

# **CYBERCAMP 2019**

Acta valoración y clasificación de las propuestas "Call For Papers"











En León, a 21 de octubre de 2019, INCIBE elabora la presente acta con las valoraciones del Jurado.

Todas las valoraciones han sido realizadas sobre la herramienta de gestión adquirida para la presente edición: <a href="https://easychair.org">https://easychair.org</a>

Con los requisitos establecidos en las <u>bases de participación del CFP de CyberCamp 2019</u> y una vez finalizados los plazos establecidos por la Organización para la presentación de propuestas, se ha procedido a realizar la selección de las mismas en base a los criterios allí definidos.

En las bases de participación se indicaba que se seleccionarán un mínimo de 19 propuestas, para el programa de CyberCamp:

- Entre 6 y 12 ponencias magistrales
- Entre 6 y 10 talleres técnicos
- Entre 2 y 4 talleres técnicos de iniciación
- Entre 2 y 3 charlas inspiracionales y de promoción del talento
- Entre 3 y 5 charlas de concienciación

#### **PONENCIAS MAGISTRALES**

Lo criterios de valoración son:

■ Enfoque práctico de la propuesta. Puntos asignados: de 0 a 35 puntos. Se establecen los siguientes sub-criterios de valoración:

Puntuación	Índice de valoración	
0 – 30 puntos	La ponencia tiene en cuenta aspectos particulares como:  Técnicas para el reconocimiento y defensa contra amenazas de seguridad.  La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros.  Presentación de nuevas herramientas o sistemas desarrollados en ciberseguridad.  Distribución pública de las herramientas presentadas.  Nuevos sistemas de defensa de ciberseguridad.  Nuevas líneas de investigación de ciberseguridad.	
0 – 5 puntos	La propuesta plantea un enfoque práctico para que el público objetivo adquiera conocimiento de carácter práctico en sus propios ámbitos de actuación y tenga una implantación sencilla dentro del ámbito de actuación del asistente.	

**Temática.** Puntos asignados: de 0 a 30 puntos. Se establecen los siguientes sub-criterios de valoración:

Puntuación	Índice de valoración







0 – 15 puntos	La temática propuesta aporta un enfoque diferenciador en el ámbito de la ciberseguridad, favoreciendo progresos científicos o tecnológicos.	
0 – 10 puntos	La temática propuesta se encuentra dentro del listado de temas que se presumen de interés aportando un enfoque innovador sobre el mismo.	
0 – 5 puntos El esquema de la presentación es adecuado para el públi objetivo y la temática presentada.		

■ Valor didáctico. Puntos asignados: de 0 a 20 puntos

Puntuación	Índice de valoración
0 – 10 puntos	El conocimiento a transmitir al público objetivo es útil e instructivo
0 – 10 puntos	El planteamiento que hace de la ponencia y su enfoque didáctico garantiza el éxito de la misma.

Que no haya sido difundida previamente en otros eventos. Puntos asignados: de 0 a 15 puntos

Puntuación =  $15 - n^{\circ}$  congresos en los que se ha presentado anteriormente la propuesta presentada

El número de propuestas recibidas en la modalidad de Ponencias Magistrales es de 40.

Una vez deliberado por el Jurado y analizadas las propuestas, han resultado seleccionadas para ser presentadas en CyberCamp un total de **8 Ponencias Magistrales** correspondientes a aquellas que han obtenido una mejor valoración<sup>1</sup>.

Según esto, las <u>seleccionadas</u> para el programa de CyberCamp 2019 son las propuestas que se enumeran a continuación:

	Título	Candidato	Puntuación
1	When a Pentester meets Machine Learning	JS	89
2	Framework de ataque para el sector eléctrico, CAFFEINE	AF	87,5
3	Hacking hardware en sistemas empotrados: De la preservación a la seguridad	TGMC	86
4	Emulación de adversarios: De entender ATT&CK a construir tu propia emulación	PGP	85
5	Amenazas y camuflaje de comunicaciones Wi-Fi en entornos urbanos	JABG	84,5
6	From crimeware ransomware to targeted ransomware - Let's evolution the ecosystem	MRL	84
7	Macro problemas, micro soluciones	SS	82
8	Plug in the Middle	JMMC	80

Como <u>reservas</u> para el programa de CyberCamp 2019 en la modalidad de Ponencias Magistrales se enumeran las propuestas siguientes:

<sup>&</sup>lt;sup>1</sup> En el anexo I se puede ver el desglose de puntuación de cada una de las ponencias.







	Título	Candidato	Puntuación
1	Las peripecias de un Perito Informático	JCSN	79,5
2	Raspberry pi como control de seguridad perimetral	EMCC	78
3	Ataques Malwareless El auge de los "lolbins"	RAJ	76
4	Visión práctica del nuevo reglamento europeo de ciberseguridad	FPD	75,5
5	Evaluación de similitud de procesos de Windows mediante algoritmos de coincidencia aproximada	MMP	75
6	Detección de malware en volcados de memoria: Desafíos y Problemas Actuales	RJR	74
7	Técnicas de Balización en diferentes entornos de la red	ES	74
8	Hacking Psicológico: Psicología de un ciberataque	CLT	73
9	UNICODE attacks from scratch. New proposals to avoid countermeasures	AMM	71,5
10	RIoT - Riesgos y retos de ciberseguridad y privacidad en IoT	PV	71,5
11	La ciberseguridad y el factor humano		71
12	Spoofing Tire Pressure Monitoring Systems (TPMS) PC		70,5
13	Ciberseguridad en el ámbito sanitario CCR 68,5		68,5
14	Encadenando la confianza a la cadena de confianza, el último JTV 67,5 reto de blockchain.		67,5
15	Desensamblando la web: Las ventajas, vulnerabilidades y JC 67 riesgos de Web Assembly.		67
16			67
17	Análisis de ciberataques en honeypots LA		66,5
18	Diario de un detective en el ciberespacio		65,5
19	Contrainteligencia en Apoyo a Ciberinteligencia JMDCG		65
20	Tu tesoro en el bolsillo: (in)seguridad en Smartphone SRF 64		64
21	Santa Rita Rita, lo que publicas ya no se quita RG 62		62
22	resolviendo las 10 preguntas RSO 61,5		61,5

Aquellas propuestas (10) que no hubieron alcanzado un **mínimo de 60 puntos** quedaron descartadas.

