International CyberEx 2023

#CyberEx23

cyberex_ INTERNATIONAL

OEA Más derechos para más gente

incibe_ SPANISH NATIONAL CYBERSECURITY INSTITUTE

ÍNDICE

INTERNATIONAL CYBEREX 2023

1 OBJETIVO

El objetivo de International CyberEx consiste en la ejecución de un ciberejercicio en el marco de los Estados Miembros de la Organización de los Estados Americanos (OEA) y de los países invitados por el Instituto Nacional de Ciberseguridad de España (INCIBE) que permita el **fortalecimiento de las capacidades de respuesta ante incidentes cibernéticos**, así como una **mejora de la colaboración y cooperación** ante este tipo de incidentes. El ejercicio se enfoca de una forma directa hacia un perfil técnico de seguridad con altos conocimientos en el campo de las Tecnologías de la Información y las comunicaciones.

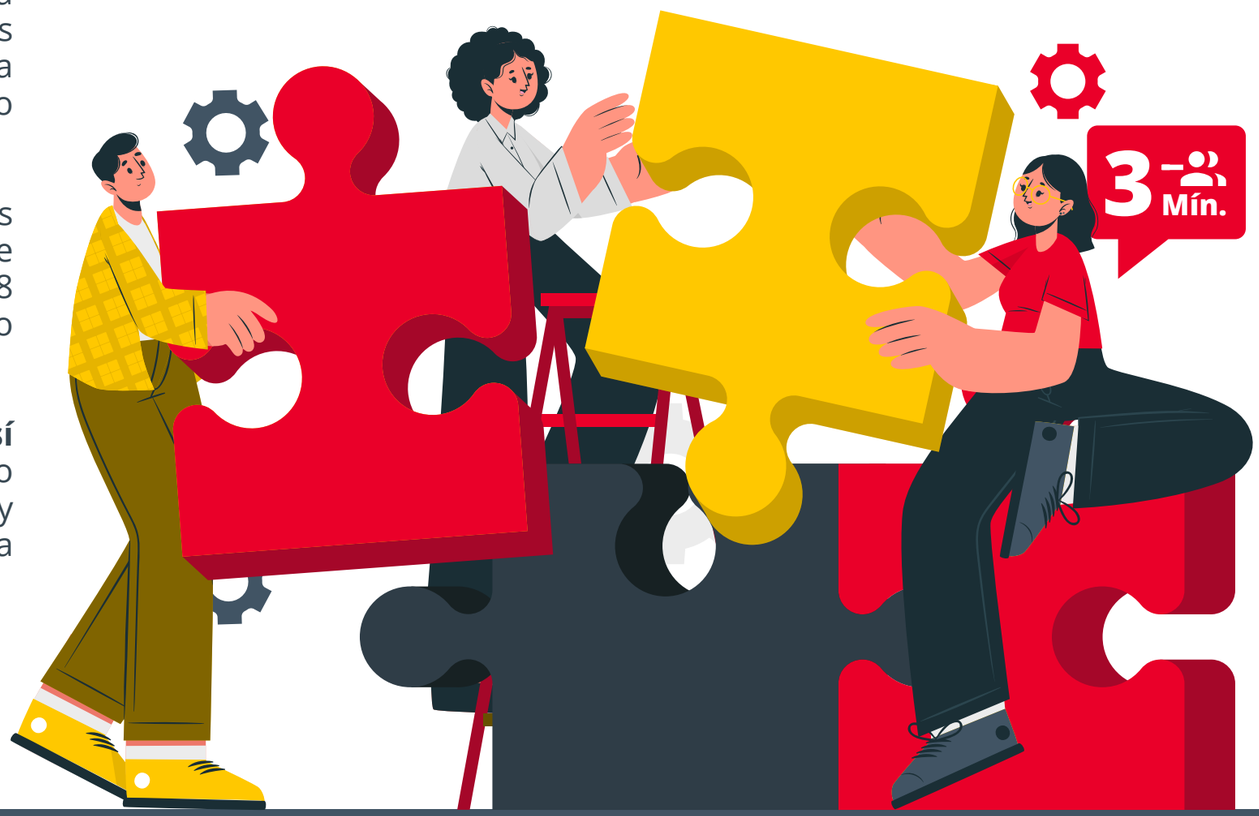
El ciberejercicio se realizará en formato CTF (del inglés, Capture The Flag) por equipos. Este formato se basa en un modelo de competición de seguridad cibernética y está diseñado para servir como un ejercicio de entrenamiento que permita otorgar a los participantes experiencia en el seguimiento de una intrusión, así como trabajar las capacidades de reacción ante ciberataques análogos a los que suceden en el mundo real. Hay dos estilos principales para los CTF: ataque/defensa y jeopardy. Este último es el elegido por ser adecuado para **ampliar las capacidades técnicas**.

