	Escenarios virtuales y materiales técnicos (uno por cada actividad aplicable)	≥1 semana antes de cada evento	Incluirán entornos simulados, licencias temporales, herramientas de evaluación, guiones de dinámica, plataformas de simulación de phishing y materiales de instrucción asociados.
E4	Materiales de difusión y convocatoria (uno por cada actividad)	≥2 semanas antes de cada evento	Incluirán landing pages, infografías, textos promocionales, banners, guías de inscripción y comunicaciones adaptadas a los distintos canales.
E5	Materiales de apoyo y recursos didácticos (uno por cada actividad)	≥1 semana antes de cada evento	Incluirán guías prácticas, infografías de referencia, mapas de riesgos, cuestionarios de autoevaluación y materiales de sensibilización para campañas de phishing (mensajes educativos, páginas de aterrizaje formativas). En sesiones temáticas especializadas se entregará un dossier digital con referencias y bibliografía técnica actualizada.
E6	Registro y documentación de actividad (una por cada actividad)	≤1 semana después de cada evento	Incluirá la relación de participantes, incidencias técnicas y logísticas, métricas preliminares de participación y satisfacción, y observaciones del equipo facilitador.
E7	Dosieres post-actividad (uno por cada actividad)	≤2 semanas después de cada evento	Incluirá resultados (anonimizados o pseudonimizados en campañas de phishing), evaluación técnica y logística, indicadores de participación y desempeño, retroalimentación de participantes, análisis de aprendizajes y propuestas de mejora. En sesiones temáticas especializadas incluirá además un resumen de las dinámicas participativas y conclusiones principales.
E8	Informe intermedio de resultados	Mes 3	Recogerá el avance parcial de la ejecución: número de actividades celebradas, indicadores agregados de impacto y satisfacción, principales incidencias y medidas correctoras aplicadas.
E9	Informe final de resultados	Mes 6	Presentará una visión consolidada del impacto, desempeño y cobertura de las 39 actividades, análisis comparativo de indicadores, lecciones aprendidas y recomendaciones para ediciones futuras.

4.2 Ámbito de gestión y coordinación

El adjudicatario deberá garantizar una adecuada gestión del servicio mediante funciones transversales que aseguren la coherencia, trazabilidad, eficiencia y calidad global del proyecto.

Estas funciones deberán coordinar de forma continua los trabajos previstos, facilitar la interlocución con la Agencia y asegurar el cumplimiento de plazos, objetivos y estándares de calidad definidos.:

a) Gestión integral del proyecto:

- El adjudicatario deberá designar una persona responsable del servicio, con dedicación estable, que actuará como interlocutor único ante la Agencia.
- El adjudicatario deberá elaborar y mantener un **Plan de Trabajo Global**, que integre cronogramas con hitos, entregables y responsables claramente definidos, y que deberá ser actualizado periódicamente en función de la evolución del proyecto.
- El adjudicatario deberá realizar revisiones periódicas del avance de actividades, identificar desviaciones y aplicar medidas correctoras en tiempo oportuno.

b) Coordinación y gobernanza operativa:

- El adjudicatario deberá organizar reuniones de seguimiento con la Agencia, con una periodicidad mínima mensual, para revisar el progreso, resolver incidencias y compartir avances clave.
- El adjudicatario deberá participar en los comités o sesiones de seguimiento que convoque la Agencia, incluyendo aquellas destinadas a la validación de contenidos, revisión de eventos o resolución de incidencias.
- El adjudicatario deberá redactar y entregar actas y documentación derivada de todas las reuniones de coordinación.

c) Coordinación técnica transversal:

- El adjudicatario deberá gestionar de manera integral los entornos digitales comunes, incluidos los sistemas de inscripción, seguimiento de usuarios, comunicación con participantes, generación de certificados, consolidación de métricas y las plataformas técnicas vinculadas al servicio.
- El adjudicatario deberá revisar y homologar los estándares técnicos aplicables en estos entornos digitales, herramientas de evaluación y materiales audiovisuales.

d) Apoyo a la comunicación institucional:

- El adjudicatario deberá apoyar a la Agencia en la definición de mensajes clave, campañas de difusión y contenidos visuales transversales para la promoción del programa formativo y de los eventos prácticos.
- El adjudicatario deberá elaborar materiales institucionales de presentación del servicio para sesiones informativas, notas de prensa o difusión interna en las organizaciones participantes.

Todas estas funciones deberán prestarse de forma continua durante todo el periodo de ejecución del contrato y estarán sujetas a la validación y supervisión de la Agencia de Ciberseguridad, quien podrá requerir ajustes metodológicos o refuerzos operativos en función de la evolución del servicio.

4.2.1 Entregables transversales

Con el fin de garantizar la coherencia, trazabilidad y supervisión global del proyecto, el adjudicatario deberá entregar la siguiente documentación mínima:

Entregable		Plazo de entrega	Requisitos y observaciones
T1	Plan de Trabajo Global del Servicio	15 días	Incluirá cronograma consolidado, hitos principales, responsables, dependencias y entregables previstos. Será la referencia de coordinación global, deberá ser aprobado por la Agencia y mantenerse actualizado periódicamente

Entregable		Plazo de entrega	Requisitos y observaciones
			durante toda la ejecución.
T2	Informe de Avance Mensual	≥1 semana antes de cada reunión mensual de seguimiento	Incluirá consolidación de progreso, análisis de desviaciones, medidas correctoras, estado de cumplimiento de hitos e indicadores de servicio. Deberá incorporar un resumen ejecutivo de 1–2 páginas que permita la elevación de resultados a instancias superiores.
T3	Actas de Reuniones de Seguimiento	Tras cada reunión (≥ mensual)	Recogerán asistentes, acuerdos, incidencias y medidas correctoras. Se entregarán en un plazo máximo de 5 días hábiles tras cada reunión.

CLÁUSULA 5.- EQUIPO Y LUGAR DE TRABAJO

5.1 Composición orientativa del equipo

El presente expediente no impone la adscripción de un equipo concreto ni de perfiles específicos. No obstante, a efectos de estimación del presupuesto base de licitación, se ha tomado como referencia un esfuerzo global orientativo distribuido entre distintos perfiles profesionales, representativos de las capacidades técnicas y funcionales necesarias para la correcta ejecución del servicio.