- No disimules y simula: Simulación de adversarios
- La inmutabilidad de Blockchain y la ciberseguridad
- Ciberseguridad al alcance de la pyme
- Cloud Big Data Security
- Ingeniería social, el Dios de muchos rostros
- ¿Por qué el phishing sigue siendo tan efectivo?
- SecDevOps (DevSecOps) con contenedores en los dockers
- Intelligence-Led Cyber Attack Methodology
- La importancia de la verdadera concienciación y la sensibilización de usuarios en ciberseguridad.
- Una introducción al Threat Hunting

#### **TALLERES TÉCNICOS**

Lo criterios de valoración son:

■ Enfoque práctico de la propuesta. Puntos asignados: de 0 a 40 puntos. Se establecen los siguientes sub-criterios de valoración:







Puntuación	Índice de valoración	
	El taller tiene en cuenta aspectos particulares como:	
0 – 30 puntos	<ul> <li>□ Técnicas para el reconocimiento y defensa contra amenazas de seguridad.</li> <li>□ La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros.</li> <li>□ Divulgación responsable de exploits 0-day, propios o de terceros.</li> <li>□ Presentación de nuevas herramientas o sistemas desarrollados en ciberseguridad, bien si son desarrollos propios o de terceros.</li> <li>□ Distribución pública de las herramientas presentadas.</li> <li>□ Nuevos sistemas de defensa de ciberseguridad.</li> <li>□ Nuevas líneas de investigación de ciberseguridad.</li> </ul>	
0 – 10 puntos	El taller plantea un enfoque práctico para que el público objetivo adquiera conocimiento de carácter práctico en sus propios ámbitos de actuación y tenga una implantación sencilla dentro del ámbito de actuación del asistente.	

**Temática.** Puntos asignados: de 0 a 30 puntos. Se establecen los siguientes sub-criterios de valoración:

Puntuación	Índice de valoración
La temática propuesta aporta un enfoque diferenciador en ámbito de la ciberseguridad, favoreciendo progresos científico tecnológicos.	
0 – 10 puntos	La temática propuesta se encuentra dentro del listado de temas que se presumen de interés aportando un enfoque innovador sobre el mismo.
0 – 5 puntos	El esquema de la presentación es adecuado para el público objetivo y la temática presentada.

**Demostración práctica** Se valorará si el taller incluye demostraciones y los minutos estimados que conllevará esta parte práctica. Puntos asignados: de 0 a 20 puntos

Puntuación = (20 \* minutos demostración) / 60

Siendo 60 los minutos máximos de demostración propuestos

Que no haya sido difundida previamente en otros eventos.

Puntos asignados: de 0 a 10 puntos

Puntuación =  $10 - n^0$  congresos en los que se ha presentado anteriormente la propuesta presentada.

El número de propuestas recibidas en esta modalidad es de 20.

Una vez deliberado por el Jurado y analizadas las propuestas, han resultado seleccionadas para ser presentadas en CyberCamp un total de **8 Talleres Técnicos** correspondientes a aquellas que han obtenido una mejor valoración<sup>2</sup>.

<sup>&</sup>lt;sup>2</sup> En el anexo I se puede ver el desglose de puntuación de cada una de los talleres.







Según esto, **las seleccionadas** para el programa de CyberCamp 2019 son las propuestas que se enumeran a continuación:

	Título	Candidato	Puntuación
1	Auditoría y hacking a dispositivos Bluetooth Low-Energy (BLE)	PGP	92
2	¡Y se Armó la Marimorena! Seguridad en Realidad Aumentada.	JC	88
3	Explotación de vulnerabilidades en el micro código de las CPUs	PC	85,5
4	Pentesting Hero: Los superpoderes de la postexplotación a	AN - RC	85,5
	través de iBombShell		
5	Detección de amenazas a escala con OSCTRL	JMP	85,5
6	HW Y SW para Redteam y Blueteam en redes WiFi DG		81,5
7	7 Threat Hunting con Sysmon RAJ		79,5
8	OSINT e Ingeniería Social como vectores de ataque a la	CS	77
	ciberseguridad		

Como <u>reservas</u> para el programa de CyberCamp 2019 en la modalidad de Talleres Técnicos se enumeran las propuestas siguientes:

	Título	Candidato	Puntuación
1	Threat Hunting y simulación de ataques	LDR	76
2	Forense para Salvar Vidas al Volante	MLG	74,5
3	Taller - Avances en criptografía moderna y privacidad de datos	AMM	72,5
4	Desarrolla aplicaciones OSINT con Python: buscadores, big	JC	72
	data y clustering		
5	DFIR en Windows ¿Qué me llevo?	LM	71,5
6	Procedimientos de RedTeam utilizando TOR.	DEM	70,5
7	Incident response con The Hive y Cortex	MRL	69,5
8	Desarrollo seguro y análisis de código	CCR	69
9	Introduccion a los CTF's con el entrenador del equipo nacional	BM	69
	(Bi-Campeon Europeo)		
10	Hacking y Forense de Vehiculos	NL	66,5
11	Detección de procesos maliciosos con Volatility	RJR	66,5

Aquellas propuestas (1) que no hubieron alcanzado un **mínimo de 60 puntos** quedaron descartadas.

Auditoría de aplicaciones web







#### TALLERES TÉCNICOS DE INICIACIÓN

Lo criterios de valoración son:

■ Enfoque práctico de la propuesta. Puntos asignados: de 0 a 40 puntos. Se establecen los siguientes sub-criterios de valoración:

Puntuación	Índice de valoración	
	El taller tiene en cuenta aspectos particulares como:	
0 – 30 puntos	Técnicas para el reconocimiento y defensa contra amenazas de seguridad.  La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros.  Nuevos sistemas de defensa de ciberseguridad.  Nuevas líneas de investigación de ciberseguridad.  Identificación de herramientas prácticas	
	El taller plantea un enfoque práctico para que el público objetivo	
0 – 10 puntos	adquiera los conocimientos de manera sencilla y adaptable a sus propias necesidades formativas.	

■ **Temática.** Puntos asignados: de 0 a 30 puntos. Se establecen los siguientes sub-criterios de valoración:

Puntuación	Índice de valoración
0 – 15 puntos	La temática propuesta aporta un enfoque diferenciador en el ámbito de la ciberseguridad, favoreciendo progresos científicos o tecnológicos.
La temática propuesta se encuentra dentro del listado de temo que se presumen de interés aportando un enfoque innovador sob el mismo.	
0 – 5 puntos	El esquema de la presentación es adecuado para el público objetivo y la temática presentada.

**Demostración** Se valorará si el taller incluye demostraciones y los minutos estimados que conllevará esta parte práctica. Puntos asignados: de 0 a 20 puntos

Puntuación = (20 * minutos demostración) / 90	
---	--

Siendo 90 los minutos máximos de demostración propuestos

Recursos didácticos. Puntos asignados: de 0 a 10 puntos.
Se valorará la inclusión y adecuación de medios y recursos materiales o conceptuales como apoyo a la exposición con la finalidad de facilitar su comprensión.

El número de propuestas recibidas en esta modalidad es de 17.







Una vez deliberado por el Jurado y analizadas las propuestas, han resultado seleccionadas para ser presentadas en CyberCamp un total de **4 Talleres técnicos de iniciación** correspondientes a aquellas que han obtenido una mejor valoración<sup>3</sup>.

Según esto, **las seleccionadas** para el programa de CyberCamp 2019 son las propuestas que se enumeran a continuación:

	Título	Candidato	Puntuación
1	Entornos SecDevOps(DevSecOps) dockerizados	AJ	85
2	Hack Like a Pro: Cómo encontrar sistemas vulnerables usando meta-buscadores	PV	80,5
3	La llamada de la muerte	JP	80,5
4	Hacker por un día	RR - MS	73

Como <u>reservas</u> para el programa de CyberCamp 2019 en la modalidad de Talleres Técnicos se enumeran las propuestas siguientes:

	Título	Candidato	Puntuación
1	Análisis de Ciberseguridad en el Internet de las Cosas	JR	69,5
2	Microcontroladores: los caminos para encontrar la diversión en	AN – RC	69,5
	la ciberseguridad		
3	Hardware y Software para Redteam y Blueteam en redes WiFi	DG	65,5
4	El maletín de un Hacker	CG	65,5
5	Introducción al Hacking con el entrenador del equipo nacional	BM	64
	(Para todas las edades)		
6	Simulación de ataques	CC	63
7	Desarrollo de CTF como método de autoaprendizaje en	GL	61,5
	Ciberseguridad.		

