CORTE SUPREMA DE JUSTICIA

Dirección General de Tecnología de la Información y las Comunicaciones

Compromiso con la gente

Asunción, 28 de octubre de 2024

Señor
Abg. Mirko Duré, Coordinador
Comité de Evaluación de Ofertas
Presente

Me dirijo a Ud., en referencia a la nota NCEO Nº 1084/2024, **LICITACIÓN POR CONCURSO DE OFERTAS PAC N° 01/2024 "CONSULTORÍA DE SEGURIDAD INFORMÁTICA - AD REFERENDUM" ID 436.577.-**, a los efectos de remitir adjunto el informe técnico final.

Sin otro particular, le saludo atentamente.

Luis Ruiz Díaz

CORTE SUPREMA DE JUSTICIA
COMITÉ DE EVALUACIÓN DE OFERTAS
MESA DE ENTRADA
28 OCT. 2024
Firma: _____ Hora: 12:00
Aclaración: Estela Marquez
Corte Suprema de Justicia

ITEM I	DESCRIPCIÓN DE CRITERIOS	PUNTAJE MÁXIMO	ITEM I PUNTOS - Rymtech	ITEM I PUNTOS - LNXnetwork	ITEM I PUNTOS - GRUPO HORUS
	Experiencia General De La Empresa	2			
	1. El oferente deberá demostrar una antigüedad de 3 (TRES) años (2021, 2022 y 2023) en el mercado través de Copia de la constitución en caso de las sociedades y la constancia de RUC en casos de las unipersonales. **EXCLUYENTE.**	EXC.	-	CUMPLE	CUMPLE
	2. El oferente deberá acreditar experiencia general en ***consultorías informáticas*** en los últimos 5 (CINCO) años, presentando copias de contratos anteriores y/o facturaciones, ya sea en entidades públicas y/o privadas. Los contratos y facturas deberán corresponder a los últimos 5 (CINCO) años (2019, 2020, 2021, 2022 y 2023) y deberá ser como mínimo el 50% del monto total del llamado. Se aclara que no es necesario contar con un contrato por año.	2	-	2	2

ITEM II	DESCRIPCIÓN DE CRITERIOS	PUNTAJE MÁXIMO	ITEM II PUNTOS - Rymtech	ITEM II PUNTOS - LNXnetwork	ITEM II PUNTOS - GRUPO HORUS
	Experiencia Específica	40			
	1. Mínimo de 3 (tres) consultorías, evaluaciones, niveles de cumplimiento e implementaciones de medidas de ciberseguridad, basados en marcos de trabajo CIS Controls, NIST SP 800-53, CSF y/o ISO 27001, realizados durante los últimos 5 (CINCO) años (2019, 2020, 2021, 2022 y 2023), los cuales valdrán 16 puntos. ***Por cada trabajo adicional al mínimo requerido se otorgará 2 puntos hasta un máximo de 20 puntos.***	20	-	20	20
	2. Mínimo de 3 (tres) auditorías de vulnerabilidades, servicios de SOC, respuestas a incidentes y/o pruebas de intrusión (PENTEST) realizadas durante los últimos 5 (CINCO) años (2019, 2020, 2021, 2022 y 2023), las cuales valdrán 12 puntos. ***Por cada trabajo adicional al mínimo requerido se otorgará 2 puntos hasta un máximo de 16 puntos.***	16	-	16	16
	3. Certificación en Ciberseguridad del oferente, mediante membresías ovcertificaciones expedidas por organismos internacionales competentes. ***Por cada una se otorgará 2 puntos, hasta un máximo de 4 puntos.***	4	-	0	0

ITEM III	DESCRIPCIÓN DE CRITERIOS	PUNTAJE MÁXIMO	ITEM III PUNTOS - Rymtech	ITEM III PUNTOS - LNXnetwork	ITEM III PUNTOS - GRUPO HORUS
	Propuesta Técnica	8			
1. Descripcion del enfoque, metodologia y plan de actividades		1	-	1	1
2. Composicion de equipo y asignacion de responsabilidades		2	-	2	2
3. Calendario de Actividades del Personal.		2	-	2	2
4. Plan de Trabajo.		3	-	3	3