Las competiciones de estilo jeopardy suelen estar compuestas de varias categorías de problemas, cada uno de los cuales contiene una variedad de preguntas de diferentes valores. Los equipos compiten, en una sesión de 8 horas por ser el **primero en resolver el mayor número de desafíos,** pero no se atacan directamente el uno al otro.

Los países participantes en potencia son los **Estados Miembros de la OEA, así como los países de los CSIRT invitados por INCIBE.** Cada país podrá tener 1 o varios equipos representantes que incluyan profesionales de varios campos y refuerce la colaboración entre instituciones. La selección final de los equipos la realizará INCI BE y el Programa de Seguridad Cibernética de la OEA.

El idioma utilizado durante el ciberejercicio será el inglés.

EL CIBEREJERCICIO SE REALIZARÁ EN FORMATO CTF (DEL INGLÉS, CAPTURE THE FLAG POR EQUIPOS



2 REQUISITOS DE PARTICIPACIÓN

Cada país podrá tener uno o más equipos representante que deberán cumplir los siguientes requisitos.

◆ 2.1. EQUIPOS Los equipos podrán estar conformados por:

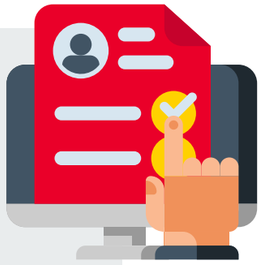
Cada equipo podrá contar con un máximo de 4 miembros y un mínimo de 3 miembros según la siguiente distribución:

- ◇ **1 capitán que ejercerá de coordinador del equipo** y será el punto único de contacto con los organizadores.
- ◇ **De 2 a 3 compañeros que apoyarán al capitán** para resolver los distintos retos. El perfil de los integrantes del equipo debería ser el de un técnico con experiencia y conocimientos en seguridad TIC al menos en uno o más de los siguientes campos:

- » Formación en seguridad TIC especialmente en la gestión de incidentes en la seguridad de la información.
- » Experiencia en gestión de incidentes de seguridad y fraude electrónico.
- » Experiencia en análisis de sistemas comprometidos, SPAM, sistemas y redes de seguridad.
- » Experiencia en análisis de malware, tanto estáticos como dinámicos y uso de herramientas de automatización de procesos como análisis de comportamiento, análisis en ejecución, etc.
- » Experiencia en análisis forense informático. Experiencia en el uso de herramientas que soporten el proceso de recopilación y análisis de la información
- » Experiencia en auditorías de seguridad: Metodologías, herramientas y experiencia técnica en auditorías de seguridad o pentesting.
- » Experiencia en administración y bastionado de sistemas operativos.
- » Experiencia en administración de redes y hardware de comunicaciones, bastidores y aplicaciones y servicios de soporte a equipos de seguridad.

2 REQUISITOS DE PARTICIPACIÓN

◆2.2. INSCRIPCIÓN



Para solicitar la participación en el ciberejercicio, el equipo de cada país deberá inscribirse en el formulario online:
https://www.surveymonkey.com/r/CYBEREX2023

◆2.3. REQUISITOS TÉCNICOS

El equipo participante tiene que contar al menos con los siguientes recursos:

Equipo cliente:

- ◇ PC de escritorio o portátil
- ◇ Navegadores soportados: Chrome (preferido) o Firefox (ambos en las últimas versiones).