Aquellas propuestas (6) que no hubieron alcanzado un **mínimo de 60 puntos** quedaron descartadas.

- Machine Learning aplicado a la Ciberseguridad a través de los videojuegos
- Fortificación de sistemas Windows
- Taller de seguridad de aplicaciones
- La Amenaza Gamer

Como enfrentarnos a la vigilancia masiva

Security Awareness (because learning can be funny)

<sup>&</sup>lt;sup>3</sup> En el anexo I se puede ver el desglose de puntuación de cada una de los talleres.







#### CHARLAS INSPIRACIONALES Y DE PROMOCIÓN DEL TALENTO

Lo criterios de valoración son:

■ Valor motivacional. Puntos asignados: de 0 a 45 puntos (sub-criterios no incrementales).

Puntuación	Índice de valoración				
0 a 15 puntos	Valor testimonial: La propuesta incluye experiencias personale				
del ponente o evidencia casos de éxito adecuados.					
0 a 15 puntos	Mensaje: Se valorará la inclusión y adecuación de los mensajes y				
o a 15 puntos	propuestas de acción claras y accionables.				
0 a 15 puntos	Carácter divulgativo de la charla. La charla es de fácil				
o a 15 punios	comprensión y el ponente utiliza un vocabulario estándar.				

■ **Temática.** Puntos asignados: de 0 a 45 puntos (sub-criterios no incrementales).

Puntuación	Índice de valoración		
0 a 15 puntos	Innovación y diferenciación. La temática propuesta aporta un enfoque diferenciador en el ámbito de la promoción del talento en ciberseguridad		
O a 15 puntos  Concreción y profundidad de tratamiento. La temáti propuesta ofrece un tratamiento profundo de alguno de la aspectos identificados dentro de las temáticas propuestas.			
0 a 15 puntos	<b>Claridad expositiva.</b> La estructura de la propuesta es adecuada y favorece la asimilación por parte de los asistentes.		

■ Carácter inédito. Puntos asignados: de 0 a 10 puntos (sub-criterios incrementales).

Puntuación =  $10 - n^0$  congresos en los que se ha presentado anteriormente la propuesta presentada.

El número de propuestas recibidas en esta modalidad es de 15.

Una vez deliberado por el Jurado y analizadas las propuestas, han resultado seleccionadas para ser presentadas en CyberCamp un total de **3 Charlas inspiracionales y de Promoción del Talento** correspondientes a aquellas que han obtenido una mejor valoración<sup>4</sup>.

Según esto, **las seleccionadas** para el programa de CyberCamp 2019 son las propuestas que se enumeran a continuación:

	Título	Candidato	Puntuación
1	Quiero dedicarme a la ciberseguridad ¿y ahora qué?	VD	87,5
2	Del rojo al azul	JAAP	85
3	¿Qué hay en la mochila de un hacker?	YC	84.5

Como <u>reservas</u> para el programa de CyberCamp 2019 en la modalidad de Talleres Técnicos se enumeran las propuestas siguientes:

	Título	Candidato	Puntuación
1	Ética Hacker	IBQ	84

<sup>&</sup>lt;sup>4</sup> En el anexo I se puede ver el desglose de puntuación de cada una de las charlas.







	Título	Candidato	Puntuación
2	Cómo montar un SOC en casa	AA	83,5
3	Papá: soy forense tecnológico	FMA	82,5
4	El nuevo horizonte de sucesos de la ciberseguridad	MA	81,5
5	Cybersecurity Life 101 (Hack yourself)	JEJM	81
6	Tanto en la vida cómo en la ciberseguridad el talento gana	SV	79,5
	partidos, pero el trabajo en equipo gana campeonatos.'		
7	Formando cantera en ciberseguridad	ES	78,5
8	Si yo puedo tú puedes! Cómo empezar una carrera en el Ciber	BDL	76,5
	Espacio desde cero!		
9	Realización de informes OSINT con garantía judicial	SG	76
10	Mujeres Hackers: así revolucionaron (y revolucionan) la	FJRV	71
	informática y la ciberseguridad		
11	Los estándares de seguridad de la información: nuevos retos	ASG	70,5
	y oportunidades profesionales		

Aquellas propuestas (1) que no hubieron alcanzado un **mínimo de 60 puntos** quedaron descartadas.

Tú deberías ser Threat Hunter







#### CHARLAS DE CONCIENCIACIÓN

Lo criterios de valoración son:

■ Carácter divulgativo. Puntos asignados: de 0 a 50 puntos.

Puntuación	Índice de valoración
0 a 25 puntos	Información clara y objetiva. La charla propuesta incluye información clara que permita dar a conocer al público el tema de concienciación abordado por el ponente.
0 a 25 puntos	Adecuación al público objetivo. La charla es de fácil comprensión, y el ponente utiliza un vocabulario estándar para referirse a un tema de interés general.

Recursos didácticos. Puntos asignados: de 0 a 20 puntos.

Se valorará la inclusión y adecuación de medios y recursos materiales o conceptuales como apoyo a la exposición con la finalidad de facilitar su comprensión.

■ **Temática.** Puntos asignados: de 0 a 30 puntos (sub-criterios no incrementales).

Puntuación	Índice de valoración
0 a 15 puntos	Innovación y diferenciación. La temática propuesta aporta un enfoque diferenciador.
0 a 15 puntos	Concreción y profundidad de tratamiento. La temática propuesta ofrece un tratamiento profundo de alguno de los aspectos identificados dentro de las temáticas propuestas.

El número de propuestas recibidas en esta modalidad es de 14.

Una vez deliberado por el Jurado y analizadas las propuestas, han resultado seleccionadas para ser presentadas en CyberCamp un total de **4 Charlas de concienciación** correspondientes a aquellas que han obtenido una mejor valoración<sup>5</sup>.

Según esto, los seleccionados para el programa de CyberCamp 2019 son las propuestas que se enumeran a continuación:

	Título	Candidato	Puntuación
1	Mediación Parental en Internet: ¿Lo estoy haciendo bien?	GM	91,5
2	Jugando con fuego. Del sexting a la sextorsión y el grooming rondando	YC	81
3	Enseñando ciberseguridad a los más pequeños	JGAT	79,5
4	Uso responsable y seguro de Instagram y WhatsApp para padres, madres, educadores y jóvenes	JCCE	69,5

Como <u>reservas</u> para el programa de CyberCamp 2019 en la modalidad de Talleres Técnicos se enumeran las propuestas siguientes:

	Título	Candidato	Puntuación
1	Fraudes online. Casos reales y análisis de varios phishings utilizados en fraudes.	LDA	67,5

<sup>&</sup>lt;sup>5</sup> En el anexo I se puede ver el desglose de puntuación de cada una de las charlas.