Dicha estimación tiene carácter meramente orientativo y no genera obligación contractual alguna para el licitador, quien podrá configurar libremente el equipo y los recursos personales que considere adecuados para el cumplimiento de las prestaciones. En todo caso, el adjudicatario será plenamente responsable de asegurar el cumplimiento de los niveles de calidad, plazos y entregables establecidos en los pliegos.

Con el objetivo de facilitar la comprensión de las capacidades previstas, el apartado siguiente incluye una relación descriptiva de perfiles considerados en la estimación económica (reflejada en la memoria justificativa), junto con su dedicación orientativa para el servicio. Esta información no tiene carácter vinculante, no constituye exigencia de solvencia ni supone composición obligatoria del equipo de trabajo.

5.2 Perfiles profesionales y dedicación

A continuación, se presenta una tabla resumen con los perfiles profesionales y la dedicación orientativa en el periodo de 6 meses (contrato mínimo o en cada una de las dos posibles prórrogas). Esta distribución responde a un modelo de referencia no obligatorio, utilizado en la estimación económica del presupuesto base.

Este modelo tiene carácter orientativo y busca ilustrar las capacidades técnicas y funcionales necesarias para la ejecución del contrato.

Perfil	Horas	Funciones	Solvencias
P1 – Jefe/a de Proyecto	156	Dirección global del servicio. Coordinación de planificación, interlocución principal con la Agencia, seguimiento de hitos y entregables (E1–E9 y T1–T3). Supervisión de la calidad de los materiales y metodologías, gestión de riesgos y resolución de incidencias estratégicas. Validación final de informes intermedios y finales.	Titulación superior. ≥8 años en gestión de proyectos TIC o ciberseguridad. Experiencia en proyectos con sector público.
P2 – Consultor Funcional Senior	585	Asesoramiento metodológico en dinámicas formativas. Diseño pedagógico	Titulación superior. ≥5 años en proyectos de formación y

Perfil	Horas	Funciones	Solvencias
		de hackathones, ciberejercicios, campañas de phishing y sesiones temáticas. Definición de fichas técnicas (E2) y materiales ejecutivos para sesiones de alta dirección. Coordinación con expertos sectoriales para la validación de actividades.	concienciación en ciberseguridad.
P3 – Especialista en Tecnologías Emergentes de Ciberseguridad	70	Diseño y desarrollo de contenidos y sesiones especializadas en tecnologías emergentes (IA, IoT sanitario, cloud, blockchain, dispositivos médicos). Identificación de casos de uso aplicables al sector sanitario y al ámbito de las entidades locales. Soporte en la elaboración de dossiers digitales y actualización de referencias técnicas.	Titulación superior en Ingeniería, Telecomunicaciones o similar. ≥3 años en proyectos de seguridad tecnológica avanzada en IA, IoT sanitario, cloud o dispositivos médicos.
P4 – Diseñador/a Gráfico	112	Creación de materiales gráficos y multimedia: infografías, maquetación de contenidos, banners, material para landing pages y campañas de difusión. Adaptación de los mensajes a distintos canales de comunicación. Soporte en materiales visuales para hackathones, ciberejercicios y sesiones ejecutivas.	Formación en diseño gráfico/multimedia. ≥2 años en proyectos de formación digital.
P5 – Especialista en Ciberseguridad y Compliance Normativo	342	Validación técnica y normativa de actividades. Asesoramiento en ENS, NIS2, CER, RGPD y buenas prácticas. Verificación de cumplimiento en campañas de phishing (anonimización, DPIA/IAE). Apoyo en sesiones temáticas y de alta dirección con foco regulatorio.	Certificación tipo CISSP, CISM o similar. ≥3 años en seguridad TIC, preferible en sector público.
P6 – Auxiliar de comunicación	214	Atención y soporte a participantes en entornos simulados o eventos.	Ciclo formativo. ≥2 años en soporte técnico a usuarios.
P7 – Responsable de Evaluación e Indicadores	152	Definición de métricas de resultado. Seguimiento de KPIs de participación, impacto y satisfacción. Elaboración de informes de evaluación para cada actividad y consolidados intermedios/finales. Diseño de cuadros de mando de indicadores.	Titulación superior. ≥3 años en evaluación de programas formativos o de ciberseguridad.
P8 – Responsable de Comunicación y Dinamización	246	Diseño y ejecución de campañas de comunicación. Gestión de materiales de difusión (E4). Dinamización activa en hackathones, ciberejercicios y sesiones formativas. Facilitación de interacciones en sesiones de alta dirección. Coordinación con diseñadores y técnicos audiovisuales para asegurar un enfoque atractivo y participativo.	Titulación en comunicación o marketing. ≥3 años en campañas digitales.
P9 – Técnico Audiovisual	44	Producción y soporte audiovisual en eventos híbridos. Grabación, retransmisión y edición de sesiones. Preparación de recursos audiovisuales para materiales de sensibilización.	Formación técnica. ≥2 años en edición audiovisual en entornos digitales.

Perfil	Horas	Funciones	Solvencias
		Garantía de accesibilidad y compatibilidad con sistemas corporativos.	
P10 – Arquitecto de Escenarios	184	Diseño técnico de entornos simulados para hackathones y ciberejercicios. Definición de roles, guiones y cronogramas de incidentes. Integración de requisitos pedagógicos y técnicos en los entornos de simulación.	Titulación técnica. ≥5 años en diseño de ejercicios de ciberseguridad.
P11 – Especialista Red Team / Ciberataques Controlados	96	Diseño de retos ofensivos (CTF, explotación de vulnerabilidades, ingeniería inversa). Configuración de entornos vulnerables. Soporte a scoring automatizado y pruebas ofensivas en hackathones y ciberejercicios.	Certificación OSCP, CRTP, etc. ≥3 años en ejercicios Red Team.
P12 – Especialista Blue Team / Defensa	110	Diseño de dinámicas defensivas en ciberejercicios. Monitorización de respuestas técnicas, análisis de incidentes simulados y evaluación de coordinación defensiva. Apoyo en lecciones aprendidas.	Certificación GCIH, GCIA, etc. ≥2 años en operación de SOCs.
P13 – Responsable de Ciberejercicio / Facilitador Senior	486	Dirección integral de cada ciberejercicio: coordinación entre roles técnicos, organizativos y de dirección. Facilitación de la dinámica, improvisación ante incidencias, y gestión de la retroalimentación inmediata (“hot wash-up”).	≥5 años en dirección de ciberejercicios o ejercicios de crisis.
P14 – Técnico Despliegues	144	Despliegue de entornos simulados en cloud y redes virtuales. Configuración de plataformas de simulación de phishing, provisionamiento de máquinas virtuales y soporte en entornos híbridos. Soporte técnico durante los eventos.	Experiencia en infraestructuras TI. ≥3 años en despliegue de plataformas y redes virtuales.