Conexión a Internet con suficiente ancho de banda por usuario:

- ◇ Mínimo: 1Mbps de download y 100Kbps de upload.
- ◇ Recomendado: 3 Mbps de download y 1Mbps de upload

Aunque no es necesario, se recomienda a cada participante contar adicionalmente con una máquina (virtual o física) que disponga de una distribución Kali Linux o similar.

◆2.4. REGLAS DE COMPETICIÓN

A continuación se indican las normas que deben cumplir los participantes ya que violar este código de conducta descalificará a todo el equipo y serán reitrados de la competición:

1. Deben comportarse de manera profesional en todo momento.
2. No manipularán o intentarán modificar ningún elemento de la plataforma, incluyendo el sistema de puntuaciones y el panel de administración.
3. No están permitidos ataques de denegación de servicio.
4. No están permitidos ataques de fuerza bruta, a menos que algún objetivo especifique expresamente lo contrario.
5. No reiniciar, apagar o deshabilitar los servicios o funciones de los sistemas de destino.
6. No están permitidas acciones ofensivas para atacar o interferir los sistemas de otros participantes.
7. No intentarán engañar o colaborar con participantes de otros equipos.
8. Deben competir sin ayuda de personas ajenas a la competición.
9. No está permitido publicar información sobre la competición, cómo la forma de resolver los objetivos o las banderas de los mismos, sin consentimiento escrito por parte de INCIBE.
10. Solo se dará a conocer el ranking de los 10 mejores equipos. El resto de posiciones serán anónimas.

3 PLANIFICACIÓN

El ciberejercicio constará de varias fases con los siguientes hitos y fechas.

◆ 3.1. INSCRIPCIÓN

Para poder participar en el ciberejercicio, el capitán de cada equipo deberá inscribirlo a través del formulario online en la siguiente dirección web **https://www.surveymonkey.com/r/CYBEREX2023.**

El formulario online estará disponible **desde el 15 de mayo de 2023 hasta el 9 junio de 2023 a las 16:00 (UTC).**

◆ 3.2. SELECCIÓN DE PARTICIPANTES

Una vez cerrada la fase de inscripción, los organizadores del ciberejercicio contactarán vía email con los capitanes de los equipos seleccionados para notificarles que han sido elegidos para participar.

Dado que el número máximo de equipos en el ciberjercicio es limitado, la OEA e INCIBE realizarán una selección de participantes entre todos los equipos inscritos en base a los criterios que se definan entre ambas organizaciones, entre los cuales se podrán tener en cuenta la participación del mayor número de países posible, y la priorización de los equipos de CSIRT de referencia nacionales. El aviso por email se realizará a lo largo del **19 de junio de 2023.**

◆ 3.3. ENTREGA DE CREDENCIALES

Antes de la sesión de prueba, los organizadores contactarán vía email con cada uno de los participantes para hacer entrega de las credenciales de acceso a la plataforma. La entrega de las credenciales por email **se realizará el 22 de junio de 2023.**

◆ 3.4. SESIÓN DE PRUEBA, INFORMACIÓN SOBRE LA PRUEBA Y DUDAS.

Una vez notificados los capitanes de los equipos seleccionados, se realizará tanto una prueba de conectividad a la plataforma y de credenciales como una sesión informativa con todos los participantes en la que se llevará a cabo una introducción al uso de la plataforma. Concluida la explicación, se resolverán las dudas y preguntas que planteen los capitanes.

Esta sesión **tendrá lugar por videoconferencia y chat online el 28 de junio de 2023 a las 14:00 (UTC)** con una duración estimada de 1 hora.

◆ 3.5. EJECUCIÓN DEL CIBEREJERCICIO

Para la realización del ciberejercicio, todos los participantes deberán conectarse a la plataforma. Los capitanes deberán además usar videoconferencia y chat para ser informados, al principio, de la situación de partida y poder contactar con los organizadores durante la ejecución. La fecha de realización del ejercicio será el **11 de Julio de 2023 desde las 14:00 (UTC) y hasta las 22:00 (UTC)**, teniendo una duración estimada de 8 horas.

◆ 3.5. SESIÓN DE CIERRE

Una vez concluida la ejecución, se establecerá una sesión por videoconferencia con todos los participantes en la que se informará del resultado del ciberejercicio. La sesión de cierre tendrá lugar el **11 de Julio de 2023 a las 22:00 (UTC).**

4 RECURSOS

El ciberejercicio se desarrollará sobre la base de la realización de retos en formato CTF (Capture The Flag) jeopardy e incluirá los siguientes recursos.

