Informe Técnico de Evaluación de Adscripción de Medios Personales

Expediente 063/24

Diseño de competición tipo Capture the Flag para CERTs/CSIRTs Internacionales Ed. 2024

ÍNDICE

1 OBJETO

Este documento recoge la evaluación de la Adscripción de Medios Técnicos y Personales presentada por la empresa Telefónica Soluciones de Informática y Comunicaciones de España, S.A.U en el expediente 063/24: *Diseño de competición tipo Capture the Flag para CERTs/CSIRTs Internacionales Ed. 2024,* en base a lo especificado en el Pliego de Características Generales.

2 REQUISITOS DE ADSCRIPCIÓN DE MEDIOS Y JUSTIFICACIÓN

Requisitos de adscrición de medios técnicos y personales

En el apartado 22.3 del Pliego de Características Generales se indica que el contratista se compromete a presentar la siguiente documentación:

- **Declaración de adscripción de medios**. Se deberá presentar el Anexo debidamente cumplimentado en el que se indique que a la ejecución del servicio:
  - Adscribirá a la ejecución del contrato su propia **organización productiva** y ejecutará el contrato con estricto cumplimiento de las obligaciones que respecto del personal adscrito al mismo incumben al contratista, y que se recogen en la cláusula 11.6, 11.3 y 20.7 del Pliego de Características Generales.
  - Adscribirá al contrato el **personal** adecuado para realizar con garantía las actividades definidas en los pliegos durante todo el periodo de ejecución del proyecto. Los profesionales que sean responsables de la ejecución del trabajo deberán disponer de la cualificación y experiencia necesaria para que se obtengan de forma satisfactoria los trabajos indicados, todo ello en consonancia con lo dispuesto en el Pliego de Características Técnicas. En concreto:

    El equipo de diseño e implementación deberá estar formado por 4 personas, con dedicación estimada a tiempo completo para el diseño e implementación, cuya experiencia profesional, al menos, debe cumplir los siguientes criterios:

    - **Equipo de diseño e implementación de retos:**
      - **Dos perfiles** de analista forense DFIR con cuatro años de experiencia en dicho campo. Análisis técnico de artefactos digitales o adquisición técnica de evidencias digitales en un contexto DFIR. Solo se considerará experiencia aplicable a respuesta a incidentes, y no la de peritaje informático (específica para obtener y custodiar pruebas para procedimientos judiciales).
      - Los **otros Dos perfiles** de experto en tests de penetración con cuatro años de experiencia en dicho campo. Realización de tests de penetración en el contexto de un red team, desarrollo de técnicas de explotación de vulnerabilidades y desarrollo de laboratorios de simulación de sistemas vulnerables

      Todos los perfiles del equipo deberán tener un nivel de inglés equivalente al nivel B2 como mínimo.

    - **Equipo de soporte:**
      - El equipo de soporte deberá de al menos cuatro personas deben como mínimo disponer de la siguiente experiencia profesional.

- El equipo de soporte estará formado por las mismas personas que el equipo de diseño e implementación, y se encargarán de dar soporte a los participantes de la competición durante los días de la ejecución. El licitador podrá aumentar el número de personas que forman parte de este equipo si fuese necesario para dar un correcto soporte en función del número de participantes

- Presentará una declaración de adscripción de medios materiales en relación a la Plataforma, por la cual se compromete a presentar y realizar, en caso de resultar primer clasificado:
  - **Informe de auditoría de seguridad** en los términos descritos en el punto 9.1.1 del Pliego de Características Técnicas, según la cual:
    - Apartado introductorio en el que se detalle al menos lo siguiente:
      - Objetivo de la auditoría y descripción de su alcance.
      - Identificación del activo a auditar: nombre, versión, URL del activo, tecnologías que utiliza el activo, credenciales de usuario, etc.
      - Marco temporal de la auditoría: fechas de inicio y de fin, horario en que se realiza la auditoría, etc.
      - Información de la auditoría: tipo de auditoría (ej. pentest web), IPs autorizadas desde las que se audita, identificación de la empresa y de los auditores que realizan la auditoría.
      - Metodología: breve descripción de la metodología de trabajo empleada (explicar qué se va a hacer y cómo para conseguir los objetivos previstos).
      - Posibles estados de seguridad del activo.
    - Resumen ejecutivo que incluya al menos los siguientes apartados:
      - Valoración del nivel de seguridad del aplicativo y su justificación.
      - Se debe incluir algún gráfico estadístico que permita ver al menos el volumen de problemas de seguridad encontrados en base a su criticidad.
      - Recomendaciones concretas a seguir para conseguir que el aplicativo auditado obtenga el nivel de seguridad más alto posible. Para cada recomendación indicar si se debería aplicar a corto/medio/largo plazo, así como el nivel de prioridad recomendado para abordar cada una de las recomendaciones.
    - Descripción técnica detallada de cada una de las vulnerabilidades encontradas, incluyendo evidencias claras de los hallazgos encontrados (capturas de pantalla, peticiones realizadas, etc.). Cada vulnerabilidad encontrada debe tener asociado un nivel de criticidad en función del peligro que corra el aplicativo si es explotado.

