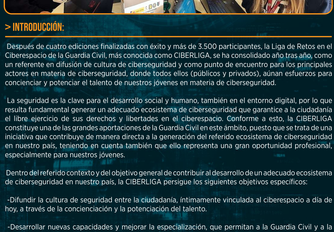
CYBERLEAGUE GC 2023
V LIGA DE RETOS EN EL CIBERESPACIO

COMPETICIÓN AMATEUR

"Una iniciativa de Seguridad Interior para poner en valor el talento de nuestros estudiantes desde una visión pluridisciplinar de la ciberseguridad."



> INTRODUCCIÓN:

Después de cuatro ediciones finalizadas con éxito y más de 3.500 participantes, la Liga de Retos en el Ciberespacio de la Guardia Civil, más conocida como CIBERLIGA, se ha consolidado año tras año, como un referente en el difusión de cultura de ciberseguridad y como punto de encuentro para los principales actores en materia de ciberseguridad, donde todos ellos (públicos y privados), aunan esfuerzos para concienciar y potenciar el talento de nuestros jóvenes en materia de ciberseguridad.

La seguridad es la clave para el desarrollo social y humano, también en el entorno digital, por lo que resulta fundamental generar un adecuado ecosistema de ciberseguridad que garantice a la ciudadanía el libre ejercicio de sus derechos y libertades en el ciberespacio. Conforme a esto, la CIBERLIGA constituye una de las grandes aportaciones de la Guardia Civil en este ámbito, puesto que se trata de una iniciativa que contribuye de manera directa a la generación del referido ecosistema de ciberseguridad en nuestro país, teniendo en cuenta también que ella representa una gran oportunidad profesional, especialmente para nuestros jóvenes.

Dentro del referido contexto y del objetivo general de contribuir al desarrollo de un adecuado ecosistema de ciberseguridad en nuestro país, la CIBERLIGA persigue los siguientes objetivos específicos:

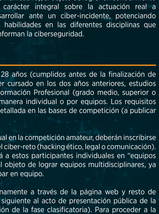
-Difundir la cultura de seguridad entre la ciudadanía, íntimamente vinculada al ciberespacio a día de hoy, a través de la concienciación y la potenciación del talento.

-Desarrollar nuevas capacidades y mejorar la especialización, que permitan a la Guardia Civil y a la administración pública en general, hacer frente a los retos y desafíos para la seguridad derivados del uso malintencionado del ciberespacio y de la actual brecha digital.

-Fomentar la coordinación y cooperación con todos los actores del ecosistema de la ciberseguridad.

> ¿EN QUÉ CONSISTE REALMENTE LA CIBERLIGA?:

La forma elegida por la Guardia Civil para alcanzar los ambiciosos objetivos establecidos, es a través del desarrollo de una divertida cyber-competición (proceso de gamificación), donde los participantes tienen la oportunidad de concienciarse y potenciar su talento en la materia, de una forma eminentemente práctica, que les permitirá profundizar en sus conocimientos sobre Ciberseguridad, tanto a nivel usuario como profesional (sector público y empresa privada).



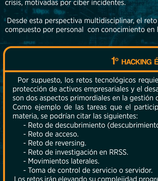
De manera concreta, se trata de una divertida cyber-competición que se desarrolla en una triple modalidad:

-En primer lugar, encontramos la modalidad "pre-amateur", orientada a estudiantes de 4º curso de la ESO, con el objetivo de concienciar.

-En segundo lugar, tenemos la modalidad "amateur, orientada a universitarios y de formación profesional, tanto nacionales e internacionales, con el objetivo de potenciar su talento.

-Por último, encontramos la modalidad "profesional", orientada a equipos de expertos pertenecientes principalmente al ámbito de la seguridad y la defensa.

Los participantes de las diferentes modalidades, desarrollan la competición de manera independiente, enfrentándose a divertidos retos, a través de los cuales se reproducen de manera muy aproximada, situaciones y cyber-incidentes reales. No obstante, todos ellos tendrán la increíble posibilidad de compartir experiencias y conocimientos durante la fase final.



> GENERALIDADES:

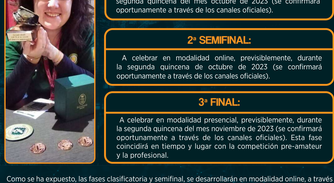
En la competición amateur, orientada a estudiantes universitarios y de formación profesional, los participantes tendrán que enfrentarse a un cyber-reto de naturaleza multidisciplinar (técnico, jurídico y comunicativo), al objeto de lograr un conocimiento de carácter integral sobre la actuación real a desarrollar ante un cyber-incidente, potenciando sus habilidades en las diferentes disciplinas que conforman la ciberseguridad.

> CÓMO PARTICIPAR:

Para participar, es imprescindible tener entre 18 y 28 años (cumplidos antes de la finalización de esta 2023). Además de ello, se debe cursar o haber cursado en los dos años anteriores, estudios Universitarios (grado, máster o doctorado) o de Formación Profesional (grado medio, superior o cursos de especialización), pudiendo participar de manera individual o por equipos. Los requisitos específicos de participación se recogen de manera detallada en las bases de competición (a publicar de manera oportuna en la web).