2.941

5.3 Lugar de trabajo

El desarrollo del servicio se realizará, con carácter general, en las instalaciones del adjudicatario, quien será plenamente responsable de la organización de los trabajos en dichos espacios. En todo caso, deberá garantizarse el cumplimiento de los requisitos técnicos, de calidad, de coordinación y de seguridad establecidos en el presente contrato.

No obstante, determinadas actividades deberán ejecutarse obligatoriamente de forma presencial en las dependencias de la Agencia de Ciberseguridad o en otras ubicaciones institucionales designadas por esta, en la medida en que impliquen interacción directa con personal institucional, usuarios destinatarios o responsables de validación, así como aquellas que conlleven dinámicas participativas. En particular:

- **Sesión inicial de planificación:** Se celebrará al menos una reunión presencial de arranque para la definición conjunta del alcance operativo, cronograma de actividades, canales de comunicación y responsables de cada línea de trabajo.

- **Sesiones de validación funcional y pedagógica:** Determinados hitos de diseño instruccional, la definición de dinámicas o la adaptación de contenidos requerirán validación conjunta con la Agencia, lo cual podrá implicar reuniones presenciales específicas.
- **Hackathones y ciberejercicios:** Los ejercicios se desarrollarán de forma presencial, aunque puedan incorporar componentes virtuales. El adjudicatario deberá desplazarse a los espacios indicados por la Agencia, colaborar en la logística del evento y asistir a la coordinación con observadores, formadores y participantes.
- **Sesiones de formación a alta dirección:** Estas sesiones serán estrictamente presenciales, realizándose en centros de la administración regional o local designados por la Agencia.
- **Sesiones temáticas especializadas:** Aunque podrán impartirse en modalidad híbrida, se prevé que una parte significativa de ellas se desarrolle de forma presencial para facilitar la interacción directa y las dinámicas participativas.
- **Sesiones de lecciones aprendidas y transferencia de conocimiento:** Las actividades de cierre, presentación de resultados o talleres internos de sistematización podrán requerir presencialidad, según determine la Agencia.

Asimismo, la Agencia podrá convocar reuniones presenciales adicionales de seguimiento, coordinación o presentación de avances en cualquier fase del proyecto. El adjudicatario deberá mostrar plena disponibilidad para atender estos requerimientos, sin que ello suponga incremento en el precio del contrato.

CLÁUSULA 6.- TECNOLOGÍAS Y HERRAMIENTAS A UTILIZAR

6.1 Entornos de simulación, virtualización y despliegue de ejercicios

Para la correcta ejecución de los hackathones y ciberejercicios contemplados en este contrato, el adjudicatario deberá desplegar entornos técnicos diseñados expresamente para cada evento, utilizados únicamente durante su desarrollo y eliminados de forma segura al finalizar, asegurando la supresión completa de datos, configuraciones y accesos.

Se distinguen dos grandes tipos de entornos, según la naturaleza del evento:

a) Entornos para Hackathones:

- Deberá habilitarse un entorno colaborativo digital que permita edición, desarrollo, compartición de código e integración de herramientas de prueba o demostración.
- Cada grupo participante deberá disponer de un espacio lógico propio, aislado del resto y con privilegios diferenciados.
- El acceso deberá realizarse prioritariamente mediante interfaz web segura, sin instalación de software adicional por los participantes.
- Cuando se propongan retos técnicos, deberán proporcionarse entornos de prueba controlados, con capacidad de restauración automática, monitorización de red y registros de actividad (logs).
- El entorno deberá permitir escalar recursos en función de la participación, soportando de forma concurrente al menos a decenas de equipos en paralelo.

b) Entornos para Ciberejercicios:

- Deberán proporcionarse entornos realistas tipo Red/Blue Team, con sistemas vulnerables, redes segmentadas, monitorización de logs y mecanismos de scoring.

- Deberán permitir la configuración de distintos roles de participantes con permisos diferenciados (defensores, atacantes, observadores, facilitadores), incluyendo sistemas de mensajería o coordinación entre ellos.
- Deberán posibilitar la simulación híbrida (técnico-organizativa), con integración de documentos, comunicaciones ficticias, toma de decisiones estratégicas y roles ejecutivos simulados.
- Deberán registrar todas las interacciones realizadas, identificar las respuestas adoptadas, los errores cometidos y los tiempos de reacción.

Las condiciones generales aplicables a todos los entornos son las siguientes:

- Los entornos deberán ser exclusivos de cada ejercicio, con vida útil limitada y eliminación segura al cierre.
- Los accesos deberán ser individualizados y trazables, con registros completos de actividad para fines de auditoría.
- La Agencia de Ciberseguridad podrá revisar previamente los entornos, establecer condiciones de despliegue y requerir informes técnicos posteriores al ejercicio como parte de los entregables (E3).
- Se admitirán entornos desplegados en infraestructura cloud gestionada por el adjudicatario o en instalaciones físicas específicas, siempre que se garantice su operatividad, seguridad, adaptabilidad y el aislamiento total respecto a redes corporativas o de producción.