ITEM IV	DESCRIPCIÓN DE CRITERIOS	PUNTAJE MÁXIMO	ITEM IV PUNTOS - Rymtech	ITEM IV PUNTOS - LNXnetwork	ITEM IV PUNTOS - GRUPO HORUS
	Plantel Técnico	50 PUNTOS			
1 Cada Oferente presentará los antecedentes académicos y profesionales del equipo de trabajo con los profesionales básicos exigidos, los cuales deberán ser complementados de acuerdo a las necesidades de la empresa consultora para el cumplimiento de las actividades solicitadas en el plazo establecido, estos antecedentes serán evaluados y se otorgará hasta un máximo de ***50 (cincuenta) puntos.***			-	26	39,5
2 Para acreditar los antecedentes académicos y profesionales se utilizará como medio de prueba el Formulario TEC-3.1: Formación Profesional - Currículum del Personal Profesional Propuesto, acompañado de los documentos que acrediten la formación profesional (Títulos, Certificados, Constancias, etc., debidamente autenticadas por escribanía). En el caso de títulos profesionales extranjeros, deberán estar convalidados por las instituciones nacionales competentes.					

		PUNTAJE ALCANZADO - Rymtech	PUNTAJE ALCANZADO - LNXnetwork	PUNTAJE ALCANZADO - GRUPO HORUS
TOTAL DE PUNTAJE MAXIMO	100 PUNTOS	00 / 100	72 / 100	85,5 / 100
PUNTAJE MINIMO REQUERIDO	70 PUNTOS			

Observación: No se evalua la empresa Rymtech ya que el mismo se encuentra descalificado documentalmente.

Luis Ruiz

ITEM IV					ANOTACIONES DPCI
EVALUACION DE PLANTEL TECNICO		PUNTAJE	PUNTAJE MAXIMO		
1	Gerente de Proyecto	8	50	6	
2	Jefe Consultor/Evaluador de Seguridad	12		7	
3	Consultor/Evaluador de Seguridad	30		13	
			TOTAL PUNTAJE	26	

OFERENTE: LNXnetwork

Gerente del Proyecto		PUNTAJES	HECTOR ANTONIO AGUIRRE
Deberá participar activamente en todas las etapas y fases comprendidas en esta consultoría de evaluación y ajustes de cumplimiento en Ciberseguridad para el PJ, trabajando de cerca con el equipo técnico de la DGTIC, redactando los documentos a ser presentados durante el avance del proyecto. Estas funciones tienen un carácter enunciativo y no delimitante.			
Perfil Técnico mínimo (Excluyente)	**Puntaje**		
1. Título universitario en Ingeniería Informática, Análisis de Sistemas, o ramas afines a las Tecnologías de la Información. EXC.	(excluyente)	Cumple	(FOLIO 125)
2. Experiencia mínima de 3 años en gerenciamiento o liderazgo de equipos de trabajo para el desarrollo e implementación de proyectos tecnológicos, lo que valdrá 2 puntos. Por cada año adicional al mínimo requerido se le otorgará 1 punto hasta un máximo de 4 puntos.	4	4	EXPERIENCIA (FOLIO 110)
3. Curso de Postgrado en Gestión de Proyectos y/o certificación PMP, PRINCE2. * Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.	2	0	
trabajo para el desarrollo e implementación de proyectos de Ciberseguridad y Protección de la Información.	2	2	EXPERIENCIA (FOLIO 110-112)
TOTAL GERENTE (1 PERSONA)	8	6	