Aquellos interesados en participar de manera individual en la competición amateur, deberán inscribirse en una de las tres disciplinas específicas que integran el cyber-reto (hacking ético, legal o comunicación). En caso de superar la fase clasificatoria, se integrará a estos participantes individuales en "equipos fusión", junto con clasificados de otras disciplinas, al objeto de lograr equipos multidisciplinares, ya que en la fase semifinal y fin al sólo se puede participar en equipo.

El periodo de inscripciones se comunicará oportunamente a través de la página web y resto de canales oficiales (previsiblemente será desde el día siguiente al acto de presentación pública de la cuarta edición, hasta fechas próximas a la celebración de la fase clasificatoria). Para proceder a la inscripción, se habilitará el correspondiente formulario en la página donde web, donde también se podrá adjuntar la correspondiente documentación requerida.



> NATURALEZA DEL RETO:

La actual concepción de la ciberseguridad requiere de un amplio conocimiento en diversas disciplinas, puesto que nos encontramos ante una materia compleja que se conforma sobre la base de diferentes áreas de conocimiento.

A la hora de enfrentarse a un cyber incidente, es necesario un enfoque que no sea únicamente técnico. Por tanto, resulta fundamental conocer las responsabilidades jurídicas en que incurre una empresa que protege de forma inadecuada sus activos, provocando un daño a sus clientes o a terceros. Asimismo, toda organización necesita disponer de una adecuada política de comunicación para la gestión de crisis, motivadas por ciber incidentes.

Desde esta perspectiva multidisciplinar, el reto de la competición necesita equipos pluridisciplinares, compuesto por personal con conocimiento en las siguientes disciplinas:

1ª HACKING ÉTICO:

Por supuesto, los retos tecnológicos requieren de expertos en esta materia. La protección de activos empresariales y el desarrollo de programación colaborativa son dos aspectos primordiales en la gestión de la ciberseguridad.
Como ejemplo de las tareas que el participante va tener que afrontar en esta materia, se podrían citar las siguientes:
- Reto de descubrimiento (descubrimiento de red).
- Reto de acceso.
- Reto de reversing.
- Reto de investigación en RRSS.
- Movimientos laterales.
- Toma de control de servicio o servidor.

Los retos irán elevando su complejidad progresivamente y los participantes usarán todo el abanico de herramientas a su alcance para la resolución de éstos.

2ª LEGAL:

La adaptación al marco normativo, tanto nacional como europeo, resulta fundamental fundamental e indispensable a la hora de asegurar la supervivencia de una organización que debe enfrentarse a un ciber incidente. Dicho marco es realmente variado, pudiendo versar las posibles tareas a desarrollar en esta disciplina sobre diferentes áreas de conocimiento, como:
- Derecho digital.
- Protección de datos.
- Seguridad de la información.
- Compliance normativo.

3ª COMUNICACIÓN:

Una adecuada estrategia comunicativa ante una situación de crisis puede representar la diferencia entre que una organización sobreviva o no, puesto que la forma de gestionar la crisis sufrido por los efectos de un cyber incidente, puede ayudar a mitigar en gran medida los efectos adversos que pudieran derivarse de éste, especialmente en el ámbito reputacional.
Es por ello, que la resolución de cualquier incidente en materia de ciberseguridad debe contar con una adecuada estrategia comunicativa, por la gran trascendencia de los efectos que dicho incidente pueda generar, no sólo hacia la propia organización sino también hacia la totalidad de la ciudadanía.

CÓMO SE DESARROLLA

1ª CLASIFICATORIA:

A celebrar en modalidad online, previsiblemente, durante la segunda quincena del mes octubre de 2023 (se confirmará oportunamente a través de los canales oficiales).

2ª SEMIFINAL:

A celebrar en modalidad online, previsiblemente, durante la segunda quincena de octubre de 2023 (se confirmará oportunamente a través de los canales oficiales).

3ª FINAL:

A celebrar en modalidad presencial, previsiblemente, durante la segunda quincena del mes noviembre de 2023 (se confirmará oportunamente a través de los canales oficiales). Esta fase coincidirá en tiempo y lugar con la competición pre-amateur y la profesional.

Como se ha expuesto, las fases clasificatoria y semifinal, se desarrollarán en modalidad online, a través de un innovador metaverso que recreará con total similitud un entorno real, donde a parte del desarrollo de la competición, tendrán lugar otras divertidas actividades formativas.

CUGC CENTRO UNIVERSITARIO DE LA GUARDIA CIVIL

FUNDACIÓN GUARDIA CIVIL

GOBIERNO DE ESPAÑA · MINISTERIO DEL INTERIOR · DIRECCIÓN GENERAL DE LA GUARDIA CIVIL

https://www.nationalcyberleague.es/