Ibero-American CyberSecurity Challenge (ICSC)

Bases de la competición

ÍNDICE

1. INTRODUCCIÓN

La S.M.E Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE), la Secretaría General de la Organización de los Estados Americanos (SG/OEA) y el Banco Interamericano de Desarrollo (BID), en colaboración con la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) y con el respaldo del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación (MAEC), organizan el evento internacional Ibero-American CyberSecurity Challenge (ICSC), que se celebrará el 13 de diciembre de 2018 en la ciudad de Cartagena de Indias, Colombia.

Teniendo en cuenta el escenario tecnológico actual, en donde la proliferación de nuevas amenazas con un grado de sofisticación creciente se amplía día a día, surge la necesidad de incorporar profesionales expertos en ciberseguridad en distintos tipos de organismos y organizaciones.

Por ello, nos encontramos ante el desafío de gestionar nuevos riesgos y amenazas, fomentando el talento en ciberseguridad y ofreciendo a los jóvenes un área de trabajo con muchas oportunidades y una gran proyección.

El evento Ibero-American CyberSecurity Challenge (ICSC) es una competición en la que equipos de jóvenes talentos en ciberseguridad de distintos países Ibero-Americanos compiten entre sí, resolviendo ejercicios de ciberseguridad en una competición de tipo Capture The Flag (CTF). Este tipo de actividad implica que, en el menor tiempo posible, los equipos tienen que resolver pruebas relacionadas con ciberseguridad y las múltiples áreas, como puede ser la seguridad web, seguridad móvil, Internet de las Cosas (IoT), criptografía, ingeniería inversa, análisis forense, entre otros.

Al tratarse de la primera vez que se realiza este evento, la organización del evento ha seleccionado un total de 5 países para este proyecto piloto.

- Colombia
- Costa Rica
- España
- Perú
- República Dominicana

El número de países participantes irá aumentando progresivamente en sucesivas ediciones.

2. ÓRGANOS DE LA COMPETICIÓN

2.1. Comité organizador

El Comité organizador está compuesto por:

- Dos representantes de INCIBE
- Dos representantes de la SG/OEA
- Dos representantes del BID

El comité organizador será el encargado de resolver cualquier incidencia que ocurra durante el evento, será también el mediador entre los equipos si fuera necesario y el encargado de tomar las decisiones necesarias durante el desarrollo del evento.

El Comité podrá descalificar a los participantes si:

- Detecta irregularidades en sus datos identificativos
- Actúan en contra del espíritu de la competición
- Incumple las presentes bases o realizan algún tipo de trampa o engaño.
- Intenten interrumpir con su actitud o comportamiento el correcto desarrollo de la competición
- Intenten dañar o atacar de forma deliberada alguno de los sistemas o infraestructura relacionados con el evento, reservándose la organización el derecho a reclamar los correspondientes daños y perjuicios, tanto por vía civil como penal

2.2. Jurado

El jurado está compuesto por el Comité organizador y los seleccionadores de cada equipo (uno por país).

Las funciones del jurado serán las siguientes:

- Revisar y aprobar los resultados obtenidos en la prueba técnica del CTF
- En caso de que fuese necesario y se produjera algún problema con las puntuaciones, el jurado será quien deba realizar un recuento manual de puntos al término de la competición
- Evaluar la exposición de retos de cada uno de los países

3. OBJETIVOS

Los objetivos buscados con la realización de esta competición son:

- Ayudar a eliminar la barrera de la ciberseguridad en Iberoamérica ayudando a identificar el talento en esta materia.
- Promocionar el talento, ofreciendo formación y mostrando las interesantes posibilidades profesionales que tiene la ciberseguridad.
- Promover el conocimiento y el fortalecimiento de las relaciones de todos los países participantes, fomentando la colaboración a distintos niveles.

Por ello, se dotará a los países participantes de capacidades para identificar el talento en ciberseguridad, de cara a construir nuevas posibilidades formativas y profesionales, así como generar industria y servicios profesionales en torno a la ciberseguridad.

Todo esto supondrá un impulso para todos los países participantes y facilitará una mejora global en términos de ciberresiliencia.