Jefe Consultor/Evaluador de Seguridad		PUNTAJES	ADRIANA PANIAGUA
Su función principal será llevar a cabo la consultoría de evaluación y ajustes de cumplimiento en Ciberseguridad para el PJ, liderando el equipo técnico del oferente y trabajando de manera coordinada con la DCPI y la DGTIC, elaborando los documentos e insumos a ser entregados en las diferentes etapas e hitos de control previstas en esta consultoría. Estas funciones tienen un carácter enunciativo y no delimitante.			
Perfil Técnico mínimo (Excluyente)	**Puntaje**		
1. Título universitario en Ingeniería Informática, Análisis de Sistemas, o ramas afines a las Tecnologías de la Información.	(excluyente)	Cumple	TITULO (FOLIO 132)
2. Experiencia mínima de 3 años de trabajo como Jefe de Consultores y Evaluadores de seguridad, lo que valdrá 2 puntos. **Por cada año adicional al mínimo requerido se le otorgará 1 punto hasta un máximo de 4 puntos.**	4	4	EXPERIENCIA (FOLIO 127)
3. Conocimientos comprobables en marcos de seguridad tales como las normas ISO/IEC 27001/2, ISO/IEC 27035, NIST, ITIL, COBIT. Los puntos serán otorgados de acuerdo a la siguiente escala de proporcionalidad: • Certificación en más de una de las mencionadas: 4 puntos • Certificación en una de ellas: 3 puntos • Certificación no vigente en alguna de las mencionadas: 2 puntos • Cursos y/o capacitaciones de preparación para certificación: 1 punto * Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.	4	0	
4. Conocimientos comprobables en seguridad de la información y/o ciberseguridad: CISSP, ECSS, ECSA, CISM, CISA, CCISO, CCIE, CCNP, CND, ECIH, CEH, CSA, CPENT, CTIA, eJPT, PenTest+, CPT, CEPT, CRTOP, GPEN, OSCP. Los puntos serán otorgados de acuerdo a la siguiente escala de proporcionalidad: • Certificación vigente en más de una de las mencionadas: 4 puntos • Certificación vigente en alguna de las mencionadas: 3 puntos • Certificación no vigente en alguna de las mencionadas: 2 puntos • Cursos y/o capacitaciones de preparación para certificación: 1 punto **Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.**	4	3	CERTIFICADO CCISO(FOLIO 131)
TOTAL JEFE (1 PERSONA)	12	7	

Equipo de trabajo (Evaluador, Analista, Auditor de Seguridad)		PUNTAJES	PABLO DAVID AGUILAR RABITO (PA) ALEJANDRO MATIAS MURDOCH CIBILS (AM)
Su función principal será llevar a cabo las tareas específicas determinadas para la consultoría de evaluación y ajustes de cumplimiento en Ciberseguridad para el PJ, reportando al Jefe Consultor/Evaluador de Seguridad y trabajando de manera coordinada con los equipos internos de la DGTIC que deben ser involucrados. • **Le corresponderá (las siguientes funciones tienen un carácter enunciativo y no delimitante):** o Realizar análisis exhaustivos de los sistemas y plataformas informáticas, así como de las redes de la institución, de tal manera a identificar vulnerabilidades y puntos débiles en su seguridad. o Realizar las pruebas de intrusión y penetración para detectar posibles brechas y riesgos, que servirán de insumo para la elaboración de recomendaciones y medidas correctivas a ser realizadas para mitigarlas o erradicarlas. o Realizar una revisión exhaustiva de los controles y medidas de seguridad implementadas por la institución. o Evaluar el cumplimiento de las políticas y estándares de seguridad, identificar posibles brechas y riesgos, y colaborar con propuestas y recomendaciones para mejorar la postura de seguridad institucional, así como el establecimiento de buenas prácticas que rigen la materia tanto a nivel nacional como internacional.			
Perfil Técnico mínimo (Excluyente)	**Puntaje**		
1. Al menos uno de los expertos deberá tener experiencia mínima de 4 años de trabajo como Evaluador, Analista, Auditor y/o Consultor de seguridad de la información y/o ciberseguridad.	(excluyente)	No Cumple	REQUERIR EXPERIENCIA (AL MENOS UNO DE LOS EXPERTOS) VER EN LOS ITEMS CORRESPONDIENTES ROCIO FLORENCIO: Ya no hace falta requerir por falla en el formulario TEC-1, que es documentación sustancial.