	Título	Candidato	Puntuación
2	Cuida tu privacidad ¿sabes quién está tras la pantalla?	JRE	67

Aquellas propuestas (8) que no hubieron alcanzado un **mínimo de 60 puntos** quedaron descartadas.

- Los riesgos 4.0 de la cultura replicante
- GeneraZion: tus acciones cuentan
- ¿Qué (puedo) hacer con mi dron?
- Riesgos en internet: adicción y ciberacoso. Nuevos retos en salud.
- Grooming y pornográfia infantil, mucho más cerca de lo que piensas
- La responsabilidad digital es cosa de 3: alumnos, familias y colegios
- Educación digital en la familia y configuración de una herramienta de control parental
- La transformación digital de la policía

Para que así conste, se suscribe el presente acta.

En León a 21 de octubre de 2019







## **ANEXO I. VALORACIONES DE CADA PROPUESTA**

#### **VALORACIÓN PONENCIAS**

Cada una de las ponencias ha sido valorada por 2 miembros del jurado y la puntuación final de la misma se ha realizado haciendo la media aritmética de ambas puntuaciones:

Candidato	Título	Decisión	Total	Ptos. Jurado	Enfoque práctico 1	Enfoque práctico 2	Temática diferenciad	Temática interés	Temática esquema	Valor didáctico conocimie	Valor didáctico planteamie	Carácter inédito
JS	When a Pentester meets Machine Learning	Propuesta seleccionada	89	78,100	15,30	3,5	10,15	10,10	5,5	10,10	10,10	15,15
AF	Framework de ataque para el sector eléctrico, CAFFEINE	Propuesta seleccionada	87,5	75,100	20,30	3,5	10,15	9,10	4,5	7,10	7,10	15,15
TGMC	Hacking hardware en sistemas empotrados: De la preservación a la seguridad	Propuesta seleccionada	86	82,90	20,25	4,5	12,10	9,10	4,5	9,10	9,10	15,15
PGP	Emulación de adversarios: De entender ATT&CK a construir tu propia emulación	Propuesta seleccionada	85	90,80	20,25	5,4	15,12	10,7	5,3	10,7	10,7	15,15
JABG	Amenazas y camuflaje de comunicaciones Wi-Fi en entornos urbanos	Propuesta seleccionada	84,5	88,81	25,25	5,5	12,10	9,7	4,3	9,9	9,7	15,15
MRL	From crimeware ransomware to targeted ransomware - Let's evolution the ecosystem	Propuesta seleccionada	84	90,78	25,20	5,3	12,10	10,7	5,4	9,9	9,10	15,15
SS	Macro problemas, micro soluciones	Propuesta seleccionada	82	70,94	15,30	3,5	8,12	10,10	5,5	10,9	5,9	14,14
JMMC	Plug in the Middle	Propuesta seleccionada	80	85,75	25,20	4,4	10,10	9,7	4,4	10,9	9,7	14,14







Candidato	Título	Decisión	Total	Ptos. Jurado	Enfoque práctico 1	Enfoque práctico 2	Temática diferenciad	Temática interés	Temática esquema	Valor didáctico conocimie	Valor didáctico planteamie	Carácter inédito
JCSN	Las peripecias de un Perito Informático	Propuesta reserva	79,5	81,78	20,20	4,4	12,10	7,7	4,4	10,9	9,9	15,15
EMCC	Raspberry pi como control de seguridad perimetral	Propuesta reserva	78	82,74	25,20	3,4	12,8	7,7	4,4	7,9	9,7	15,15
RAJ	Ataques Malwareless El auge de los "lolbins"	Propuesta reserva	76	88,64	25,15	5,4	12,8	10,5	4,4	9,7	9,7	14,14
FPD	Visión práctica del nuevo reglamento europeo de ciberseguridad	Propuesta reserva	75,5	70,81	15,25	5,4	10,10	7,7	4,4	7,7	7,9	15,15
MMP	Evaluación de similitud de procesos de Windows mediante algoritmos de coincidencia aproximada	Propuesta reserva	75	67,83	20,25	4,3	8,12	7,9	3,3	7,9	5,9	13,13
RJR	Detección de malware en volcados de memoria: Desafíos y Problemas Actuales	Propuesta reserva	74	81,67	25,20	4,3	10,5	7,5	4,5	9,7	7,7	15,15
ES	Técnicas de Balización en diferentes entornos de la red	Propuesta reserva	74	88,60	25,20	4,3	15,8	9,5	4,3	7,3	9,3	15,15
CLT	Hacking Psicológico: Psicología de un ciberataque	Propuesta reserva	73	73,73	20,15	4,4	10,12	7,7	4,5	7,9	7,7	14,14
AMM	UNICODE attacks from scratch.  New proposals to avoid countermeasures	Propuesta reserva	71,5	59,84	20,25	0,5	0,10	10,7	5,5	5,9	5,9	14,14
PV	RIoT - Riesgos y retos de ciberseguridad y privacidad en IoT	Propuesta reserva	71,5	59,84	15,20	3,5	8,10	5,10	3,5	5,9	5,10	15,15
VD	La ciberseguridad y el factor humano	Propuesta reserva	71	68,74	15,20	5,4	8,10	7,7	4,4	9,7	5,7	15,15
PC	Spoofing Tire Pressure Monitoring Systems (TPMS)	Propuesta reserva	70,5	81,60	20,20	5,3	10,8	9,5	4,3	9,3	9,3	15,15
CCR	Ciberseguridad en el ámbito sanitario	Propuesta reserva	68,5	70,67	15,15	3,3	12,12	9,7	3,4	7,7	7,5	14,14







Candidato	Título	Decisión	Total	Ptos. Jurado	Enfoque práctico 1	Enfoque práctico 2	Temática diferenciad	Temática interés	Temática esquema	Valor didáctico conocimie	Valor didáctico planteamie	Carácter inédito
JTV	Encadenando la confianza a la cadena de confianza, el último reto de blockchain.	Propuesta reserva	67,5	49,86	5,25	1,3	8,15	5,10	3,4	7,7	5,7	15,15
JC	Desensamblando la web: Las ventajas, vulnerabilidades y riesgos de Web Assembly.	Propuesta reserva	67	77,57	25,15	3,3	12,5	5,5	5,4	7,5	5,5	15,15
JME	Free tour: la industria del cibercrimen	Propuesta reserva	67	61,73	15,20	3,4	5,8	5,5	4,5	7,9	7,7	15,15
LAO	Análisis de ciberataques en honeypots	Propuesta reserva	66,5	61,72	15,20	4,3	5,8	5,7	4,4	7,9	7,7	14,14
SG	Diario de un detective en el ciberespacio	Propuesta reserva	65,5	54,77	15,20	5,3	5,10	5,9	1,4	5,7	3,9	15,15
JMDCG	Contrainteligencia en Apoyo a Ciberinteligencia	Propuesta reserva	65	70,60	20,20	0,1	10,5	5,3	4,4	9,7	7,5	15,15
SRF	Tu tesoro en el bolsillo: (in)seguridad en Smartphone	Propuesta reserva	64	76,52	20,10	5,3	8,5	5,5	4,4	10,5	9,5	15,15
RG	Santa Rita Rita, lo que publicas ya no se quita	Propuesta reserva	62	60,64	15,20	4,5	8,5	3,3	3,4	7,7	7,7	13,13
RSP	Resolviendo las 10 preguntas	Propuesta reserva	61,5	57,66	10,15	3,3	10,8	3,7	4,4	5,7	7,7	15,15
JM	No disimules y simula: Simulación de adversarios	Propuesta descartada	58,5	56,61	15,15	3,3	5,5	5,5	5,4	3,9	5,5	15,15
CR	La inmutabilidad de Blockchain y la ciberseguridad	Propuesta descartada	55	39,71	5,15	1,1	5,15	5,9	3,5	3,5	3,7	14,14
FC	Ciberseguridad al alcance de la pyme	Propuesta descartada	53,5	62,45	15,15	3,1	10,5	7,3	1,1	7,3	5,3	14,14
CEM	Cloud Big Data Security	Propuesta descartada	50,5	56,45	15,10	1,1	8,5	5,5	4,3	5,3	3,3	15,15
DSJ	Ingeniería social, el Dios de muchos rostros	Propuesta descartada	49	39,59	15,15	0,3	0,8	5,5	1,3	3,5	0,5	15,15







