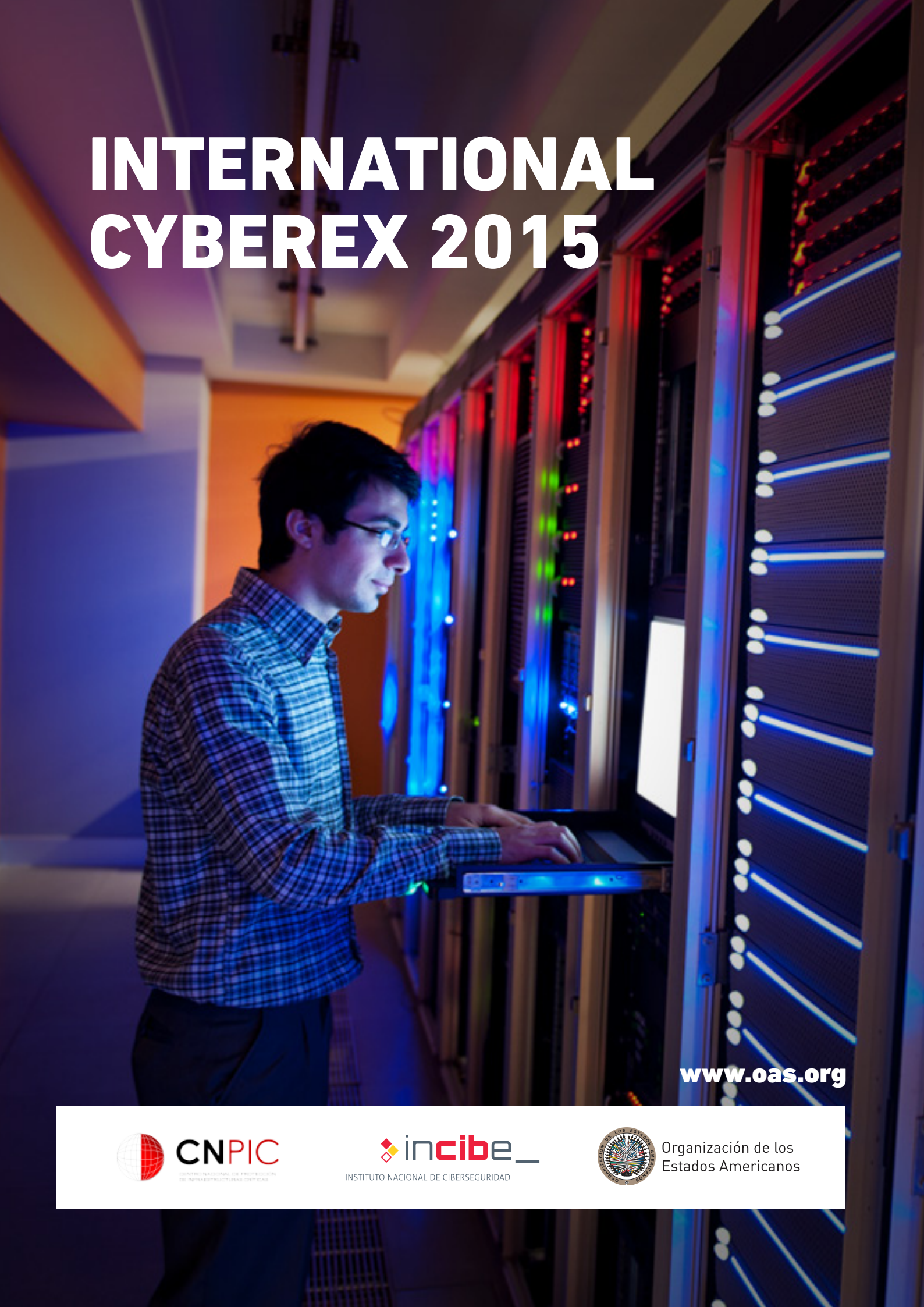
INTERNATIONAL CYBEREX 2015



www.oas.org

CNPIC

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Organización de los Estados Americanos

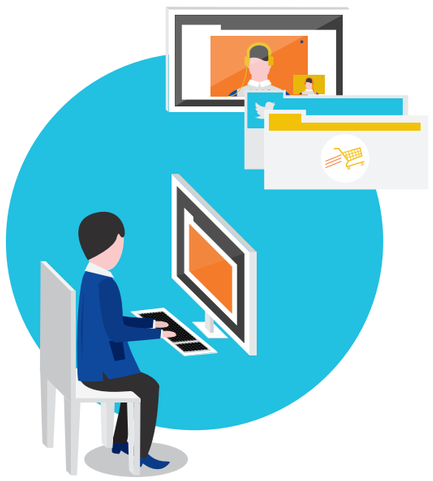
INTERNATIONAL CYBEREX 2015
PROPUESTA DE DESARROLLO

01/
OBJETO

El objeto 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) 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. Dicho ejercicio se enfoca de una forma directa hacia un perfil técnico de seguridad con altos conocimientos en el ámbito de las Tecnologías de la Información y las Comunicaciones (TIC).