6.2 Herramientas de dinamización, puntuación y evaluación

Durante la ejecución de los hackathones y ciberejercicios incluidos en este contrato, el adjudicatario deberá aportar herramientas específicas que garanticen la participación activa, la monitorización objetiva de las actividades y la evaluación integral del rendimiento de los equipos y participantes.

a) Herramientas de dinamización y comunicación:

- Deberán garantizar la interacción fluida de los participantes en todo el evento, ya sea presencial, virtual o híbrido, sin requerir configuraciones complejas.
- Deberán ofrecer salas virtuales segmentadas por equipos o roles, paneles informativos centralizados con retos, avisos y materiales de apoyo, sistemas de mensajería o canales temáticos para resolver dudas y gestionar incidencias.
- Deberán incluir mecanismos básicos de gamificación (insignias, niveles, reconocimientos simbólicos) que refuercen la motivación y el dinamismo de la actividad.

b) Herramientas de puntuación y scoring técnico:

- Deberán permitir la evaluación objetiva y en tiempo real del desempeño de los equipos mediante sistemas automatizados que registren y validen la resolución de retos o fases del ejercicio con tokens, banderas o eventos definidos.
- Deberán establecer criterios de valoración como tiempo de resolución, calidad de la respuesta o progresión alcanzada, mostrando un panel de puntuación dinámico y transparente accesible a equipos y coordinadores.
- Deberán posibilitar la personalización de retos y métricas según los objetivos del ejercicio y los perfiles participantes.
- Los resultados deberán poder exportarse en formato editable para su integración en los entregables de evaluación (E7, E8 y E9).

c) Herramientas de evaluación cualitativa y analítica:

- Deberán facilitar un análisis integral de la actividad, incluyendo la recogida de feedback estructurado a través de encuestas digitales.
- Deberán permitir el estudio del desempeño organizativo y conductual de los equipos mediante observación estructurada o registros de decisiones.
- Deberán generar informes individuales y globales con resultados, incidencias y áreas de mejora.
- Deberán garantizar la trazabilidad de la participación y la actividad de cada integrante, preservando la privacidad y la igualdad entre participantes.
- Todos los informes deberán entregarse en formato editable y alineados con los entregables documentales E7 y E9.

6.2.1 Requisitos de conectividad e infraestructura

Los hackathones y ciberejercicios podrán realizarse en modalidad presencial o híbrida. El adjudicatario deberá garantizar la infraestructura necesaria para su correcto desarrollo técnico y para ofrecer una experiencia satisfactoria a todos los perfiles participantes.

a) Infraestructura física y tecnológica mínima:

- Los espacios presenciales serán facilitados por la Agencia de Ciberseguridad u otras instituciones colaboradoras.
- Deberán incluir puestos de trabajo adecuados, acceso a red eléctrica suficiente, conectividad institucional (cable o Wi-Fi) y medios básicos de presentación (pantallas, proyectores, audio).
- El adjudicatario deberá realizar una revisión técnica previa para verificar requisitos, detectar limitaciones y coordinar ajustes con el equipo técnico de la Administración

b) Equipamiento específico de eventos:

- El adjudicatario será responsable de proporcionar, desplegar y retirar la infraestructura técnica temporal requerida, que incluirá servidores, estaciones de trabajo, dispositivos de red dedicados, nodos de virtualización, sistemas de respaldo, pantallas adicionales, elementos de señalización y recursos materiales complementarios (credenciales, hojas de puntuación, blocs).
- Todo el equipamiento deberá estar disponible únicamente durante el evento y desmontarse al finalizar.

c) Requisitos para la participación remota:

- En eventos híbridos el adjudicatario deberá asegurar un sistema de streaming profesional, con calidad de audio e imagen, para retransmitir sesiones clave.
- Deberá instalar medios audiovisuales adecuados (cámaras, microfonía, sistemas de mezcla y codificación en tiempo real).
- Deberá gestionar plataformas digitales de participación con soporte técnico en tiempo real y funcionalidades de interacción (chat, encuestas, turnos de palabra).

6.2.2 Requisitos de ciberseguridad para entornos prácticos y de simulación

Todos los entornos, herramientas y plataformas empleados en hackathones y ciberejercicios deberán cumplir condiciones mínimas de seguridad, garantizando la integridad del evento, la protección de la información y la seguridad de los participantes.

a) Aislamiento y control del entorno:

- Los entornos deberán estar totalmente aislados de redes corporativas y sistemas de producción.
- Deberán ejecutarse en infraestructuras independientes (virtuales o físicas) y permitir pruebas controladas sin riesgo de propagación.
- El acceso deberá limitarse a participantes y técnicos autorizados mediante autenticación robusta.

b) Gestión del ciclo de vida del entorno:

- Cada entorno deberá desplegarse exclusivamente para el ejercicio correspondiente y eliminarse al finalizar, sin continuidad posterior.

c) Protección de la información y supervisión:

- La información generada deberá cifrarse en tránsito y en reposo cuando sea almacenada temporalmente.
- Los datos deberán ser ficticios y anonimizados, sin correspondencia con usuarios o entidades reales.
- Al cierre del evento, el adjudicatario deberá garantizar la eliminación segura de máquinas virtuales, usuarios, datos y configuraciones, evitando persistencia de información sensible.

d) Seguridad ofensiva y defensiva controlada:

- Los retos Red Team deberán limitar el alcance de los ataques simulados para no comprometer la estabilidad del entorno.
- Se prohíbe el uso de herramientas no controladas o que introduzcan vulnerabilidades reales.
- Los escenarios defensivos deberán permitir la evaluación de respuestas técnicas sin exponer a riesgos innecesarios a los participantes.

6.2.3 Herramientas de apoyo para campañas de entrenamiento de phishing

El adjudicatario deberá proporcionar herramientas específicas para la planificación, ejecución y evaluación de campañas de simulación de phishing (correo electrónico, SMS y llamadas telefónicas), orientadas a reforzar la capacidad de detección y respuesta de los participantes. Deberán atenderse los siguientes requisitos:

a) Diseño y personalización de campañas:

- La plataforma deberá permitir la creación de campañas adaptadas al contexto organizativo, con plantillas configurables de correos electrónicos, mensajes SMS y guiones de llamadas telefónicas simuladas.
- Deberá ofrecer distintos niveles de dificultad y realismo.

b) Gestión de participantes y segmentación:

- La herramienta deberá posibilitar la selección de colectivos específicos, garantizando la trazabilidad de los envíos y la segregación de resultados por grupo.

c) Ejecución controlada y segura:

- Las campañas deberán ejecutarse en un entorno controlado, evitando cualquier riesgo real para los sistemas de la organización.
- Los enlaces o adjuntos utilizados deberán ser simulados e inofensivos, sin exposición a amenazas externas.

d) Medición y retroalimentación:

- La herramienta deberá registrar métricas clave (tasas de apertura, clics, descargas, respuestas a simulaciones).
- Deberá generar informes detallados de resultados individuales y agregados.
- Deberá proporcionar retroalimentación inmediata y formativa a los usuarios que interactúen con las simulaciones.

e) Cumplimiento legal y protección de datos:

- El diseño y ejecución de las campañas deberá respetar el marco normativo vigente en protección de datos y relaciones laborales.
- Los informes globales deberán garantizar anonimización de resultados.
- El acceso a resultados individuales quedará restringido a responsables expresamente autorizados.