4. FASES DEL EVENTO ICSC

4.1. FASE I: Preselección de candidatos

Cada país identifica a diferentes participantes para que formen parte de una primera prueba de tipo CTF online. Como resultado de esta prueba, se obtuvo un ranking basado en los conocimientos de cada participante en cada una de las áreas en las que se distribuyeron los distintos retos del ejercicio.

A partir de dicho ranking, se realizó un proceso de selección de candidatos en base a las distintas puntuaciones obtenidas en cada área. El número de preseleccionados por cada país era de 12 aspirantes, los cuales pasaban a la siguiente Fase II.

4.2. FASE II: Formación / Capacitación

Como parte del evento ICSC, se proporciona una formación presencial avanzada a los 12 aspirantes de cada uno de los países.

Está formación se subdivide en dos partes:

- Formación técnica: Compuesta por un curso de 32 horas en el que se ofrece capacitación avanzada sobre distintas áreas de la ciberseguridad y sobre las características que tendrá la competición presencial en la que consistirá la siguiente fase de la competición. Durante esta formación, los aspirantes tienen la oportunidad de mejorar sus habilidades técnicas en ciberseguridad y ampliar sus conocimientos, aprendiendo distintas técnicas y aprendiendo a utilizar herramientas de pentesting, análisis forense, etc.

- Formación en "*Soft Skills*": Compuesta por una formación basada en fomentar el trabajo en equipo, hablar en público, gestión de conflictos, exposición de los resultados obtenidos, etc. Durante esta formación, los aspirantes adquieren habilidades que también les serán de gran utilidad de cara a su desarrollo profesional en la ciberseguridad.

Una vez finalizada esta doble formación, de los 12 aspirantes de cada país, se seleccionan finalmente a 10 para formar el equipo titular que representará, como selección nacional, a cada uno de los países participantes. Los otros 2 aspirantes formarán parte del equipo como reservas, en caso de que algún titular no pudiera asistir a la siguiente fase.

4.3. FASE III: Competición presencial

La fase final del Ibero-American CyberSecurity Challenge (ICSC) tendrá lugar en Cartagena de Indias (Colombia), el día 13 de diciembre de 2018. Concretamente esta fase final tendrá lugar en el centro de formación de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) situado en Centro, Plaza de Santo Domingo, carrera 36 No. 2-74, Cartagena de Indias - Colombia

Esta tercera fase es el objeto de la regulación de las presentes bases.

INCIBE se harán cargo de los gastos derivados de los viajes y alojamientos del equipo español. La SG/OEA se hará cargo de los gastos de viaje y alojamiento del resto de equipos participantes.

Esta competición presencial se compone de 2 actividades que se tendrán en cuenta para la puntuación final obtenida por cada equipo.

Cada equipo que participe en la competición contará con un capitán y un seleccionador.

- **Capitán**: Es designado por el propio equipo. Esta persona tendrá el rol de único interlocutor (junto con el seleccionador) para discutir los asuntos del equipo con la organización durante la competición. Será la única persona habilitada para hablar con el seleccionador durante la competición. Las preguntas de otros compañeros deberán ser trasladadas a través del capitán o el seleccionador de cada equipo.
- **Seleccionador**: Es el responsable del bienestar y correcto comportamiento de los concursantes y debe asegurarse de que la información sobre la competición llegue a su equipo, que la comprendan y actúen en consecuencia.

Durante la competición, el seleccionador estará separado del equipo. La comunicación entre el entrenador y el equipo será a través del capitán mediante canal abierto, es decir, dentro del alcance del oído de otros seleccionadores y limitado a un nivel general no técnico. Por ejemplo: Hablar sobre sugerencia de prioridades o informar del estado del desafío, pero no detalles técnicos ni ayudas de cualquier tipo sobre la resolución de retos.

4.3.1. Competición técnica: CTF presencial

Este CTF consiste en que los participantes pongan a prueba sus conocimientos y habilidades en diferentes áreas y categorías, con diferentes grados de dificultad de tal forma que vayan obteniendo puntos a medida que resuelven los retos que se les plantean.