El ciberejercicio se realizará en formato CTF (del inglés, **Capture The Flag**). 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 segundo es el elegido para este caso por ser el más adecuado a la hora de **ampliar capacidades** técnicas.

El ciberejercicio se realizará en formato Capture The Flag (CTF).



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

Los potenciales países participantes son los **34 Estados Miembros de la OEA, así como países Observadores de la OEA que podrían llegar a ser invitados**. La participación por países (con un número máximo total de equipos de 45) permitirá la configuración interna de cada país de un equipo que incluya profesionales de distintos ámbitos y refuerce la colaboración entre instituciones. La selección final de los Equipos será realizada por el INCIBE y el Programa de Seguridad Cibernética de la OEA.

El idioma por defecto para la realización del ciberejercicio será el **inglés.**

02/
PERFIL DEL EQUIPO

Cada equipo estará integrado con un máximo de 8 integrantes. En algunos casos habrá países con participación de más de dos equipos.

Los equipos podrán estar integrados por Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés), o por expertos del sector público, privado o la sociedad civil.

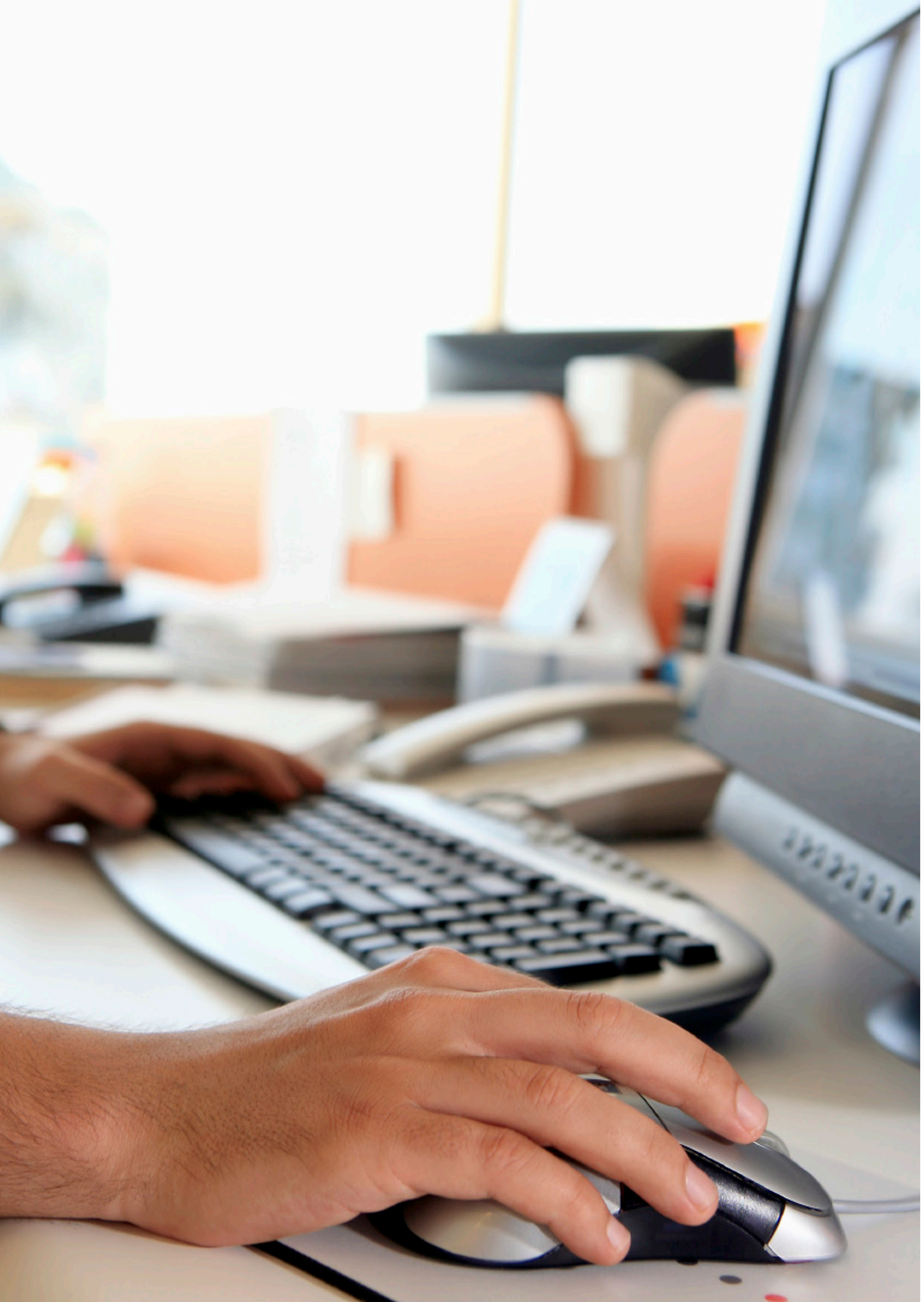
El perfil de los integrantes del equipo se dirige hacia un técnico con **conocimientos y experiencia en seguridad TIC** al menos en uno o varios de los siguientes campos:

Cada equipo deberá identificar un capitán, quien será el punto de enlace con el equipo de coordinación.

- Formación en seguridad TIC y especialmente en gestión de incidentes de seguridad informática.
- Experiencia en gestión de incidentes de seguridad y fraude electrónico.
- Experiencia en análisis de sistemas comprometidos, SPAM, seguridad en redes y sistemas.
- Experiencia en análisis de malware, tanto análisis estático como dinámico y el uso de herramientas que automaticen tales procesos, como análisis de comportamientos, análisis en ejecución, etc.
- Experiencia en análisis forense informático. Experiencia en el uso de herramientas que soporten los procesos de recopilación de información y análisis de la misma.
- Experiencia en auditorías de seguridad: metodologías, herramientas y conocimientos técnicos sobre auditorias técnicas de seguridad o pentesting.
- Experiencia en administración y bastionado de sistemas operativos.
- Experiencia en administración de redes y hardware de comunicaciones, bastidores y aplicativos y servicios de soporte a equipos de seguridad.

Cada equipo deberá identificar un capitán, quien será el punto de enlace con el equipo de coordinación.

Para poder ser parte de este ejercicio, cada equipo deberá completar un formulario de registro en el que se indique la información del equipo y la información de contacto del capitán. El formulario deberá ser enviado a la dirección de correo electrónico International@cyberex.es.



03/ PLANIFICACIÓN

El ciberejercicio tendrá varias fases que serán completadas con la siguiente planificación.

1. Sesión de presentación

El ciberejercicio comenzará con una reunión de presentación con todos los participantes en el que se trasladará la iniciativa y permitirá establecer el marco de colaboración tanto técnico como organizativo entre las entidades. Dicha sesión tendrá lugar por videoconferencia el día **16 de julio de 2015 a las 10:00 (GMT-4), y subsecuentemente el 28 de julio de 2015 a las 10:00 (GMT-4/EDT).**

2. Implementación de retos

Tras la sesión de presentación se llevará a cabo la implementación técnica de los retos por parte de la OEA-INCIBE. Esta fase servirá también para recabar los acuerdos legales entre entidades en caso de que sean necesarios y los datos de los participantes. Al final de la fase la plataforma del ciberejercicio se encontrará lista para su ejecución. Esta fase tendrá lugar durante los meses de julio y agosto de 2015.

3. Sesión de resolución de dudas

Esta sesión tendrá lugar **el jueves 17 de septiembre de 2015 a las 10.00 (GMT-4/EDT),** y servirá para que, de forma remota a través de audio o videoconferencia, los participantes puedan plantear sus dudas y la organización dé respuesta a todas ellas como paso previo a la ejecución del ejercicio.

4. Ejecución del ejercicio

La fecha del ejercicio será el 24 de septiembre de 2015. El ejercicio tendrá una duración de **8 HORAS** y se desarrollará en una única jornada. Teniendo en cuenta la dispersión de zonas horarias que abarca a los países de la OEA (tal y como se muestra en el Anexo I), se plantea que la zona horaria de referencia debe ser **GMT-4/EDT**. Esta zona horaria permite, con una diferencia de una hora, incluir 29 países.