6.3 Requisitos transversales de soporte y mantenimiento

El adjudicatario deberá garantizar un soporte técnico transversal adaptado a la naturaleza de las actividades contempladas en este contrato, limitado a la resolución de incidencias críticas que puedan comprometer la operatividad de los entornos, herramientas o servicios durante su preparación, ejecución o cierre.

En particular:

- En los hackathones y ciberejercicios, el soporte deberá cubrir toda la fase de preparación, ejecución y cierre, incluyendo la resolución de incidencias técnicas puntuales que puedan impedir el normal desarrollo del evento.
- En las campañas de phishing, el soporte deberá garantizar la correcta ejecución de los envíos, la monitorización en tiempo real de incidencias y la validación de resultados generados por las herramientas de simulación.
- En las sesiones de formación a alta dirección y sesiones temáticas especializadas, el soporte deberá asegurar la disponibilidad y funcionamiento de los medios audiovisuales, plataformas digitales y materiales de apoyo necesarios.

De forma general, el adjudicatario deberá:

- Habilitar un punto de contacto técnico único para la gestión de incidencias sobre las tecnologías y herramientas utilizadas.
- Registrar todas las actuaciones realizadas, incluyendo descripción de la incidencia, tiempos de resolución y responsables intervinientes.
- Emitir un informe de cierre en caso de intervención, que describa la incidencia, su impacto y la solución aplicada.

CLÁUSULA 7.- MODELO DE GESTIÓN DEL SERVICIO**7.1 Gobernanza y actores clave**

El modelo de gestión del servicio se articula en torno a un esquema de gobernanza ágil, colaborativo y orientado a resultados, que asegure la adecuada planificación, ejecución, supervisión y validación técnica de las actividades contempladas en este contrato. Se definen los siguientes actores y responsabilidades:

- **Dirección del contrato (Agencia de Ciberseguridad):** Ejercerá la supervisión general, la validación de entregables y la resolución de incidencias estratégicas. Entre sus funciones se incluyen la aprobación del plan de trabajo y cronograma, la validación de productos e hitos clave, la aprobación de ajustes al modelo cuando proceda, la resolución de controversias y la evaluación del desempeño del adjudicatario mediante indicadores.
- **Coordinación técnica del contrato (Agencia de Ciberseguridad):** Asumida por un/a coordinador/a designado/a como punto de contacto operativo y canal formal de interlocución. Sus funciones abarcan la supervisión continua de los trabajos, la revisión de entregables intermedios, la coordinación con áreas u organismos implicados, el seguimiento de indicadores de calidad y la convocatoria de reuniones de seguimiento.
- **Dirección del proyecto (Adjudicatario):** Responsabilidad del perfil P1 (Jefe/a de Proyecto), definido en la cláusula 5.2, que actuará como responsable último de la ejecución de los trabajos. Deberá contar con experiencia acreditada en gestión de servicios complejos en ciberseguridad y formación. Sus funciones incluyen la dirección global del proyecto, la coordinación interna de los equipos, la elaboración de informes periódicos, la gestión de incidencias operativas y la representación del adjudicatario ante la Agencia y en el Comité de Seguimiento.
- **Comité de Seguimiento:** Se reunirá al menos mensualmente y con carácter extraordinario cuando sea necesario. Estará integrado por representantes de la Agencia (Dirección del contrato y Coordinación técnica) y del adjudicatario (perfil P1 y otros perfiles cuando corresponda). Sus funciones comprenden la revisión del estado de ejecución, el seguimiento de hitos e indicadores, la identificación de desviaciones y medidas correctoras, la aprobación de cambios menores en el plan de trabajo y la canalización formal de incidencias y propuestas.

7.2 Planificación, cronograma y fases

La ejecución del contrato se estructura en fases adaptadas a la naturaleza y tipología de las actividades previstas, asegurando una gestión ordenada, la validación progresiva de entregables y el cumplimiento de los compromisos técnicos y temporales.

El adjudicatario deberá presentar un **Plan de Trabajo Global del Servicio** en un plazo máximo de quince (15) días naturales desde la formalización del contrato, detallando hitos, tareas y entregables asociados a cada fase. Dicho plan será validado por la Agencia de Ciberseguridad y tendrá carácter vinculante. Cualquier modificación sustancial del cronograma o de la secuencia de fases deberá ser justificada por el adjudicatario y aprobada por la Agencia.

El contrato tendrá una duración inicial de seis (6) meses, prorrogables hasta dos (2) veces por idéntico periodo, y se desarrollará en cuatro fases principales:

- **F1. Planificación y diseño de actividades** (Mes 1): elaboración del calendario general, definición de objetivos pedagógicos y técnicos, identificación de perfiles destinatarios, diseño de retos y escenarios, validación de dinámicas de campañas de phishing y sesiones temáticas, y coordinación logística.
- **F2. Preparación técnica y logística** (Meses 1–2): configuración de entornos virtuales y simulados, habilitación de herramientas de evaluación y scoring, preparación de materiales de comunicación y soporte, y pruebas técnicas de conectividad e infraestructura.
- **F3. Ejecución de actividades** (Meses 2–5): desarrollo de las 39 actividades previstas (hackathons, ciberejercicios, campañas de phishing, sesiones de alta dirección y sesiones temáticas especializadas), con gestión operativa, asistencia técnica en tiempo real y generación de dossiers post-evento.
- **F4. Evaluación y cierre** (Mes 6): análisis del impacto formativo y organizativo, sistematización de buenas prácticas, consolidación de métricas e indicadores, sesiones de lecciones aprendidas y entrega del informe final consolidado.

Estas fases constituyen el marco de referencia para la planificación operativa del contrato y estarán directamente vinculadas con los hitos técnicos y entregables definidos en las cláusulas 4.3 y 11.2.

7.3 Comunicación y reporte

El adjudicatario deberá garantizar un modelo de comunicación ágil, transparente y documentado con la Agencia de Ciberseguridad, que asegure el seguimiento continuo del servicio, la resolución temprana de incidencias y la toma de decisiones informada.