La duración de esta actividad técnica es de 7 horas, las cuales se desarrollarán de manera ininterrumpida.

Las **principales categorías** a las que se enfrentarán los distintos equipos durante el CTF serán:

- **Criptografía y esteganografía**: Retos relacionados con la criptografía, y con la ocultación de información. Los participantes se podrán encontrar textos cifrados mediante un criptosistema determinado.
- **Análisis forense**: Retos en los cuales hay que recuperar información o datos ocultos. Los participantes se podrán encontrar imágenes de memoria, de discos duros o capturas de red, las cuales ocultan diferentes tipos de información.
- **Reversing y exploting**: Retos relacionados con la explotación de binarios y la ingeniería inversa, descubrimiento de vulnerabilidades en un servidor, inferir en el funcionamiento del software, etc.
- **Web**: Retos relacionados con descubrir vulnerabilidades en servicios, páginas web, etc. y explotarlas de una determinada forma.
- **Otros/Miscelánea**: Retos pertenecientes a otros campos de la ciberseguridad y que requieran diferentes habilidades para poder ser resueltos.

El CTF presencial estará compuesto por un total de 15 retos, distribuidos en tres tipos diferentes de dificultad:

- Retos de dificultad baja: 40% del total de retos.
- Retos de dificultad media: 40% del total de retos.
- Retos de dificultad alta: 20% del total de retos.

Para esta parte de la competición, los participantes deberán llevar su propio ordenador. No hay reglas sobre qué sistema operativo usar, pero las recomendaciones sobre los requisitos mínimos son:

- Sistema operativo Windows 7, como principal.
- Distribución Kali Linux.
- 4GB de memoria RAM.

Los participantes deberán tener en cuenta las siguientes normas de uso de la Plataforma durante el desarrollo de la competición:

- **DoS/ DDoS**: Los participantes no deben iniciar ataques de denegación de servicio. Todos dependemos de una única red y tirar servicios no es lo que se persigue.
- **Cortes de red**: Los participantes no deben contaminar / envenenar / atascar la conexión utilizada para el desarrollo de la competición.
- **Dispositivos de red**: Los participantes solo pueden conectar sus dispositivos a los puertos habilitados por la organización; serán comunicados al comienzo de la competencia.
- **Ataques de Capa 2**: Los participantes no deberán usar ataques de Capa 2 en la red cableada o inalámbrica.
- **Credenciales**: Cada participante solo puede usar sus propias credenciales de acceso proporcionadas. Las credenciales no se pueden intercambiar ni reutilizar.
- **Sistema de puntuación**: Los participantes no deben interferir con el sistema de puntuación.
- **Sistema de monitorización**: Los participantes no deben interferir con el sistema de monitorización.
- **Infraestructura de la plataforma**: Los participantes no deben interferir con la infraestructura de la plataforma.
- **Bloqueos**: Si un participante queda bloqueado por algún motivo y no puede continuar compitiendo normalmente, el capitán del equipo deberá solicitar ayuda al personal de desafío designado.
- **Comentarios públicos**: Durante el desarrollo de la competición, no está permitido publicar comentarios sobre la propia competición, ni en redes sociales ni de ninguna otra forma.

4.3.2. Exposición de un reto por parte de cada equipo

De forma simultánea y en paralelo al CTF presencial, durante el último tramo de competición, se llevarán a cabo las exposiciones/presentaciones de retos por parte del capitán del equipo.

En esta fase de la competición, los equipos participantes deberán seleccionar y exponer un reto del CTF presencial que hayan resuelto con éxito previamente durante la competición.

Las presentaciones de los retos tendrán lugar, a puerta cerrada, en una sala anexa a la sala principal de competición. Los retos serán expuestos ante el jurado designado por la organización.