- Pruebas realizadas: Incluyendo evidencias claras de los hallazgos encontrados (capturas de pantalla, peticiones realizadas, etc.). Cada vulnerabilidad encontrada debe tener asociado un nivel de criticidad en función del peligro que corra el aplicativo si es explotado..
- Aspectos importantes a tener en cuenta
  - Se permite (incluso se recomienda) el uso de herramientas automáticas, pero la auditoría no debe limitarse al uso de este tipo de herramientas. Se deben realizar pruebas manuales por parte de un auditor especializado.
  - Adicionalmente no se debe proporcionar en el informe la salida en crudo de las herramientas automáticas. Esta información debe ser procesada e interpretada adecuadamente por parte de un auditor especializado, de tal forma que se determine y compruebe si se trata de problemas reales de seguridad o no.
  - La auditoría debe ser realizada por parte de un auditor experto en la materia. Este debe contar con experiencia profesional demostrable en la realización de auditorías de seguridad del tipo en cuestión. Por ejemplo una auditoría de una web debe ser realizada por un auditor experto en la realización de auditorías web, el cual no tiene por qué ser experto en otros tipos de auditorías.
  - La auditoría debe ser realizada por parte de una empresa que esté especializada y que tenga experiencia contrastada en la realización de auditorías de seguridad.
  - Las auditorías deben realizarse con antelación a la fecha en la que se va a hacer uso del servicio, dado que si se detectan problemas de seguridad durante la auditoría estos tendrán que ser resueltos por parte del equipo de desarrollo del aplicativo auditado. En términos generales se recomienda que la auditoría de seguridad se lleve a cabo al menos tres semanas antes de la fecha en la que se va a hacer uso del servicio.
  - Una vez corregidos los fallos de seguridad encontrados en la auditoría el equipo de auditorías debe comprobar y certificar en un informe (puede ser un apartado adicional al informe de auditoría) si efectivamente se han corregido o no.

- **Informe de concurrencia** en los términos descritos en el apartado 2.4.4 del Pliego de Características Técnicas, según la cual:
  - La plataforma deberá soportar de forma estable y fluida la participación simultánea de al menos 100 equipos con 4 usuarios cada uno, haciendo un total efectivo de al menos 400 usuarios concurrentes.

- Se considera concurrencia no solo a la navegación en el portal web sino al trabajo simultáneo de los usuarios en el entorno de virtualización.
- El proveedor deberá presentar un informe con pruebas de concurrencia que avale que la plataforma puede soportar, al menos, esta carga de usuarios concurrentes. Se valorará en los criterios de valoración, mejora sobre estos requisitos de concurrencia que se presenten a través de dichas pruebas e informes.

Justificación de los requisitos de adscrición de medios

Por otra parte, para la acreditación de la declaración de adscripción de medios técnicos y personales se define lo siguiente en el Pliego de Características Generales en su apartado 18 de la tabla resumen:

- **Para acreditar el conocimiento en el idioma inglés podrán presentarse indistintamente:**
  - **Títulos oficiales del nivel de inglés o certificados expedidos por entidad reconocida**, cuya actividad consista en la formación y evaluación de inglés. Los títulos vendrán acompañados con la justificación de la correspondencia en el marco común europeo de referencia para las lenguas del Consejo de Europa. La evaluación certificada deberá estar basada en el marco común europeo de referencia para las lenguas del Consejo de Europa. A estos efectos se tendrán en cuenta páginas oficiales. A título de ejemplo la del Ministerio de Empleo y Seguridad Social que recoge equivalencias:
    - http://www.empleo.gob.es/es/mundo/consejerias/reinounido/portalempleo/es/curriculum/acreditacion-idiomas/index.htm
    - Certificados expedidos por entidad cuya actividad consista en la formación y evaluación de inglés. La evaluación certificada deberá estar basada en el marco común europeo de referencia para las lenguas del Consejo de Europa