Como obligaciones mínimas de reporte se establecen las siguientes:

- Informe inicial de planificación y arranque, con el Plan de Trabajo Global del Servicio validado por la Agencia.
- Informes ejecutivos de avance, emitidos al cierre de cada fase definida en la planificación (F1–F4).
- Actas de reuniones de coordinación, que reflejen asistentes, acuerdos alcanzados, tareas asignadas y próximos pasos.
- Alertas inmediatas sobre riesgos, desviaciones o decisiones críticas, acompañadas de la correspondiente propuesta de actuación o mitigación.

El adjudicatario será responsable de mantener documentación completa, estructurada y actualizada de todos los entregables, versiones intermedias y elementos relevantes, utilizando los entornos colaborativos o canales designados por la Agencia. Las comunicaciones oficiales se realizarán siempre a través del correo institucional.

Asimismo, la Agencia podrá requerir la participación del adjudicatario en reuniones de seguimiento, comités de coordinación o sesiones técnicas, tanto periódicas como puntuales, sin que ello suponga coste adicional para la Administración.

CLÁUSULA 8.- GESTIÓN DE LA SEGURIDAD

8.1 Confidencialidad y uso de la información

El adjudicatario deberá mantener la más estricta confidencialidad respecto a toda la información a la que acceda como consecuencia de la ejecución del contrato, comprometiéndose a no divulgarla, reproducirla ni utilizarla para fines distintos de los contemplados en el mismo. Esta obligación se extenderá a toda la documentación, datos, sistemas o conocimientos generados o compartidos durante la ejecución del contrato, y continuará vigente tras su finalización, con carácter indefinido salvo autorización expresa y por escrito de la Agencia de Ciberseguridad.

8.2 Cumplimiento del ENS y normativa de protección de datos

El adjudicatario se compromete a cumplir en todo momento con las exigencias del Esquema Nacional de Seguridad (ENS), en la categoría que corresponda a los sistemas utilizados, así como con la normativa vigente en materia de protección de datos personales, en especial el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD), junto con cualquier otra disposición normativa aplicable a los servicios prestados.

Cuando proceda, el adjudicatario asumirá la condición de encargado del tratamiento, de conformidad con lo establecido en la normativa de protección de datos, y suscribirá el correspondiente acuerdo de encargo del tratamiento con la Agencia de Ciberseguridad.

8.3 Obligaciones del personal del contratista

Todo el personal del adjudicatario que intervenga en la ejecución del contrato deberá ser informado de manera expresa y fehaciente sobre las obligaciones relativas a la confidencialidad, el uso

responsable de la información, el cumplimiento del ENS y la protección de datos personales, y, cuando proceda, recibir formación específica y actualizada al respecto. El adjudicatario será responsable de que todo su personal actúe de conformidad con estos principios y responderá ante cualquier incumplimiento o actuación negligente.

El adjudicatario deberá asegurar que cualquier acceso a sistemas, plataformas o documentación sensible se realice exclusivamente por parte del personal autorizado y dentro del marco de sus funciones asignadas, manteniendo un registro actualizado de accesos y autorizaciones.

8.4 Medidas específicas de protección de la documentación

Toda la documentación generada en el marco del contrato tendrá la consideración de propiedad exclusiva de la Agencia de Ciberseguridad, y deberá almacenarse, transmitirse y conservarse mediante medios que garanticen su integridad, disponibilidad y confidencialidad. En particular:

- La transmisión de información sensible deberá realizarse a través de canales cifrados o sistemas equivalentes de comunicación segura que eviten accesos no autorizados.
- Los sistemas utilizados por el adjudicatario deberán contar con medidas técnicas y organizativas proporcionales al nivel de sensibilidad de la información tratada.
- La destrucción o devolución de documentación al finalizar el contrato se realizará conforme a las indicaciones de la Agencia de Ciberseguridad, garantizando que no persista información residual en sistemas o dispositivos del adjudicatario, mediante procedimientos de borrado seguro o destrucción certificada.

8.5 Notificación de incidentes de seguridad

El adjudicatario deberá notificar de forma inmediata a la Agencia de Ciberseguridad cualquier incidente de seguridad que afecte o pueda afectar a la confidencialidad, integridad, disponibilidad o trazabilidad de la información, sistemas o servicios objeto del contrato. Esta obligación incluye tanto los incidentes detectados directamente por el adjudicatario como aquellos comunicados por terceros que puedan tener impacto en la prestación del servicio.

La notificación deberá realizarse en un plazo máximo de veinticuatro (24) horas desde la detección inicial del incidente, proporcionando al menos la siguiente información mínima: descripción detallada del incidente, alcance potencial, sistemas o datos afectados, medidas adoptadas de forma inmediata y previsión de actuaciones de contención, mitigación o recuperación.

Asimismo, el adjudicatario se compromete a colaborar plenamente en la investigación, análisis y resolución de los incidentes, adoptando de forma diligente las medidas correctoras y preventivas que le sean indicadas por la Agencia. Una vez resuelto el incidente, deberá entregar un informe final de cierre, que recoja las causas, el impacto real, las acciones correctoras aplicadas y las recomendaciones de mejora para evitar su repetición.

CLÁUSULA 9.- DERECHOS Y OBLIGACIONES

9.1 Obligaciones del contratista

El contratista deberá ejecutar el contrato conforme a los términos establecidos en los pliegos, con la debida diligencia profesional, respetando plazos, entregables, niveles de calidad y requisitos técnicos comprometidos. Asimismo, deberá colaborar activamente con la Agencia de Ciberseguridad y con cualquier otro agente designado por el órgano de contratación en el seguimiento del servicio, la resolución de incidencias y la atención a requerimientos razonables derivados de su correcta ejecución.

9.2 Derechos del órgano de contratación

La Agencia de Ciberseguridad podrá supervisar en todo momento el desarrollo del servicio, requerir aclaraciones o documentación adicional, y proponer ajustes razonables en la planificación, siempre que no alteren sustancialmente el objeto del contrato ni supongan modificación de los elementos esenciales del mismo. Igualmente, podrá rechazar entregables que no se ajusten a lo previsto en los pliegos, exigiendo su corrección sin coste adicional para la Administración.

9.3 Propiedad de los resultados y derechos de uso

Todos los materiales, desarrollos, configuraciones, contenidos formativos, documentación técnica, entornos virtuales, recursos audiovisuales, informes y cualquier otro elemento generado en la ejecución del contrato serán de titularidad exclusiva de la Comunidad de Madrid, a través de la Agencia de Ciberseguridad.