Candidato	Título	Decisión	Total	Ptos. Jurado	Enfoque práctico 1	Enfoque práctico 2	Temática diferenciad	Temática interés	Temática esquema	Valor didáctico conocimie	Valor didáctico planteamie	Carácter inédito
JA	¿Por qué el phishing sigue siendo tan efectivo?	Propuesta descartada	42	27,57	5,15	1,4	0,5	0,3	0,1	3,7	3,7	15,15
AJ	SecDevOps(DevSecOps) con contenedores en los dockers	Propuesta descartada	40,5	33,48	5,10	1,0	5,5	3,7	3,3	0,5	3,5	13,13
FLAP	Intelligence-Led Cyber Attack Methodology	Propuesta descartada	37,5	29,46	10,10	0,3	0,8	3,3	1,4	3,3	0,3	12,12
MBB	La Importancia de la verdadera concienciación y la sensibilización de usuarios en ciberseguridad.	Propuesta descartada	36	29,43	0,0	3,3	0,8	5,5	1,3	3,5	3,5	14,14
LDR	Una introducción al Threat Hunting	Propuesta descartada	33	41,25	10,0	1,1	0,0	5,3	5,1	3,3	3,3	14,14







#### **VALORACIÓN TALLERES TÉCNICOS**

Cada uno de los talleres ha sido valorado por 2 miembros del jurado y la puntuación final de la misma se ha realizado haciendo la media aritmética de ambas puntuaciones

Candidato	Título	Decisión	Total	Ptos. Jurado	Enfoque práctico 1	Enfoque práctico 2	Temática diferencia dora	Temática interés	Temática esquema	Demostrac ión práctica	Carácter inédito
PGP	Auditoría y hacking a dispositivos Bluetooth Low-Energy (BLE)	Propuesta seleccionada	92	94,90	25,30	10,10	15,15	9,10	5,5	20,10	10,10
JC	¡Y se Armó la Marimorena! Seguridad en Realidad Aumentada.	Propuesta seleccionada	88	88,88	25,25	9,9	15,12	5,9	4,3	20,20	10,10
PC	Explotación de vulnerabilidades en el micro código de las CPUs	Propuesta seleccionada	85,5	84,87	25,25	9,10	10,12	7,7	5,5	20,20	8,8
ANRC	Pentesting Hero: Los superpoderes de la postexplotación a través de iBombShell	Propuesta seleccionada	85,5	82,89	20,25	10,9	10,12	9,9	4,5	20,20	9,9
JMP	Detección de amenazas a escala con osctrl	Propuesta seleccionada	85,5	86,85	30,25	10,10	10,10	3,7	4,4	20,20	9,9
DG	Hardware y software para redteam y blueteam en redes wifi	Propuesta seleccionada	81,5	63,100	15,30	5,10	5,15	5,10	3,5	20,20	10,10
RAJ	Threat Hunting con Sysmon	Propuesta seleccionada	79,5	68,91	15,30	10,10	5,10	5,7	4,5	20,20	9,9
CS	OSINT e ingeniería social: como vectores de ataque a la ciberseguridad	Propuesta seleccionada	77	92,62	30,15	10,3	10,5	7,5	5,4	20,20	10,10
LDR	Threat Hunting y simulación de ataques	Propuesta reserva	76	75,77	25,25	7,9	12,10	7,9	4,4	10,10	10,10
MLG	Forense para Salvar Vidas al Volante	Propuesta reserva	74,5	73,76	15,20	10,7	8,10	5,5	5,4	20,20	10,10
AMM	Taller - Avances en criptografía moderna y privacidad de datos	Propuesta reserva	72,5	63,82	15,25	5,10	10,12	9,10	4,5	10,10	10,10







Candidato	Título	Decisión	Total	Ptos. Jurado	Enfoque práctico 1	Enfoque práctico 2	Temática diferencia dora	Temática interés	Temática esquema	Demostrac ión práctica	Carácter inédito
JC	Desarrolla aplicaciones OSINT con Python: buscadores, big data y clustering	Propuesta reserva	72	64,80	25,30	10,9	5,12	5,9	4,5	5,5	10,10
LM	DFIR en Windows ¿Qué me llevo?	Propuesta reserva	71,5	63,80	15,20	10,7	0,10	5,10	5,5	20,20	8,8
DEM	Procedimientos de RedTeam utilizando TOR.	Propuesta reserva	70,5	65,76	15,20	7,9	5,8	5,5	3,4	20,20	10,10
MRL	Incident response con The Hive y Cortex	Propuesta reserva	69,5	70,69	15,20	10,5	5,8	5,5	5,1	20,20	10,10
CCR	Desarrollo seguro y análisis de código	Propuesta reserva	69	62,76	15,20	5,9	5,8	3,5	4,4	20,20	10,10
BM	Introducción a los CTF's con el entrenador del equipo nacional (Bi-Campeon Europeo)	Propuesta reserva	69	79,59	20,10	7,5	10,8	7,3	5,3	20,20	10,10
NL	Hacking y Forense de Vehículos	Propuesta reserva	66,5	65,68	10,20	10,7	10,10	10,7	5,4	10,10	10,10
RJR	Detección de procesos maliciosos con Volatility	Propuesta reserva	65,5	54,77	10,20	3,7	5,10	5,7	1,3	20,20	10,10
JNC	Auditoría de aplicaciones web	Propuesta descartada	41,5	31,52	10,20	3,7	5,5	3,7	1,4	0,0	9,9







#### VALORACIÓN TALLERES TÉCNICOS DE INICIACIÓN

Cada uno de los talleres ha sido valorado por 2 miembros del jurado y la puntuación final de la misma se ha realizado haciendo la media aritmética de ambas puntuaciones