    Para acreditar la certificación deberá presentarse la certificación o prueba fehaciente de tenencia de la misma donde se pueda comprobar fecha de emisión y vigencia.
- **Para la acreditación de la experiencia de los perfiles:**

  Para acreditar la experiencia de cada persona, el licitador deberá entregar, para cada perfil del equipo propuesto:
  - **Informe oficial detallado de vida laboral** donde se describa la/s empresa/s en la/s que ha trabajado y fechas de inicio y fin.
  - **Datos identificativos del perfil, y rol dentro del equipo propuesto,** de entre los perfiles solicitados
  - Una **tabla** que recoja los siguientes datos, por cada proyecto o servicio que sirva para acreditar experiencia de la que se considera de interés para su evaluación:

- Proyecto/Servicio: nombre de los proyectos o servicios que justifican los años de experiencia aportados y nombre de la empresa contratante. Una fila por proyecto o servicio. No se permiten nombres ambiguos como: "Varios", "Proyecto interno"
- Fecha de inicio: fechas de inicio de la participación de las personas en los proyectos o servicios que justifican los años de experiencia aportados. Formato: MM/AAAA. No se permiten fechas que indiquen sólo el año.
- Fecha de fin: fechas de fin de la participación de las personas en los proyectos o servicios que justifican los años de experiencia aportados. Formato: MM/AAAA. No se permiten fechas que indiquen sólo el año.
- Descripción: descripción del objeto del proyecto o servicio. No se permiten descripciones ambiguas como: "Proyecto interno" o similares. Es necesario describir con detalle el objeto del proyecto o servicio para que pueda ser evaluado y se indiquen claramente las actividades en relación con la experiencia de interés a acreditar para el presente expediente (realizando tareas relacionadas con la adquisición y análisis forense de evidencias digitales, hacking ético, explotación de vulnerabilidades y operaciones red team). Además se indicará:
  - Entidad. Entidad para la cual se realizó el proyecto o servicio.
  - Persona de contacto. Persona de la entidad para la que se realizó el proyecto o servicio con la que se pueda contactar para contrastar la información aportada. Se deberá incluir email y/o teléfono de contacto.
- Tipo de experiencia acreditado: Se deberá incluir, además de lo anterior, indicación del tipo de experiencia de interés que acredita el proyecto o servicio. La información deberá corresponderse con la de los perfiles presentada y valorada en la oferta. El tipo de experiencia de interés a indicar dependerá de cada tipo de perfil:
  - **Para los dos perfiles de analista forense DFIR**, se deberá señalar en cada proyecto o servicio si hace referencia a uno de los siguientes:
    - Análisis técnico de artefactos digitales o adquisición técnica de evidencias digitales en un contexto DFIR. Solo se considerará experiencia aplicable a respuesta a incidentes, y no la de peritaje informático (específica para obtener y custodiar pruebas para procedimientos judiciales)
  - **Para los dos perfiles de experto** en tests de penetración y operaciones red team, se deberá señalar en cada proyecto o servicio si hace referencia a uno de los siguientes:
    - Realización de tests de penetración en el contexto de un red team
    - Desarrollo de técnicas de explotación de vulnerabilidades

- Desarrollo de laboratorios de simulación de sistemas vulnerables

- A continuación, se adjunta un modelo de tabla con toda la información necesaria requerida por cada proyecto o servicio que sirva para acreditar experiencia de la que se considera de interés para su evaluación (en el modelo se incluye sólo la experiencia de interés para el perfil de analista forense/DFIR).