El contratista no podrá reproducir, reutilizar, distribuir ni divulgar total o parcialmente dichos materiales sin autorización expresa y previa por escrito de la Agencia, quedando prohibido su uso con fines promocionales, comerciales, académicos o de portafolio. Se exceptúan los elementos de dominio público o aquellos expresamente excluidos en los pliegos.

9.4 Licenciamiento, formatos y reutilización institucional

Los materiales generados deberán entregarse con licencia de uso que permita su reutilización gratuita con fines institucionales, docentes o divulgativos no comerciales, bajo condiciones de atribución y compartición en los mismos términos.

El adjudicatario se compromete a no incorporar componentes, plantillas o software sujetos a restricciones incompatibles con este régimen de reutilización, y garantizará que los recursos se entregan, en la medida de lo posible, en formatos abiertos, estandarizados y editables.

La Agencia podrá emplear, adaptar, traducir, divulgar o redistribuir libremente dichos materiales, sin que ello genere compensación adicional para el adjudicatario.

9.5 Responsabilidad frente a terceros

El contratista será el único responsable frente a terceros de los daños que puedan derivarse de su actuación en la ejecución del contrato, incluyendo los ocasionados por personal propio, subcontratado o vinculado. La Agencia de Ciberseguridad quedará plenamente exonerada de cualquier reclamación derivada de dichos actos.

CLÁUSULA 10.- CALIDAD DEL SERVICIO

Los criterios y estándares de calidad definidos en este apartado se considerarán de obligado cumplimiento a efectos del artículo 192 de la LCSP y servirán de referencia para la aceptación o rechazo de los entregables, así como para la aplicación de penalidades.

10.1 Criterios de calidad de los entregables

Todos los entregables deberán cumplir con los estándares técnicos, funcionales y formales definidos en los pliegos, ajustarse al marco institucional de la Consejería de Digitalización y demostrar una aplicabilidad práctica y una utilidad efectiva para los fines previstos.

Se valorará especialmente la claridad expositiva, la corrección técnica, la adecuación de los contenidos al público objetivo y el cumplimiento riguroso de los requisitos de interoperabilidad, accesibilidad y ciberseguridad establecidos. Los entregables deberán presentarse en formatos abiertos y editables, con estructura coherente, documentación de soporte y control de versionado.

Cualquier entregable que presente carencias significativas en su estructura, calidad técnica o utilidad práctica podrá ser rechazado por el órgano de seguimiento del contrato. Si no es subsanado

en el plazo de diez (10) días hábiles desde la notificación formal, se podrá aplicar la penalidad correspondiente, conforme a lo dispuesto en el Pliego de Cláusulas Administrativas Particulares.

10.2 Validación técnica de resultados

La validación técnica de los resultados corresponderá a la Agencia de Ciberseguridad de la Comunidad de Madrid, quien podrá contar con apoyo de personal técnico propio o designado. Esta validación se basará en:

- La verificación del cumplimiento de los requisitos técnicos y funcionales establecidos para cada entregable.
- La evaluación de la calidad técnica, aplicabilidad, accesibilidad y alineación con los objetivos del contrato.
- La consistencia metodológica y el respeto a las fases y cronograma validados.

El proceso podrá incluir reuniones de contraste, requerimientos de mejora o solicitudes de aclaración. En caso de incumplimiento reiterado o retrasos injustificados, se podrán adoptar medidas correctoras o aplicar las penalizaciones previstas en el PCAP.

10.3 Indicadores de calidad y mejora continua

Durante la ejecución del contrato, se emplearán indicadores básicos para el seguimiento de la calidad del servicio, entre los que se incluyen:

- Cumplimiento del cronograma aprobado y las fases F1–F4.
- Grado de aceptación de los entregables en primera versión.
- Capacidad de respuesta técnica ante incidencias, solicitudes de mejora y cambios menores.
- Participación y valoración de usuarios finales, en particular en actividades formativas y eventos.
- Impacto operativo medido a través de informes de resultados, métricas de uso y nivel de aprovechamiento.

Estos indicadores serán revisados en los hitos definidos y podrán dar lugar, si procede, a medidas de ajuste del modelo de ejecución o a penalizaciones cuando se superen los umbrales de incumplimiento establecidos. Asimismo, podrán servir de base para identificar oportunidades de mejora continua, que el adjudicatario deberá proponer en los comités de seguimiento.

CLÁUSULA 11.- PLAZOS, DURACIÓN Y ETAPAS

11.1 Duración total del contrato

La duración del contrato será de seis (6) meses, contados a partir de la fecha de formalización y reflejados en el acta de inicio con la Agencia de Ciberseguridad.

El contrato podrá prorrogarse hasta un máximo de dos (2) periodos adicionales de seis (6) meses cada uno, previa autorización expresa y formalización por el órgano de contratación.

11.2 Hitos técnicos

Los hitos técnicos se corresponden con los entregables principales definidos en la Cláusula 4.1.4, que servirán de base para la validación formal de cada fase (F1–F4) y para la activación de los pagos parciales.

La fecha de referencia establecida para el “Plazo de entrega” será la de formalización del contrato, recogida en el acta de inicio.

Cualquier alteración de los plazos establecidos deberá contar con justificación y autorización expresa de la Agencia de Ciberseguridad.

11.3 Plazos de revisión y validación de entregables

Los entregables asociados a cada hito serán evaluados por el equipo técnico de la Agencia de Ciberseguridad en un plazo máximo de diez (10) días hábiles desde su recepción formal.

En caso de requerirse subsanaciones, el contratista dispondrá de un máximo de diez (10) días hábiles adicionales para su corrección y reenvío.

La validación de cada hito será condición necesaria para la aceptación del siguiente y para el reconocimiento del derecho a facturación de las fases correspondientes.

CLÁUSULA 12.- GARANTÍA DE LOS TRABAJOS

12.1 Compromisos de garantía

El adjudicatario garantizará la calidad, funcionalidad, seguridad y adecuación de todos los trabajos, desarrollos y entregables realizados en el marco del contrato durante un periodo de doce (12) meses, contados desde la fecha de recepción formal y conformidad expresa por parte de la Agencia de Ciberseguridad.