◆ 4.1. WEB DEL CIBEREJERCICIO

El sitio web del ciberejercicio será **https://www.incibe.es/eventos/international-cyberex** será el punto de referencia de los equipos participantes y contará al menos con la siguiente información:

Pública:

- ◇ Resumen explicativo del ciberejercicio e instrucciones sencillas para la realización.
- ◇ Requisitos técnicos para la participación.
- ◇ Preguntas frecuentes (FAQ).
- ◇ Calendarios con las fechas claves del ciberejercicio.
- ◇ Formulario online de inscripción.

Privada:

- ◇ Manual de usuario de la plataforma.
- ◇ Acceso a la plataforma para resolver los desafíos.

◆ 4.2. PLATAFORMA DE EJECUCIÓN DEL CTF

INCIBE proveerá la plataforma de ejecución y la infraestructura necesaria para la ejecución de los desafíos, el sistema de juego y la puntuación (scoring).

El backend de la plataforma incluye un sistema de aprovisionamiento para formar la infraestructura virtual acorde al escenario. Asimismo, incluye un sistema de vigilancia que verifica que las redes virtuales, los sistemas y las "banderas" (sistemas objetivo, servicios o procesos, archivos, etc.) están disponibles y funcionan de manera correcta.

Asimismo, la plataforma incluye acceso y funciones de control de cuenta, logging, controles de seguridad, capacidad de gestión y rendimiento de la infraestructura, etc. De igual manera, permite arrancar varias copias del mismo escenario, escalando horizontalmente. La gestión y el balanceo de la carga permiten ajustar el rendimiento y el factor atenuante si el escenario se daña como resultado de las acciones de los jugadores (por ejemplo: uso indebido de un exploit que inhabilite un sistema). Este ambiente compartido está reservado en un punto dado para evitar la superposición y permite precisar la estabilidad y adaptabilidad para desarrollar los desafíos.

Una vez que el usuario se conecte al entorno:

- ◇ Recibe la información de los desafíos.
- ◇ Recibe la información de las banderas que se deben capturar.
- ◇ Envía las banderas capturadas para que se validen.
- ◇ Accede al sistema de pistas. Sólo el capitán del equipo podrá solicitar las pistas.
- ◇ Dispone de información general, una sección de ayuda.
- ◇ Conoce su progreso en el juego así como la posición relativa de otros participantes.

Una buena coordinación entre miembros de un equipo y su capitán es parte fundamental del ciberejercicio, y debe potenciarse. INCIBE se reserva el derecho a limitar el acceso a la plataforma solo a ciertos usuarios (por ejemplo, solo a capitanes), o a modificar el flujo del ejercicio durante la ejecución del mismo si las circunstancias lo requieren. Los participantes deben estar preparados para ese tipo de eventos.

◆ 4.3. EQUIPO TÉCNICO Y RESOLUCIÓN DE INCIDENCIAS

El equipo técnico de los organizadores se encargará de ofrecer la ayuda necesaria en la realización de todas las fases del ciberejercicio, desde la presentación de la iniciativa hasta la sesión de clausura.

Ejercerá tareas de apoyo, en particular y prestando especial atención, durante la ejecución del ejercicio para atender incidencias

En caso de problemas técnicos que impidan la normal consecución de la competición, la organización se reserva el derecho a aplicar las medidas necesarias que permitan continuar con la ejecución de la misma.

◆ 4.4. PREMIOS

Los equipos que se clasifiquen en los primeros puestos del ciberejercicio podrán optar a una serie de premios, de los que se informarán durante la ejecución del ciberejercicio y durante la sesión de cierre del mismo. Para consultar sobre dichas gratificaciones una vez finalizado el ejercicio, podrán contactar con la organización a través de la dirección: **cybersecurity@oas.org**

International

CyberEx 2023

#CyberEx23

cyberex_ INTERNATIONAL

OEA Más derechos para más gente

incibe_ SPANISH NATIONAL CYBERSECURITY INSTITUTE