Nombre Proyecto	***(nombre del proyecto concreto y no genérico)***			**Entidad**	***(entidad cliente del proyecto/servicio)***
Datos Contacto	*(nombre, apellidos, email y teléfono)*	Fecha Inicio	*(MM/AAAA)*	Fecha Fin	*(MM/AAAA)*
Descripción Proyecto/servicio	*(descripción detallada del proyecto o servicio, indicando claramente las actividades en relación con la experiencia de interés a acreditar para este caso)*				
Tipo Experiencia acreditado	*(Marcar con una "x" el que corresponda. Se incluyen a continuación de ejemplo sólo los tipos de experiencia relevantes para el perfil de analista forense DFIR)* ☐ Análisis técnico de artefactos digitales o adquisición técnica de evidencias digitales en un contexto DFIR. Solo se considerará experiencia aplicable a respuesta a incidentes, y no la de peritaje informático (específica para obtener y custodiar pruebas para procedimientos judiciales) ☐ Experiencia en test de penetración y operaciones Red Team en alguna de las siguientes: • Realización de test de penetración en el contexto de un Red Team. • Desarrollo de técnicas de explotación de vulnerabilidades. • Desarrollo de laboratorios de simulación de sistemas vulnerables.				

- **<u>Para la acreditación de las certificaciones:</u>**

  Para acreditar las certificaciones de cada persona, el licitador deberá entregar lo siguiente:

  - Certificados expedidos por la entidad que acredita cada una de las certificaciones.
  - Evidencia de que la certificación está o ha estado en vigor durante los últimos 4 años.

3 EVALUACIÓN

Experiencia

Los 4 perfiles adscritos **CUMPLEN** **con los requisitos de experiencia exigidos**, de acuerdo a la oferta realizada por la empresa en el equipo de diseño e implementación de retos como en el equipo de soporte.

3.1.1.1 Equipo de diseño e implementación de retos

La siguiente tabla recoge el detalle de la evaluación realizada, en cuanto al "equipo de diseño e implementación de retos", donde deben justificarse al menos 4 años:

Evaluación de la Experiencia					
Equipo	**Requisito**	**Perfil**	**Experiencia aportada**	**Cumplimiento**	**Observaciones**
Equipo de diseño e implementación de retos	2 perfiles - Analistas forense DFIR				
	Perfil 1 - al menos cuatro años de experiencia	CPG	18años + 8 meses	SI	**Trabajos realizados:** Liderazgo en respuesta a incidentes de seguridad y contención de brechas. Análisis forense para identificar y rastrear actividades maliciosas. Adquisición y preservación de pruebas digitales para investigaciones. Análisis de malware y desarrollo de firmas para su detección. Mejora de políticas de seguridad y capacitación de empleados. **Consideraciones:** Cumple con lo especificado como requisito mínimo de experiencia (4años) y con lo especificado en los criterios objetivos (más de 64 meses). Se contrasta lo aportado en el CV con la vida laboral. **Documentación:** Se entrega toda la documentación solicitada por pliego (informe de vida laboral, datos identificativos CV en formato tabla).
	Perfil 1 - Nivel inglés mínimo B2		Certificado B2	SI	Aporta certificado
	Perfil 2 - al menos cuatro años de experiencia	JRC	9 años + 6 meses	SI	**Trabajos realizados:** Gestión de incidentes. Analista forense. **Consideraciones:** Cumple con lo especificado como requisito mínimo de experiencia (4años) y con lo especificado en los criterios objetivos (más de 64 meses). Se contrasta lo aportado en el CV con la vida laboral. **Documentación:** Se entrega toda la documentación solicitada por pliego (informe de vida laboral, datos identificativos CV en formato tabla).
	Perfil 2 - Nivel inglés mínimo B2		Certificado B2	SI	Aporta certificado
	2 perfiles - expertos en test de penetración				
	Perfil 1 - al menos cuatro años de experiencia	JRV	15 años + 7 meses	SI	**Trabajos realizados:** Pentesting técnico. Auditoría de vulnerabilidades en aplicaciones web. Experiencia en pruebas de penetración Evaluación de seguridad informática, entre otros **Consideraciones:** Cumple con lo especificado como requisito mínimo de experiencia (4años) y con lo especificado en los criterios objetivos (más de 64 meses). Se contrasta lo aportado en el CV con la vida laboral. **Documentación:** Se entrega toda la documentación solicitada por pliego (informe de vida laboral, datos identificativos CV en formato tabla).
	Perfil 1 - Nivel inglés mínimo B2		Certificado B2	SI	Aporta certificado
	Perfil 2 - al menos cuatro años de experiencia	PNCF	7 años	SI	**Trabajos realizados:** Pentesting técnico. Auditoría de vulnerabilidades en aplicaciones web. Experiencia en pruebas de penetración Evaluación de seguridad informática, entre otros **Consideraciones:** Cumple con lo especificado como requisito mínimo de experiencia (4años) y con lo especificado en los criterios objetivos (más de 64 meses). Se contrasta lo aportado en el CV con la vida laboral. **Documentación:** Se entrega toda la documentación solicitada por pliego (informe de vida laboral, datos identificativos CV en formato tabla).
	Perfil 2 - Nivel inglés mínimo B2		Certificado B2	SI	Aporta certificado
Equipo de diseño e implementación de retos	Debe ser el mismo equipo que el de diseño			SI	Serán los mismos perfiles