Candidato	Título	Decisión	Total	Ptos. Jurado	Enfoque práctico 1	Enfoque práctico 2	Temática diferenciador a	Temática interés	Temática esquema presentación	Demostración práctica	Recursos didácticos
AJ	Entornos SecDevOps(DevSecOps) dockerizados	Propuesta seleccionada	85	74,96	15,30	9,10	10,12	7,10	4,4	20,20	9,10
JP	La llamada de la muerte	Propuesta seleccionada	80,5	75,86	10,20	10,9	10,15	10,9	5,4	20,20	10,9
PV	Hack Like a Pro: Cómo encontrar sistemas vulnerables usando meta-buscadores	Propuesta seleccionada	80,5	91,70	30,20	10,7	12,10	9,7	5,4	15,15	10,7
RS - MS	Hacker por un día	Propuesta seleccionada	73	83,63	25,15	10,7	10,8	9,7	5,4	15,15	9,7
JR	Análisis de Ciberseguridad en el Internet de las Cosas	Propuesta reserva	69,5	70,69	25,25	9,7	10,10	7,9	4,4	10,5	5,9
AN - RC	Microcontroladores: los caminos para encontrar la diversión en la ciberseguridad	Propuesta reserva	69,5	68,71	10,15	7,9	12,10	7,5	3,5	20,20	9,7
DG	Hardware y Software para Redteam y Blueteam en redes WiFi	Propuesta reserva	65,5	54,77	10,25	7,9	5,8	5,7	3,4	15,15	9,9
CG	El maletín de un Hacker	Propuesta reserva	65,5	68,63	25,20	7,5	8,8	7,9	4,4	10,10	7,7
ВМ	Introducción al Hacking con el entrenador del equipo nacional (Para todas las edades)	Propuesta reserva	64	60,68	15,25	10,5	5,5	5,10	5,4	10,10	10,9
CC	Simulación de ataques	Propuesta reserva	63	63,63	20,20	7,7	8,8	7,7	4,4	10,10	7,7
GL	Desarrollo de CTF como método de autoaprendizaje en Ciberseguridad.	Propuesta reserva	61,5	54,69	20,25	7,7	10,12	7,9	3,4	0,5	7,7







Candidato	Título	Decisión	Total	Ptos. Jurado	Enfoque práctico 1	Enfoque práctico 2	Temática diferenciador a	Temática interés	Temática esquema presentación	Demostración práctica	Recursos didácticos
FJRV	Machine Learning aplicado a la Ciberseguridad a través de los videojuegos	Propuesta descartada	54	48,60	10,15	5,9	5,10	10,7	3,5	5,5	10,9
FPD	Fortificación de sistemas Windows	Propuesta descartada	49	40,58	10,15	7,7	5,8	0,9	3,4	10,10	5,5
LS	Taller de seguridad de aplicaciones	Propuesta descartada	46	58,34	20,10	10,3	8,5	5,5	1,1	5,5	9,5
AN	LA AMENAZA GAMER Taller práctico sobre seguridad en videojuegos online	Propuesta descartada	43,5	34,53	15,20	3,3	0,8	0,0	1,5	10,10	5,7
JNC	Como enfrentarnos a la vigilancia masiva	Propuesta descartada	42,5	44,41	5,15	5,5	5,8	3,5	1,3	20,0	5,5
CEM	Security Awareness (because learning can be funny)	Propuesta descartada	40,5	35,46	5,15	5,5	5,5	5,5	0,3	10,10	5,3







#### VALORACIÓN CHARLAS INSPIRACIONALES Y DE PROMOCIÓN DEL TALENTO

Cada una de las charlas ha sido valorada por 2 miembros del jurado y la puntuación final de la misma se ha realizado haciendo la media aritmética de ambas puntuaciones.

Candidato	Título	Decisión	Total	Ptos. Jurado	Valor testimonial	Mensaje	Carácter divulgativo	Innovación	Concreción	Claridad expositiva	Carácter inédito
VD	Quiero dedicarme a la ciberseguridad ¿y ahora qué?	Propuesta seleccionada	87,5	84,91	15,15	10,12	12,12	10,12	12,15	15,15	10,10
JAAP	Del rojo al azul	Propuesta seleccionada	85	88,82	15,12	12,12	12,12	12,12	12,12	15,12	10,10
YC	¿Qué hay en la mochila de un hacker?	Propuesta seleccionada	84,5	91,78	15,10	15,12	12,12	12,10	12,12	15,12	10,10
IBQ	Ética Hacker	Propuesta reserva	84	94,74	12,15	12,8	15,12	15,12	15,12	15,5	10,10
AA	Cómo montar un SOC en casa	Propuesta reserva	83,5	82,85	15,15	12,15	8,15	12,10	12,12	15,10	8,8
FMA	Papá: soy forense tecnológico	Propuesta reserva	82,5	86,79	15,12	12,12	12,12	10,8	12,10	15,15	10,10
MA	El nuevo horizonte de sucesos de la ciberseguridad	Propuesta reserva	81,5	78,85	10,15	12,12	10,12	12,12	10,10	15,15	9,9
JEJM	Cybersecurity Life 101 (Hack yourself)	Propuesta reserva	81	88,74	15,12	12,12	12,12	12,8	12,10	15,10	10,10
SV	Tanto en la vida cómo en la ciberseguridad el talento gana partidos, pero el trabajo en equipo gana campeonatos.'	Propuesta reserva	79,5	75,84	10,15	10,15	8,12	10,12	12,10	15,10	10,10
ES	Formando cantera en ciberseguridad	Propuesta reserva	78,5	66,91	10,12	10,15	10,15	8,12	10,12	8,15	10,10







Candidato	Título	Decisión	Total	Ptos. Jurado	Valor testimonial	Mensaje	Carácter divulgativo	Innovación	Concreción	Claridad expositiva	Carácter inédito
BDL	Si yo puedo tú puedes! Cómo empezar una carrera en el Ciber Espacio desde cero!	Propuesta reserva	76,5	89,64	15,10	15,8	12,8	10,8	15,10	12,10	10,10
SG	Realización de informes OSINT con garantía judicial	Propuesta reserva	76	73,79	15,15	10,12	12,12	10,10	8,10	8,10	10,10
FJRV	Mujeres Hackers: así revolucionaron (y revolucionan) la informática y la ciberseguridad	Propuesta reserva	71	82,60	12,5	12,5	15,10	10,10	8,10	15,10	10,10
ASG	Los estándares de seguridad de la información: nuevos retos y oportunidades profesionales	Propuesta reserva	70,5	74,67	10,8	12,8	10,10	10,8	10,8	12,15	10,10
СМ	Tú deberías ser Threat Hunter	Propuesta descartada	44,5	53,36	5,5	8,5	5,8	12,8	8,0	5,0	10,10







#### VALORACIÓN CHARLAS CONCIENCIACIÓN

Cada una de las charlas ha sido valorada por 2 miembros del jurado y la puntuación final de la misma se ha realizado haciendo la media aritmética de ambas puntuaciones