El ciberejercicio comenzará a las 10.00 (GMT-4/EDT) y finalizará a las 18.00 (GMT-4/EDT) e incluirá un tiempo al inicio para la explicación del escenario, así como un tiempo al final para su análisis. Cada equipo de cada país participará en remoto desde su ubicación.

5. Sesión de cierre

Durante la sesión de cierre se analizará el escenario ejecutado, así como los procesos que llevan a la consecución de banderas. Asimismo se otorgará la palabra a los participantes para que puedan dar su opinión colaborando a la mejora de futuras ediciones del ciberejercicio. La sesión de cierre tendrá carácter presencial y se llevará a cabo durante la ejecución de ENISE el **20 de octubre de 2015**. De igual forma habrá un proceso de retroalimentación informal en el Coloquio Técnico de la OEA y FIRST a realizarse el 29 de septiembre de 2015.

04/
ACTIVOS DEL CIBEREJERCICIO

El ciberejercicio se desarrollará sobre la base de la realización de retos en formato CTF jeopardy y contará con los siguientes activos.

1.1 Sitio web del ciberejercicio

El sitio web del ciberejercicio será el punto de referencia para los países participantes y contendrá al menos la siguiente información:

- Resumen explicativo sobre el ciberejercicio e instrucciones básicas para la realización.
- Detalles técnicos para la participación.
- Manual de usuario de la plataforma.
- Fechas relativas a la realización del ciberejercicio.
- Acceso a la plataforma para la resolución de los retos.
- Chat de soporte.

1.2 Plataforma de ejecución del CTF

La plataforma de ejecución se encuentra en la nube y albergará la infraestructura necesaria para la implementación de los retos, el sistema de juego y de scoring.

El backend de la plataforma incluye un sistema de aprovisionamiento para conformar la infraestructura virtual de acuerdo al escenario. Además incluye un sistema de monitorización que comprueba que las redes virtuales, los sistemas y las "banderas" (sistemas objetivo, servicios o procesos, ficheros, etc.) están disponibles y con el rendimiento adecuado.

La plataforma incluye también funciones de control de cuentas y accesos, logging, controles de seguridad, gestión de capacidad y rendimiento de la infraestructura etc. Asimismo permite arrancar múltiples copias de un mismo escenario, escalando horizontalmente. La gestión y balanceo de la carga permiten ajustar el rendimiento así como factor de mitigación si el escenario resulta dañado como resultado de las acciones de los jugadores (por ejemplo el uso incorrecto de un exploit que deshabilite un sistema). Este entono compartido está reservado en un momento dado para evitar la concurrencia y permite la estabilidad y escalabilidad precisada para desarrollar retos.

La plataforma comprende todos los servicios precisos para completar el juego:

- Servidores de diferentes tipos
- DNS
- LDAPs
- Terminadores VPN
- Proxys
- Servidores web
- etc.

De cara al jugador, éste emplea su propio portátil con las herramientas que considere necesarias e interactúa con el entorno a través de una Red Privada Virtual (VPN), que se establece para el evento en concreto, y el navegador web. Una vez conectado al entorno, el usuario:

- Recibe la información de los retos.
- Recibe la información de las banderas que se deben capturar.
- Envía las banderas capturadas para su validación.
- Accede al sistema de pistas.
- Tiene información general, un apartado de ayuda y la posibilidad de la configuración de su perfil.
- Conoce sus progresos en el juego así como su posición relativa respecto al resto de participantes.

La fecha del ejercicio será el 24 de septiembre de 2015. El ejercicio tendrá una duración de 8 horas.

1.3 Equipo técnico

El equipo técnico del ciberejercicio se encargará de ofrecer el soporte necesario durante la realización de todas las fases del ciberejercicio, desde la presentación de la iniciativa a la sesión de cierre.

En particular y con mayor énfasis llevará a cabo las tareas de soporte durante la ejecución del ejercicio para atender a incidencias.

1.4 Requisitos de participación

El equipo participante deberá disponer de al menos los siguientes elementos:

- Conexión a Internet sin filtrar con ancho de banda mínimo: 256kbp/s

- PCs con herramientas de hacking tipo:
  - · Kali Linux
  - · Backtrack

- Un capitán de equipo encargado de la coordinación del equipo y de la interlocución con el equipo técnico de la organización del ciberejercicio.

INCIBE pertenece al Ministerio de Industria, Energía y Turismo de España.
CNPIC pertenece al Ministerio del Interior de España.

Organización de los Estados Americanos
17th St. and Constitution Ave., NW
Washington, D.C., 20006-4499
Estados Unidos de América

www.oas.org