Figura 1 - Evaluación experiencia de los perfiles propuestos

3.1.1.2 Equipo de soporte

Proponen los mismos perfiles, por lo que **CUMPLEN** con lo solicitado en el pliego.

Certificaciones

Los 4 perfiles adscritos **CUMPLEN** **con los requisitos de Certificaciones exigidos**, de acuerdo a la oferta realizada por la empresa en los criterios de valoración cuantificables.

La siguiente tabla recoge el detalle de la evaluación realizada:

Evaluación de las Certificaciones					
Equipo	**Requisito**	**Perfil**	**Certificaciones**	**Cumplimiento**	**Observaciones**
Equipo de diseño e implementación de retos	2 perfiles - Analistas forense DFIR				
	Perfil 1 - Certificaciones	CPG	GPEN OSCP OSEP OSWE	SI	Se adjuntan los certificados de todas ellas. Se encuentran vigentes. Son las referidas en lo especificado para su valoración en el sobre 2
	Perfil 2 - Certificaciones	JRC	OSCP OSEP	SI	Se adjuntan los certificados de todas ellas. Se encuentran vigentes. Son las referidas en lo especificado para su valoración en el sobre 2
	2 perfiles - expertos en test de penetración				
	Perfil 1 - Certificaciones	JRV	OSCP	SI	Se adjuntan los certificados de todas ellas. Se encuentran vigentes. Son las referidas en lo especificado para su valoración en el sobre 2
	Perfil 2 - Certificaciones	PNCF	OSCP	SI	Se adjuntan los certificados de todas ellas. Se encuentran vigentes. Son las referidas en lo especificado para su valoración en el sobre 2

Figura 2 - Evaluación certificaciones de los perfiles propuestos

Plataforma

Los informes aportados **CUMPLEN** **con los requisitos exigidos en el Pliego de Características Generales y en el Pliego de Características Técnicas**.

El adjudicatario ha entregado toda la documentación necesaria para su evaluación:

- Informe de auditoría de seguridad.
- Informe de concurrencia.

Las siguientes tablas recogen el detalle de la evaluación realizada:

Informe de auditoría de seguridad			
Apartado	**Requisito**	**Cumplimiento**	**Observaciones**
General	N/A	SI	Se presentan dos informes de auditoría, uno de la infraestructura de la plataforma y otro de código
Introducción	Objetivo de la auditoría y descripción de su alcance.	SI	Ambos informes continienen un apartado de "Objetivo" que define el alcance de cada una de las auditorías realizadas de manera detallada.
	Identificación del activo a auditar: nombre, versión, URL del activo, tecnologías que utiliza el activo, credenciales de usuario, etc.	SI	Se incorpora un listado de los activos auditados. En el caso de la auditoría de infraestructura se indica la URL de los dos activos auditados (back y front) y los puertos para dichas URL. En el caso de la auditoría de código, se indica el aplicativo a auditar así como la versión y el número y tipo de archivos de código auditados.
	Marco temporal de la auditoría: fechas de inicio y de fin, horario en que se realiza la auditoría, etc.	SI	En ambos informes se incorporan los marcos temporales de las auditorías realizadas incluyendo la fecha inicio y fin de las mismas para cada uno de los activos auditados. Aunque no se incluyen horarios específicos se entiendo como cumplido el requisito.
	Información de la auditoría: tipo de auditoría (ej. pentest web), IPs autorizadas desde las que se audita, identificación de la empresa y de los auditores que realizan la auditoría.	SI	Se indican los datos en los apartados correspondientes de ambos informes "Tratamiento del documento" y en la "introducción"
	Metodología: breve descripción de la metodología de trabajo empleada (explicar qué se va a hacer y cómo para conseguir los objetivos previstos).	SI	Se incluye un apartado de metodología en ambos informes que incluye tanto la experiencia del equipo de trabajo, como el detalle de las pruebas que se van a llevar a cabo dentro de cada tipología de auditoría. También se incorpora un apartado de métricas y el estándar utilizado.
	Posibles estados de seguridad del activo.	SI	Se incorpora un detalle del estándar (CVSS) que icorpora el rango de riesgo