Candidato	Título	Decisión	Total	Ptos jurado	Claridad	Adecuación	Recursos didácticos	Temática innovadora	Tratamiento
GM	Mediación Parental en Internet: ¿Lo estoy haciendo bien?	Propuesta seleccionada	91,5	91,92	25,25	25,22	17,15	12,15	12,15
YC	Jugando con fuego. Del sexting a la sextorsión y el grooming rondando	Propuesta seleccionada	81	79,83	22,20	20,22	15,17	10,12	12,12
JGAT	Enseñando ciberseguridad a los más pequeños	Propuesta seleccionada	79,5	77,82	25,20	20,25	15,10	12,15	5,12
JCE	Uso responsable y seguro de Instagram y WhatsApp para padres, madres, educadores y jóvenes	Propuesta reserva	69,5	72,67	22,15	15,15	15,17	12,12	8,8
LDA	Fraudes online. Casos reales y análisis de varios phishings utilizados en fraudes.	Propuesta reserva	67,5	79,56	20,15	22,20	17,5	8,8	12,8
JRE	Cuida tu privacidad ¿sabes quién está tras la pantalla?	Propuesta reserva	67	70,64	20,15	20,20	10,5	10,12	10,12
MA	Los riesgos 4.0 de la cultura replicante	Propuesta descartada	57	57,57	20,20	10,10	5,5	12,12	10,10
EM	GeneraZion: tus acciones cuentan	Propuesta descartada	53	54,52	22,15	0,0	10,17	12,10	10,10
JSJ	¿Qué (puedo) hacer con mi dron?	Propuesta descartada	50,5	56,45	15,20	15,5	10,5	8,5	8,10
MAAG	Riesgos en internet: adicción y ciberacoso. Nuevos retos en salud.	Propuesta descartada	49,5	46,53	15,15	5,15	10,5	8,8	8,10
DSJ	Grooming y pornografía infantil, mucho más cerca de lo que piensas	Propuesta descartada	49	50,48	15,15	10,10	10,10	10,5	5,8







Candidato	Título	Decisión	Total	Ptos jurado	Claridad	Adecuación	Recursos didácticos	<b>Temática</b> innovadora	Tratamiento
RP	La responsabilidad digital es cosa de 3: alumnos, familias y colegios	Propuesta descartada	49	48,50	20,15	10,15	10,5	0,5	8,10
DC	Educación digital en la familia y configuración de una herramienta de control parental	Propuesta descartada	39	43,35	20,15	0,0	10,10	8,10	5,0
AN	La transformación digital de la policía	Propuesta descartada	39	68,10	20,5	15,5	15,0	10,0	8,0







# ANEXO II. FORMULARIOS DE VALORACIÓN EN **HERRAMIENTA**

PON	IENCIA MAGIS	STRAL
- Técr de nu o siste	nicas para el recono evas vulnerabilidad emas desarrollados	riterio 1.* De 0 a 30 puntos. La ponencia tiene en cuenta aspectos particulares como: cimiento y defensa contra amenazas de seguridad La exposición y/o descubrimiento es de ciberseguridad, propias o de terceros Presentación de nuevas herramientas en ciberseguridad Distribución pública de las herramientas presentadas Nuevos ciberseguridad Nuevas líneas de investigación de ciberseguridad.
0	30: Excelente	
0	25: Sobresaliente	
0	20: Notable	
0	15: Suficiente	
0	10: Insuficiente	
0	5: Muy deficiente	
0	0: Descartada	
públic	o objetivo adquiera	criterio 2.* De 0 a 5 puntos. La propuesta plantea un enfoque práctico para que el conocimiento de carácter práctico en sus propios ámbitos de actuación y tenga una tro del ámbito de actuación del asistente.
0	5: Sobresaliente	
0	4: Notable	
0	3: Suficiente	
0	1: Insuficiente	
0	0: Descartada	
		- diferenciadora.* De 0 a 15 puntos. La temática propuesta aporta un enfoque o de la ciberseguridad, favoreciendo progresos científicos o tecnológicos.
0	15: Excelente	, , , , , , , , , , , , , , , , , , , ,
_		

12: Sobresaliente







0	10: Notable
0	8: Suficiente
0	5: Insuficiente
0	0: Descartado
	tica. Subcriterio 2 nas que se presum
Ö	10: Excelente
0	9: Sobresaliente
0	7: Notable
0	5: Suficiente
0	3: Insuficiente
0	0: Descartada
<b>emá</b> t decu	tica. Subcriterio 3 ado para el público
0	5: Excelente
0	4: Notable
0	3: Suficiente
0	1: Insuficiente
0	0: Descartada
alor	didáctico - conoc
0	10: Excelente
0	9: Sobresaliente
0	7: Notable







0	5: Suficiente
0	3: Insuficiente
0	0: Descartada
Valor didác	didáctico - plante tico garantiza el éx
0	10: Excelente
0	9: Sobresaliente
0	7: Notable
0	5: Suficiente
0	3: Insuficiente
0	0: Descartada
Caráo	cter inédito.* De 0
0	15: 0 congresos
0	14: 1 congreso
0	13: 2 congresos
0	12: 3 congresos
0	11: 4 congresos
0	10: 5 congresos
0	9: 6 congresos
0	8: 7 congresos
0	7: 8 congresos
0	6: 9 congresos







0	5: 10 congresos
0	4: 11 congresos
0	3: 12 congresos
0	2: 13 congresos
0	1: 14 o más congresos

#### **TALLER TÉCNICO**

**Enfoque práctico. Subcriterio 1.\*** De 0 a 30 puntos. El taller tiene en cuenta aspectos particulares como: - Técnicas para el reconocimiento y defensa contra amenazas de seguridad. - La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros. - Divulgación responsable de exploits 0-day, propios o de terceros. - Presentación de nuevas herramientas o sistemas desarrollados en ciberseguridad, bien si son desarrollos propios o de terceros. - Distribución pública de las herramientas presentadas. - Nuevos sistemas de defensa de ciberseguridad. - Nuevas líneas de investigación de ciberseguridad.

0	30: Excelente
0	25: Sobresaliente
0	20: Notable
0	15: Suficiente
0	10: Insuficiente
0	5: Muy deficiente
0	0: Descartada

**Enfoque práctico de la propuesta. Subcriterio 2.\*** De 0 a 10 puntos. El taller plantea un enfoque práctico para que el público objetivo adquiera conocimiento de carácter práctico en sus propios ámbitos de actuación y tenga una implantación sencilla dentro del ámbito de actuación del asistente.