202 11/

2. Graduado Universitario de las carreras de Ingeniería Electrónica, Software, Informática, Analista de sistemas y TIC en general, valdrán 2 puntos, por cada profesional con título, hasta un máximo de 4 (cuatro) puntos.	4	4	[PA] 2 pts (FOLIO 142). [AM] 2 pts (FOLIO 151)
3. Experiencia comprobable de al menos 2 años en seguridad de la información y/o ciberseguridad: SIEM, Forensica digital (Forensic Tools), Respuesta a Incidentes (Incident Response Tools), Inteligencia de amenazas, orquestación y automatización de respuesta, auditoría de vulnerabilidades, administración de logs (Log Management tools), Virtualización, Gestión de Identidad y Accesos, Emulación de adversarios, SOAR, UTM, Firewalls, , Vulnerability Management tools, Cyberthreat Intelligence Platform, Security by Deception tools, Traffic Capture & Flow Analyses, Adversary Emulation/Simulation tools, DFIR stacks/tools, SASE, plataformas o herramientas de Zero Trust, IAM, CASB, Native Virtualization Platforms, Switching/Routing Intermediate, trabajos de revisión, auditorías, capacitaciones, etc. u otros tipos de herramientas/tecnologías asociados. Por cada persona del equipo: • Más 2 y menos de 3 años de experiencia laboral (conforme al criterio anterior) puntuará 3 puntos. • Más de 3 y menos de 5 años puntuará 5 puntos. • Más de 5 años puntuará 10 puntos. Hasta un máximo de 20 (veinte) puntos por las dos personas. * Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.	20	3	[PA] 3 pts (FOLIOS 134) [AM] 0 pts (FOLIO 146)
4. Conocimientos comprobables en seguridad de la información y/o ciberseguridad: CISSP, ECSS, ECSA, CISM, CISA, CCISO, CCIE, CCNP, CND, ECIH, CEH, CSA, CPENT, CTIA, eJPT, PenTest+, CPT, CEPT, CRTOP, GPEN, OSCP. Por cada persona del equipo, los puntos serán otorgados de acuerdo a la siguiente escala de proporcionalidad: • Certificación vigente en alguna de las mencionadas: 2 puntos • Certificación no vigente en alguna de las mencionadas: 1 puntos • Cursos y/o capacitaciones de preparación para certificación: 0.5 puntos Hasta un máximo de 6 (seis) puntos por las dos personas. * Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.	6	6	[PA] 5 pts (CERTIFICADO CEH FOLIO 139 / CERTIFICADO CND FOLIO 140 VENCIDO y puntua 1 / CERTIFICADO CSA FOLIO 140) [AM] 1 pts (CERTIFICADO CEH FOLIO 149 VENCIDO y puntua 1)
TOTAL EQUIPO (2 PERSONAS)	30	13	

ITEM IV					ANOTACIONES DPCI
EVALUACION DE PLANTEL TECNICO		PUNTAJE	PUNTAJE MAXIMO		
1	Gerente de Proyecto	8	50	6	
2	Jefe Consultor/Evaluador de Seguridad	12		10	
3	Consultor/Evaluador de Seguridad	30		23,5	
			TOTAL PUNTAJE	39,5	

OFERENTE: HORUS

Gerente del Proyecto		PUNTAJES	TITO ADRIANO OCAMPOS NEGREIROS
Deberá participar activamente en todas las etapas y fases comprendidas en esta consultoría de evaluación y ajustes de cumplimiento en Ciberseguridad para el PJ, trabajando de cerca con el equipo técnico de la DGTIC, redactando los documentos a ser presentados durante el avance del proyecto. Estas funciones tienen un carácter enunciativo y no delimitante.			
Perfil Técnico mínimo (Excluyente)	Puntaje		
1. Título universitario en Ingeniería Informática, Análisis de Sistemas, o ramas afines a las Tecnologías de la Información. EXC.	(excluyente)	Cumple	(FOLIO 248-253)
2. Experiencia mínima de 3 años en gerenciamiento o liderazgo de equipos de trabajo para el desarrollo e implementación de proyectos tecnológicos, lo que valdrá 2 puntos. Por cada año adicional al mínimo requerido se le otorgará 1 punto hasta un máximo de 4 puntos.	4	4	EXPERIENCIA (FOLIO 242-246)
3. Curso de Postgrado en Gestión de Proyectos y/o certificación PMP, PRINCE2. * Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.	2	0	
4. Experiencia comprobable en gerenciamiento o liderazgo de equipos de trabajo para el desarrollo e implementación de proyectos de Ciberseguridad y Protección de la Información.	2	2	EXPERIENCIA (FOLIO 242-246)
TOTAL GERENTE (1 PERSONA)	8	6	