Resumen ejecutivo	Valoración del nivel de seguridad del aplicativo y su justificación.	SI	Se incorpora en ambos informes un resumen ejecutivo con el resultado de vulnerabilidades (en el caso de la auditoría de código se encuentra una de riesgo bajo y en el caso de la auditoría de seguridad en las infraestructuras no se detectan vulnerabilidades). Se incorporan varias tablas con el detalle de las vulnerabilidades, en caso de existir, y un resumen visual de los resultados. Se incorpora la valoración del nivel de seguridad que incluye los resultados de estas auditorías pero que también incluyen los antecedentes y contextos y la historia en cuanto a las auditorías realizadas previamente sobre la aplicación desde su puesta en marcha, que dan como resultado los buenos resultados de estas auditorías y el nivel alto de seguridad de la plataforma.
	Se debe incluir algún gráfico estadístico que permita ver al menos el volumen de problemas de seguridad encontrados en base a su criticidad.		
	Recomendaciones concretas a seguir para conseguir que el aplicativo auditado obtenga el nivel de seguridad más alto posible. Para cada recomendación indicar si se debería aplicar a corto/medio/largo plazo, así como el nivel de prioridad recomendado para abordar cada una de las recomendaciones.		
Descripción técnica detallada de cada una de las vulnerabilidades encontradas	Incluyendo evidencias claras de los hallazgos encontrados (capturas de pantalla, peticiones realizadas, etc.). Cada vulnerabilidad encontrada debe tener asociado un nivel de criticidad en función del peligro que corra el aplicativo si es explotado.	SI	Se incorpora esta información para la vulnerabilidad encontrada en uno de los informes (recordando que en el otro no se ha encontrado ninguna).
Pruebas realizadas	Incluyendo evidencias claras de los hallazgos encontrados (capturas de pantalla, peticiones realizadas, etc.). Cada vulnerabilidad encontrada debe tener asociado un nivel de criticidad en función del peligro que corra el aplicativo si es explotado.	SI	Se incorpora esta información para la vulnerabilidad encontrada en uno de los informes (recordando que en el otro no se ha encontrado ninguna), con pantallzos, recomendaciones, referencias, etc.
Otros aspectos importantes	Uso de herramientas automáticas y manuales. Procesamiento de los resultados automáticos,. Auditores expertos y una empresa especializada. Fecha anterior a la del uso de la plataforma. Corrección de las vulnerabilidades encontradas.	SI	A lo largo de ambos informes se detalla esta información, dando por cumplidos los requisitos solicitados.

Figura 3 - Evaluación de los informes de auditoría

Informe de concurrencia		
Requisito	**Cumplimiento**	**Observaciones**
La plataforma deberá soportar de forma estable y fluida la participación simultánea de al menos 100 equipos con 4 usuarios cada uno, haciendo un total efectivo de al menos 400 usuarios concurrentes. (NOTA: Se considera concurrencia no solo a la navegación en el portal web sino al trabajo simultáneo de los usuarios en el entorno de virtualización. El proveedor deberá presentar un informe con pruebas de concurrencia que avale que la plataforma puede soportar, al menos, esta carga de usuarios concurrentes. Se valorará en los criterios de valoración, mejora sobre estos requisitos de concurrencia que se presenten a través de dichas pruebas e informes.)	SI	Se superan en pruebas de concurrencia los datos solicitados. En el informe se realizan diversas pruebas y se adjuntan pruebas documentales y gráficas de las diferentes pruebas realizadas así como los resultados.

Figura 4 - Evaluación informe de concurrencia

4 CONCLUSIÓN

En base a la evaluación realizada, se concluye que **la empresa Telefónica Soluciones de Informática y Comunicaciones de España, S.A.U. CUMPLEN con los requisitos de los Medios Personales adscritos al contrato correspondiente al** 063/24: *Diseño de competición tipo Capture the Flag para CERTs/CSIRTs Internacionales Ed. 2024,* en base a lo especificado en el Pliego de Características Generales.

Firmado en León a 26 de septiembre de 2024

SGB

Responsable del Área de Ciberejercicios y Ciberresilencia de INCIBE-CERT