0	10: Excelente
0	9: Sobresaliente
0	7: Notable







5: Suficiente
3: Insuficiente
0: Descartada
tica. Subcriterio 1
nciador en el ámbi
15: Excelente
12: Sobresaliente
10: Notable
8: Suficiente
5: Insuficiente
0: Descartado
tica. Subcriterio 2 nas que se presum
10: Excelente
9: Sobresaliente
7: Notable
7: Notable 5: Suficiente
5: Suficiente
<ul><li>5: Suficiente</li><li>3: Insuficiente</li><li>0: Descartada</li></ul>
<ul><li>5: Suficiente</li><li>3: Insuficiente</li></ul>
5: Suficiente 3: Insuficiente 0: Descartada tica. Subcriterio 3







0	3: Suficiente
0	1: Insuficiente
0	0: Descartada
Demo	ostración prácti
estim	ados que conlle
0	20: 60 minutos
0	15: 45 minutos
0	10: 30 minutos
0	5: 15 minutos
0	0: Menos de 15
Caráo	cter inédito.* De
0	10: 0 congreso
0	9: 1 congreso
0	_
	8: 2 congresos
0	7: 3 congresos
0	6: 4 congresos
0	5: 5 congresos
0	4: 6 congresos
0	3: 7 congresos
0	2: 8 congresos
0	1: 9 congresos
0	0: 10 congresos







### **TALLER DE INICIACIÓN**

Técnic descu defens	cas para el reconoci brimiento de nueva	criterio 1.* De 0 a 30 puntos. El taller tiene en cuenta aspectos particulares como: - cimiento y defensa contra amenazas de seguridad La exposición y/o les vulnerabilidades de ciberseguridad, propias o de terceros Nuevos sistemas de lad Nuevas líneas de investigación de ciberseguridad Identificación de
0	30: Excelente	
0	25: Sobresaliente	
0	20: Notable	
0	15: Suficiente	
0	10: Insuficiente	
0	5: Muy deficiente	
0	0: Descartada	
		riterio 2.* De 0 a 10 puntos. El taller plantea un enfoque práctico para que el público ocimientos de manera sencilla y adaptable a sus propias necesidades formativas.
	·	
0	10: Excelente	
0	9: Sobresaliente	
0	7: Notable	
0	5: Suficiente	
0	3: Insuficiente	
0	0: Descartada	
		- diferenciadora.* De 0 a 15 puntos. La temática propuesta aporta un enfoque o de la ciberseguridad, favoreciendo progresos científicos o tecnológicos.
-		
0	15: Excelente	
0	12: Sobresaliente	

10: Notable







0	8: Suficiente
0	5: Insuficiente
0	0: Descartado
	itica. Subcriterio 2 mas que se presum
0	10: Excelente
0	9: Sobresaliente
0	7: Notable
0	5: Suficiente
0	3: Insuficiente
0	0: Descartada
	itica. Subcriterio 3 uado para el público
0	E. Evenlant
_	5: Excelente
0	4: Notable
0	3: Suficiente
0	1: Insuficiente
0	0: Descartada
Demo	ostración práctica.
	ados que conllevar
0	20: 90 minutos
0	15: 65 minutos
0	10: 45 minutos







0	5: 20 minutos								
0	0: Menos de 20 mi	inutos							
	rsos didácticos.* Diales o conceptuales								
0	10: Excelente								
0	9: Sobresaliente								
0	7: Notable								
0	5: Suficiente								
0	3: Insuficiente								
0	0: Descartada								
CHA	ARLA INSPIRA	CION	AL Y DI	E PROI	MOCIÓI	N DEL 1	<b>FALENT</b>	0	
Valor	ARLA INSPIRA testimonial.* De 0 nte o evidencia caso	a 15 pur	itos. Valoi	r testimoni					onales del
Valor	testimonial.* De 0	a 15 pur	itos. Valoi	r testimoni					onales del
<b>Valor</b> poner	testimonial.* De 0 nte o evidencia caso	a 15 pur	itos. Valoi	r testimoni					onales del
Valor poner	testimonial.* De 0 nte o evidencia caso 15: Excelente	a 15 pur	itos. Valoi	r testimoni					onales del
Valor poner	testimonial.* De 0 nte o evidencia caso 15: Excelente 12: Sobresaliente	a 15 pur	itos. Valoi	r testimoni					onales del
Valor poner	testimonial.* De 0 nte o evidencia caso 15: Excelente 12: Sobresaliente 10: Notable	a 15 pur	itos. Valoi	r testimoni					onales del
Valor poner	testimonial.* De 0 nte o evidencia caso 15: Excelente 12: Sobresaliente 10: Notable 8: Suficiente	a 15 pur	itos. Valoi	r testimoni					onales del
Valor poner	testimonial.* De 0 nte o evidencia caso 15: Excelente 12: Sobresaliente 10: Notable 8: Suficiente 5: Insuficiente	a 15 pur os de éxit	itos. Valoi o adecuad	r testimoni dos.	ial: La prop	puesta inc	luye experi	encias pers	
Valor poner	testimonial.* De 0 nte o evidencia caso  15: Excelente  12: Sobresaliente  10: Notable  8: Suficiente  5: Insuficiente  0: Descartado	a 15 pur os de éxit	itos. Valoi o adecuad	r testimoni dos.	ial: La prop	puesta inc	luye experi	encias pers	







0	10: Notable			
0	8: Suficiente			
0	5: Insuficiente			
0	0: Descartado			
	cter divulgativo.* Donente utiliza un voc			
0	15: Excelente			
0	12: Sobresaliente			
0	10: Notable			
0	8: Suficiente			
0	5: Insuficiente			
0	0: Descartado			
	ación y diferencia			
un en	foque diferenciador			
0	15: Excelente			
0	12: Sobresaliente			
0	10: Notable			
0	8: Suficiente			
0	5: Insuficiente			
0	0: Descartado			
Concrección.* De 0 a 15 tratamiento profundo de a				
0	15: Excelente			







0	12: Sobresaliente				
0	10: Notable				
0	8: Suficiente				
0	5: Insuficiente				
0	0: Descartado				
<b>Claric</b> por pa	lad expositiva.* De arte de los asistente				
0	15: Excelente				
0	12: Sobresaliente				
0	10: Notable				
0	8: Suficiente				
0	5: Insuficiente				
0	0: Descartado				
Carácter inédito.* De 0 a 1					
0	10: 0 congresos				
0	9: 1 congreso				
0	8: 2 congresos				
0	7: 3 congresos				
0	6: 4 congresos				
0	5: 5 congresos				
0	4: 6 congresos				
0	3: 7 congresos				







0	2: 8 congresos	
0	1: 9 congresos	
0	0: 10 congresos o r	nás
CHA	ARLA DE CON	CIENCIACIÓN
		os. Información clara y objetiva. La charla propuesta incluye información clara que úblico el tema de concienciación abordado por el ponente.
0	25: Excelente	
0	22: Sobresaliente	
0	20: Notable	
0	15: Suficiente	
0	10: Insuficiente	
0	5: Muy deficiente	

**Adecuación.\*** De 0 a 25 puntos. Adecuación al público objetivo. La charla es de fácil comprensión, y el ponente utiliza un vocabulario estándar para referirse a un tema de interés general.

0	25: Excelente
0	22: Sobresaliente
0	20: Notable
0	15: Suficiente
0	10: Insuficiente
0	5: Muy deficiente
0	0: Descartada

0: Descartada







**Recursos didácticos.\*** De 0 a 20 puntos. Se valorará la inclusión y adecuación de medios y recursos materiales o conceptuales como apoyo a la exposición con la finalidad de facilitar su comprensión.

0	20: Excelente
0	17: Sobresaliente
0	15: Notable
0	10: Suficiente
0	5: Insuficiente
0	0: Descartada
	tica innovadora.* [ ue diferenciador.
Sinoqi	ao anorendiador.
0	15: Excelente
0	12: Sobresaliente
0	10: Notable
0	8: Suficiente
0	5: Insuficiente
0	0: Descartada
	miento.* De 0 a 15
tratam	niento profundo de a
0	15: Excelente
0	12: Sobresaliente
0	10: Notable
0	8: Suficiente
0	5: Insuficiente
0	0: Descartada