12.2 Corrección de deficiencias

Durante el periodo de garantía, el adjudicatario estará obligado a subsanar, sin coste adicional alguno, cualquier error, deficiencia técnica, desviación funcional o incumplimiento de requisitos detectado en los trabajos entregados, siempre que no se deriven de modificaciones normativas sobrevenidas o cambios no imputables a su ejecución.

En caso de requerirse correcciones, el adjudicatario dispondrá de un plazo máximo de diez (10) días hábiles desde la notificación formal para su resolución. El incumplimiento de esta obligación podrá dar lugar a la aplicación de penalidades conforme al régimen previsto en el PCAP.

12.3 Alcance del compromiso de garantía

La obligación de garantía subsistirá con independencia de que el contrato haya finalizado, y se entenderá sin perjuicio de otras responsabilidades legales que puedan derivarse por daños o perjuicios ocasionados por deficiencias imputables al adjudicatario.

El adjudicatario deberá garantizar que todos los entornos de simulación, herramientas técnicas, materiales y recursos entregados mantienen su operatividad básica, integridad y disponibilidad durante el periodo de garantía, incluyendo las configuraciones y adaptaciones realizadas en el marco del presente contrato.

CLÁUSULA 13.- CUMPLIMIENTO NORMATIVO ADICIONAL

13.1 Principio DNSH (Art. 5 Orden HFP/1030/2021)

La empresa adjudicataria deberá respetar los principios de economía circular y evitar impactos negativos en el medio ambiente (DNSH, por sus siglas en inglés, “do no significant harm”) en la ejecución de las actuaciones llevadas a cabo en el marco del PRTR.

13.2 Etiquetado verde y etiquetado digital (Art. 4 Orden HFP/1030/2021)

El contratista estará obligado al preceptivo cumplimiento de las obligaciones asumidas en materia de etiquetado verde y etiquetado digital y los mecanismos establecidos para su control, así como al

preceptivo cumplimiento de las obligaciones asumidas por la aplicación del principio de no causar un daño significativo y las consecuencias en caso de incumplimiento.

El Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia, establece en sus Anexos VI y VII la Metodología de seguimiento para la acción por el clima y la metodología para el etiquetado digital en el marco del Mecanismo, respectivamente. Según estos anexos, el Campo de Intervención 021quinquies – Desarrollo y despliegue de tecnologías, medidas e instalaciones de apoyo en materia de ciberseguridad para los usuarios de los sectores público y privado, contribuye con un 0% al cálculo de la ayuda de los objetivos climáticos y medioambientales, y con un 100% al cálculo de la ayuda a la transición digital.

El Plan de Recuperación, Transformación y Resiliencia, en su componente 15, Programa de Impulso a la Industria de la Ciberseguridad Nacional y en aplicación del Reglamento (UE) 2021/241, recoge que la contribución a la transición ecológica de este componente es de un 0% y a la transición digital de un 100%.

El contrato en tramitación corresponde a la ejecución de la inversión C15.I7, por lo que la contribución a los objetivos de transición ecológica y digital será de un 0% y 100% respectivamente. Con el objetivo de facilitar el seguimiento y evaluación del cumplimiento del compromiso de etiquetado verde y digital, se incorporará al sistema de información y seguimiento la aportación del subproyecto indicado al objetivo fijado.

13.3 Comunicación y publicidad

El artículo 34 del Reglamento Europeo 2021/241 del Parlamento Europeo y del Consejo, por el que se establece el Mecanismo de Recuperación y Resiliencia, recoge que “los perceptores de fondos de la Unión harán mención del origen de esta financiación y velarán por darle visibilidad, incluido, cuando proceda, mediante el uso del emblema de la Unión y una declaración de financiación adecuada que indique “financiado por la Unión Europea – NextGenerationEU”, en particular cuando promuevan las acciones y sus resultados, facilitando información coherente, efectiva y proporcionada dirigida a múltiples destinatarios, incluidos los medios de comunicación y el público”.

En este sentido, el artículo 9 de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia, recoge la necesidad de incorporar el logo oficial del Plan de Recuperación del Reino de España en las iniciativas de comunicación y divulgación de las actuaciones financiadas con cargo al MRR: “Las actuaciones de comunicación relacionadas con la ejecución del Plan incorporarán el logo oficial del Plan de Recuperación, Transformación y Resiliencia del Reino de España, en los términos que se comuniquen por la Autoridad Responsable”. Deberá exhibirse de forma correcta y destacada el emblema de la UE con una declaración de financiación adecuada que diga (traducida a las lenguas locales cuando proceda) “financiado por la Unión Europea - NextGenerationEU”, junto al logo del PRTR.

Para la incorporación del logotipo del Plan de Recuperación, Transformación y Resiliencia (PRTR) elaborado por el Gobierno, se deberá mantener la misma proporción y peso en el tamaño de todos los logotipos. El logo del PRTR irá siempre acompañado de su texto identificativo y del emblema del Gobierno de España. Los logotipos e información de las distintas fuentes de financiación deberán realizarse de manera conjunta y en el orden establecido en el Manual de Identidad Visual del PRTR. En el caso específico del uso del logotipo de la Unión junto con el de INCIBE, ambos deberán mostrarse al menos de forma tan prominente y visible como los otros logotipos. Siendo el logotipo de la UE como mínimo del mismo tamaño, medido en altura y anchura, que el mayor de los demás logotipos. Si se quiere añadir el emblema de la organización, municipio o CCAA beneficiaria de las ayudas, éste también debe ubicarse en la esquina contraria a la de la UE, tener una tipografía y colores distintos y ser más pequeño o, como mucho, del mismo tamaño que el emblema europeo.

CLÁUSULA 14.- CONSULTAS SOBRE EL PLIEGO TÉCNICO

Durante el periodo de presentación de la oferta y, ante cualquier duda o necesidad de aclaración referida a las especificaciones del Pliego de Prescripciones Técnicas, el licitador podrá dirigirse a:


Agencia de Ciberseguridad de la Comunidad de Madrid, **Licita_Agencia_Ciber@madrid.org**

*Área Técnica, Operaciones y Transformación
Ciberseguridad*


Dña. María Isabel González Centenera

Conforme,

*El Consejero Delegado de la Agencia de
Ciberseguridad de la Comunidad de Madrid*


D. Alejandro Las Heras Vázquez