Aspectos importantes a tener en cuenta:

- Cada equipo deberá elegir un reto que haya sido resuelto previamente durante la competición.
- Dos horas antes del cierre de la competición el capitán deberá informar a la organización (a través del capitán o seleccionador), de cuál será el reto a exponer.
- La exposición al jurado será llevada a cabo por un único componente de cada equipo.
- El tiempo de cada exposición será de 10 minutos como máximo. Si se sobrepasase ese tiempo, el jurado interrumpirá la exposición y se dará por finalizado el contenido a valorar para la puntuación.
- El ordenador sobre el que se realizará la presentación será el de la sala del jurado, por lo que se deberá llevar la presentación en un pendrive/pincho USB.

Las exposiciones deberán presentarse en formato (PowerPoint, PDF, o similar) y deberán de seguir un patrón de 5 slides (también llamadas diapositivas / filminas / transparencias), con el fin de poder evaluar en igualdad de condiciones a todos los equipos.

La estructura de la presentación deberá ser la siguiente:

- **Slide 1**: Breve introducción del equipo y de la persona que expone el reto.
- **Slide 2**: Reto seleccionado y justificación de la elección del mismo.
- **Slide 3**: Explicación sobre los pasos que ha seguido el equipo para resolver el reto.
- **Slide 4**: Dificultades a las que se ha enfrentado el equipo para resolver el reto.
- **Slide 5**: Conclusiones sobre el trabajo realizado. Por ejemplo; recomendaciones sobre cómo prevenir ese tipo de incidentes (si procede), lecciones aprendidas, etc.

El jurado se reserva el derecho de realizar preguntas, máximo durante 5 minutos, a la finalización de la exposición.

Una vez finalizada la exposición el jurado se reunirá para deliberar y otorgar la puntuación por la presentación realizada. Posteriormente, se dará paso al siguiente equipo para que comience su exposición.

4.3.3. Valoración

4.3.3.1. Puntuación/Scoring de la competición

4.3.3.2. Competición técnica: CTF presencial

- Retos de dificultad baja: 200 puntos.
- Retos de dificultad media: 250 puntos.
- Retos de dificultad alta: 300 puntos.

Para la resolución de los retos estarán disponibles varias pistas/ayudas en cada uno de ellos. El uso de estas pistas facilitará la resolución del reto, pero descontará puntos de la recompensa final.

- Primera pista: Reducción de un 20% de los puntos del reto
- Segunda pista: Reducción de un 40% de los puntos del reto

- Tercera pista: Reducción de un 60% de los puntos del reto

Las reducciones de puntos por pistas consultadas no serán acumulables. Por tanto, de todas las pistas consultadas para un mismo reto, tan sólo se aplicará la reducción de la pista más alta que haya sido desvelada.

4.3.3.3. Exposición de retos

Las exposiciones serán evaluadas por el jurado, pudiendo obtenerse los siguientes resultados, en base al desempeño mostrado:

- **Muy bien**: obtendrá el 20% del total de puntos de la parte técnica
- **Bien**: obtendrán el 15% del total de puntos de la parte técnica
- **Normal**: obtendrán el 10% del total de puntos de la parte técnica

Criterios de valoración de las presentaciones que tendrá en cuenta el jurado serán:

- Puntualidad (ajustar la presentación a los 10 minutos)
- Correcta introducción del equipo
- Correcta estructura de la exposición
- Cumplimiento del tiempo estipulado
- Claridad en la expresión oral y argumentación de ideas
- Presentación de información sintetizada y clara
- Foco en los aspectos más relevantes
- Balance de lenguaje técnico y no técnico
- Calidad de las conclusiones

4.3.3.4. Valoración final

La calificación final de cada equipo se obtendrá a partir de la suma de las puntuaciones obtenidas en la “Competición técnica: CTF presencial” y la puntuación obtenida en la “Exposición de retos”.

El jurado podrá decidir expulsar de la competición y no otorgar premios a equipos y/o participantes que incumplan las normas del evento.

5. NORMATIVA DEL EVENTO

5.1. Derechos y obligaciones de los organizadores

La organización se reserva el derecho de realizar cambios sobre la normativa aquí descrita si, por causas técnicas o de cualquier otra índole ajenas a su voluntad, no pudiera se pudiera realizar un normal desarrollo del evento.