Jefe Consultor/Evaluador de Seguridad		PUNTAJES	JORGE DANIEL ZUNINI CASAMAYOURET
Su función principal será llevar a cabo la consultoría de evaluación y ajustes de cumplimiento en Ciberseguridad para el PJ, liderando el equipo técnico del oferente y trabajando de manera coordinada con la DCPI y la DGTIC, elaborando los documentos e insumos a ser entregados en las diferentes etapas e hitos de control previstas en esta consultoría. Estas funciones tienen un carácter enunciativo y no delimitante.			
Perfil Técnico mínimo (Excluyente)	Puntaje		
1. Título universitario en Ingeniería Informática, Análisis de Sistemas, o ramas afines a las Tecnologías de la Información.	(excluyente)	Cumple	TITULO (FOLIO 271-275)
2. Experiencia mínima de 3 años de trabajo como Jefe de Consultores y Evaluadores de seguridad, lo que valdrá 2 puntos. **Por cada año adicional al mínimo requerido se le otorgará 1 punto hasta un máximo de 4 puntos.**	4	4	EXPERIENCIA (FOLIO 264-269)
3. Conocimientos comprobables en marcos de seguridad tales como las normas ISO/IEC 27001/2, ISO/IEC 27035, NIST, ITIL, COBIT. Los puntos serán otorgados de acuerdo a la siguiente escala de proporcionalidad: • Certificación en más de una de las mencionadas: 4 puntos • Certificación en una de ellas: 3 puntos • Certificación no vigente en alguna de las mencionadas: 2 puntos • Cursos y/o capacitaciones de preparación para certificación: 1 punto * Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.	4	3	CERTIFICADO ISO/IEC 27001:2022 (FOLIO 288) (QR VERIFICADO)
4. Conocimientos comprobables en seguridad de la información y/o ciberseguridad: CISSP, ECSS, ECSA, CISM, CISA, CCISO, CCIE, CCNP, CND, ECIH, CEH, CSA, CPENT, CTIA, eJPT, PenTest+, CPT, CEPT, CRTOP, GPEN, OSCP. Los puntos serán otorgados de acuerdo a la siguiente escala de proporcionalidad: • Certificación vigente en más de una de las mencionadas: 4 puntos • Certificación vigente en alguna de las mencionadas: 3 puntos • Certificación no vigente en alguna de las mencionadas: 2 puntos • Cursos y/o capacitaciones de preparación para certificación: 1 punto Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.	4	3	CERTIFICADO CRISC-1004622 (FOLIO 284) (VERIFICADO vencido 31 enero 2023) CERTIFICADO CISA-0023418 (FOLIO 283) (VERIFICADO valido hasta 31 enero 2025)
TOTAL JEFE (1 PERSONA)	12	10	

Equipo de trabajo (Evaluador, Analista, Auditor de Seguridad)		PUNTAJES	VICTOR DAVID CASARES [VDC] CARLOS ALBERTO BENITEZ GALVAN [CABG]
Su función principal será llevar a cabo las tareas específicas determinadas para la consultoría de evaluación y ajustes de cumplimiento en Ciberseguridad para el PJ, reportando al Jefe Consultor/Evaluador de Seguridad y trabajando de manera coordinada con los equipos internos de la DGTIC que deben ser involucrados. • Le corresponderá (las siguientes funciones tienen un carácter enunciativo y no delimitante): o Realizar análisis exhaustivos de los sistemas y plataformas informáticas, así como de las redes de la institución, de tal manera a identificar vulnerabilidades y puntos débiles en su seguridad. o Realizar las pruebas de intrusión y penetración para detectar posibles brechas y riesgos, que servirán de insumo para la elaboración de recomendaciones y medidas correctivas a ser realizadas para mitigarlas o erradicarlas. o Realizar una revisión exhaustiva de los controles y medidas de seguridad implementadas por la institución. o Evaluar el cumplimiento de las políticas y estándares de seguridad, identificar posibles brechas y riesgos, y colaborar con propuestas y recomendaciones para mejorar la postura de seguridad institucional, así como el establecimiento de buenas prácticas que rigen la materia tanto a nivel nacional como internacional.			
Perfil Técnico mínimo (Excluyente)	Puntaje		