La organización se reserva el derecho de interpretar y modificar las presentes Bases. En este último caso se comunicarán las modificaciones y condiciones del evento, por los mismos canales que las presentes, con la suficiente antelación y publicidad, sin que surja derecho a indemnización alguna a favor de los participantes o interesados. Si fuera necesario realizar un cambio en las Bases durante el propio evento, se informará verbalmente a todos los participantes, justificando el motivo de la modificación.

Asimismo se deja constancia de que ninguna de las disposiciones de las presentes bases constituye renuncia alguna a los privilegios e inmunidades de los que goza la SG/OEA, la OEA, sus órganos, su personal y sus bienes y haberes, de conformidad con la Carta de la OEA, los acuerdos y las leyes sobre la materia, y los principios y prácticas que inspiran el derecho internacional.

5.2. Derechos y obligaciones de los participantes

Toda persona que participe en el Ibero-American CyberSecurity Challenge (ICSC), deberá:

- Cumplir con lo dispuesto en las presentes Bases.
- Atender y respetar en todo momento las indicaciones de la Organización del evento.
- Respetar las instalaciones y material utilizado para el desarrollo del evento, manteniendo su buen estado de conservación y absteniéndose de llevar a cabo actuación alguna que pueda dañar, deteriorar o menoscabar el buen estado de aquellas.
- Actuar de buena fe, y comportarse con respeto y decoro hacia el resto de participantes. La violencia y ataques están estrictamente prohibidos.
- No se permite a los equipos participantes la comunicación con otras personas que no sean del propio equipo. Con la excepción de las comunicaciones entre el capitán y la organización, así como la de los seleccionadores y sus equipos.
- No se permite compartir soluciones a los retos, exploits o cualquier información entre equipos.
- No se permitirá la realización de fotos durante el evento ni el uso de los logos, marcas, imagen, nombre o similares, del evento o de los organizadores, en cualquier tipo de soporte, comunicación, redes sociales y medios sociales o de comunicación tradicional, sin contar con el previo consentimiento la organización.

La participación en el evento implica el conocimiento y la aceptación íntegra de las presentes Bases.

5.3. Cesión de derechos de imagen

Los participantes del evento, mediante la aceptación de estas Bases, ceden en exclusiva y de forma gratuita a la organización el uso de su imagen personal, que pudiera ser captada durante su participación en el evento, sin más limitación que la legislación aplicable en materia de honor y propia imagen.

En particular, los participantes autorizan de forma irrevocable y gratuita a la organización para hacer uso de su imagen y/o sus nombres en cualquier aviso o comunicación que se realice a través de cualquier medio escrito o audiovisual, en todo el mundo y durante todo el tiempo permitido legalmente. La participación y se comprometen a suscribir cualesquiera documentos o autorizaciones que pudieren ser necesarios para el uso de dicha imagen y/o nombre.

5.4. Protección de datos de carácter personal

Para la realización de la competición presencial la SG/OEA ha subcontratado con un tercero la plataforma online de retos. Dicha plataforma requiere que los participantes informen de un correo electrónico para el envío de datos de alta en la plataforma (usuario y contraseña de acceso).

En este caso la SG/OEA actúa como responsable del tratamiento de los datos y el subcontratista como encargado del tratamiento.

Los datos personales se tratarán de conformidad con lo establecido en las normas que resulten de aplicación en la materia a la SG/OEA.

Los datos no serán tratados para una finalidad distinta de la prevista en las presentes bases y serán eliminados tras la finalización del evento.

5.5. Aceptación de las Bases

La participación en el evento implica la total aceptación del contenido de estas Bases. La organización del evento se reserva el derecho a modificarlas, comunicándolo a los participantes a través del sitio web: https://www.incibe.es/icsc. Cualquier controversia en la aplicación de las presentes Bases será resuelta por el Comité organizador.

7 de diciembre de 2018

Director General

D. Alberto Hernández Moreno

INCIBE

Cybersecurity Program Manager

D. Belisario Contreras

OEA

E-Government Lead Specialist, Innovation for Citizen Services Division (ICS)

D. Miguel Angel Porrúa

BID

ICSC

Ibero-American
CyberSecurity
Challenge