290

12

1. Al menos uno de los expertos deberá tener experiencia mínima de 4 años de trabajo como Evaluador, Analista, Auditor y/o Consultor de seguridad de la Información y/o ciberseguridad.	(excluyente)	Cumple	EXPERIENCIA (AL MENOS UNO DE LOS EXPERTOS) VER EN LOS ITEMS CORRESPONDIENTES
2. Graduado Universitario de las carreras de Ingeniería Electrónica, Software, Informática, Analista de sistemas y TIC en general, valdrán 2 puntos, por cada profesional con título, hasta un máximo de 4 (cuatro) puntos.	4	2	[VDC] 0 pts (FOLIO 331, TIENE título de INGENIERO EN SISTEMAS de la Universidad Nacional de la Rioja Argentina. NO ACOMPAÑA documentos que acrediten que este homologado). [CABG] 2 pts (FOLIO 347). Tiene título de Lic. en Ciencias Informáticas, Énfasis en Prog. de Computadoras.
3. Experiencia comprobable de al menos 2 años en seguridad de la información y/o ciberseguridad: SIEM, Forensica digital (Forensic Tools), Respuesta a incidentes (Incident Response Tools), Inteligencia de amenazas, orquestación y automatización de respuesta, auditoría de vulnerabilidades, administración de logs (Log Management tools), Virtualización, Gestión de identidad y Accesos, Emulación de adversarios, SOAR, UTM, Firewalls, , Vulnerability Management tools, Cyberthreat Intelligence Platform, Security by Deception tools, Traffic Capture & Flow Analyses, Adversary Emulation/Simulation tools, DFIR stacks/tools, SASE, plataformas o herramientas de Zero Trust, IAM, CASB, Native Virtualization Platforms, Switching/Routing Intermediate, trabajos de revisión, auditorías, capacitaciones, etc. u otros tipos de herramientas/tecnologías asociados. Por cada persona del equipo: • Más 2 y menos de 3 años de experiencia laboral (conforme al criterio anterior) puntuará 3 puntos. • Más de 3 y menos de 5 años puntuará 5 puntos. • Más de 5 años puntuará 10 puntos. Hasta un máximo de 20 (veinte) puntos por las dos personas. * Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.	20	20	[VDC] 10 pts (FOLIOS 328-329, constancia 1000 HORAS BANCARD FOLIO 338) [CABG] 10 pts (FOLIO 338) OBS: se le da por la CERTIFICACIÓN
4. Conocimientos comprobables en seguridad de la información y/o ciberseguridad: CISSP, ECSS, ECSA, CISM, CISA, CCISO, CCIE, CCNP, CND, ECIH, CEH, CSA, CPENT, CTIA, eJPT, PenTest+, CPT, CEPT, CRTOP, GPEN, OSCP. Por cada persona del equipo, los puntos serán otorgados de acuerdo a la siguiente escala de proporcionalidad: • Certificación vigente en alguna de las mencionadas: 2 puntos • Certificación no vigente en alguna de las mencionadas: 1 puntos • Cursos y/o capacitaciones de preparación para certificación: 0.5 puntos Hasta un máximo de 6 (seis) puntos por las dos personas. * Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.	6	1,5	[VDC] 1 pts (CERTIFICADO CISCO CCNA FOLIO 333 VENCIDO SET 2014/ CERTIFICADO CEH FOLIO 334 VENCIDO 31 AGOSTO 2012 / CERTIFICADO OSCP FOLIO 336 CERTIFICACIÓN 2016 / Certificaciones no consideradas por no ser ninguna de las solicitadas: ~~CERTIFICADO ISO/IEC 27001:2013 FOLIO 332 CERTIFICACIÓN JUN 2023)~~ [CABG] 0,5 pts Certificaciones no consideradas por no ser ninguna de las solicitadas: (~~CERTIFICADO PROFESIONAL DE HACKING ÉTICO EXPERTO FOLIO 349 CERTIFICACION 22 OCTUBRE 2019 con 180 HORAS~~ ~~CERTIFICADO GPPT FOLIO 350 CERTIFICACION 10 ABRIL 2021, CERTIFICADO CIBERSEGURIDAD AD FOLIO 351 CERTIFICACION FEBRERO 2023~~)
TOTAL EQUIPO (2 PERSONAS)	30	23,5	