**Oficina de Desarrollo**
**de las Telecomunicaciones (BDT)**

Ref.: Circular/BDT/DNS/CYB/051

Ginebra, 24 de julio de 2020

- Estados Miembros de la UIT
- Miembros de Sector del UIT-D
- Instituciones Académicas
- Organizaciones regionales e internacionales
- Sectores nacionales esenciales/ EIEI nacionales
- Coordinadores de ciberseguridad de la UIT

**Asunto: Invitación a participar en el Cibersimulacro Mundial de la UIT de 2020**

Muy Señora mía/muy Señor mío:

Tengo el placer de invitarle a participar en el Cibersimulacro Mundial de la Unión Internacional de Telecomunicaciones (UIT), que se celebrará de septiembre a noviembre de 2020. El Cibersimulacro de la UIT se llevará a cabo de forma virtual, a causa de la actual pandemia de COVID-19 y de los riesgos y restricciones asociados a los viajes y reuniones.

La pandemia de COVID-19 ha intensificado la dependencia de las tecnologías de la información y la comunicación (TIC) a escala mundial. Gracias a las TIC, las personas han podido ser productivas y relacionarse, incluso en contextos de distanciamiento social. Esa mayor dependencia de las TIC también ha planteado serios obstáculos a la ciberseguridad, debido a un aumento de las ciberamenazas.

Los Cibersimulacros Regionales que la UIT había previsto realizar en 2020 serán sustituidos por un único Cibersimulacro Mundial virtual. En el marco del Cibersimulacro Mundial, organizaremos una serie de diálogos regionales, seminarios web internacionales, sesiones de formación y ejercicios basados en casos hipotéticos a lo largo de tres (3) meses, a fin de ayudar a los países a desarrollar las capacidades necesarias para gestionar mejor las ciberamenazas. El folleto del evento, adjunto a la presente carta (véase el Anexo 1), contiene más información al respecto.

El Cibersimulacro Mundial es un evento de creación de capacidad, cuyo objetivo es mejorar las capacidades de comunicación y respuesta a incidentes de los equipos participantes y promover los esfuerzos colectivos de los equipos de intervención en caso de incidente informático (EIII) y los equipos de intervención en caso de incidente de seguridad informática (EIISI) nacionales.

En este Cibersimulacro pueden participar equipos de EIII/EIISI nacionales, ministerios, organismos reguladores, operadores de telecomunicaciones, universidades e instituciones educativas, fabricantes de equipos de telecomunicaciones, institutos de investigación y diseño, desarrolladores de software y otros interesados de los Estados Miembros, los Miembros de Sector y las Instituciones Académicas de la UIT. Se recomienda que cada equipo participante esté formado por un mínimo de dos (2) miembros del personal técnico y un (1) miembro del personal directivo.

Para obtener más información e inscribirse en los eventos del Cibersimulacro Mundial, le rogamos visite el siguiente sitio web: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx.

Los responsables de las prioridades temáticas regionales en materia de ciberseguridad de la UIT están a su disposición para cualquier consulta relativa a los eventos del Cibersimulacro Mundial de la UIT de 2020.

- Oficina Regional para África, Sr. Serge Valery Zongo (serge.zongo@itu.int)
- Oficina Regional para las Américas, Sr. Pablo Palacios (Pablo.Palacios@itu.int)
- Oficina Regional para los Estados Árabes, Sra. Rouda Al Amir Ali (Rouda.AlamirAli@itu.int)
- Oficina Regional para Asia y el Pacífico, Sr. Sameer Sharma, (sameer.sharma@itu.int)
- Oficina Regional para la CEI, Sr. Farid Nakhli (farid.nakhli@itu.int)
- Oficina Regional para Europa, Sr. Jaroslaw Ponder (jaroslaw.ponder@itu.int)

Atentamente.

[Original firmado]

Doreen Bogdan-Martin
Directora

ANEXO 1

# Cibersimulacro Mundial de la UIT de 2020

## 1 INTRODUCCIÓN

La Unión Internacional de Telecomunicaciones (UIT) mejora la preparación de los Estados en términos de ciberseguridad, su nivel de protección y su capacidad de respuesta en caso de incidente mediante la realización de cibersimulacros en los planos regional e internacional. Un cibersimulacro es un evento anual durante el cual se simulan ciberataques, incidentes relacionados con la seguridad de la información y problemas de diversa índole, a fin de poner a prueba las cibercapacidades de una organización, desde su capacidad para detectar un incidente de seguridad hasta su capacidad para responder de manera adecuada y minimizar cualquier repercusión conexa. Los participantes en un cibersimulacro pueden validar políticas, planes, procedimientos, capacidades y procesos en favor de la preparación, la prevención, la respuesta, la recuperación y la continuidad de las actividades. Hasta la fecha, la UIT ha organizado más de 29 cibersimulacros en todo el mundo, con miras al refuerzo de las habilidades y capacidades relacionadas con la ciberseguridad mediante la colaboración y la cooperación regionales.

## 2 OBJETIVOS

Los objetivos principales de este cibersimulacro son:

- dotar a los participantes clave de los sectores público y privado, que dirigen empresas, organizaciones o jurisdicciones, de conciencia situacional en caso de ciberperturbación;
- congregar a la comunidad de EIEI/EIII/EIISI en un ejercicio unificado, a fin de crear capacidades de respuesta y recuperación a escala mundial;
- poner a prueba los conceptos fundamentales de la resiliencia operacional en el conjunto de la comunidad de EIEI/EIII/ EIISI;
- determinar y ejecutar procesos, procedimientos, interacciones y mecanismos de intercambio de información, que existen o deberían existir entre EIEI/EIISI, SOC, agencias y organismos públicos, así como en organizaciones regionales responsables de la gestión de crisis y organismos reguladores, y fomentar su mejora;
- poner en práctica mecanismos de coordinación, iniciativas de intercambio de información, ejercicios de desarrollo de una conciencia situacional compartida y procedimientos de toma de decisiones de la comunidad de ciberseguridad en el marco de eventos cibernéticos; y
- crear conciencia sobre otras iniciativas relacionadas con ciberejercicios.

## 3 ACTIVIDADES PREVISTAS

Debido a las restricciones aplicables a los viajes, así como a otras medidas importantes adoptadas en respuesta a la pandemia de COVID-19, los eventos del cibersimulacro se llevarán a cabo en línea a lo largo de tres (3) meses, concretamente, de septiembre a noviembre de 2020. En colaboración con los asociados sobre el terreno, los expertos de la UIT se han propuesto llevar a cabo y/u organizar:

- **Seis (6) diálogos regionales sobre las enseñanzas extraídas de la pandemia de COVID-19:**
  a) La pandemia de COVID-19 ha incrementado la presión a la que estaban sometidos los sistemas nacionales de TIC, haciéndolos en ocasiones más vulnerables a ciberataques contra infraestructuras críticas. Los diálogos regionales brindarán a representantes de EIISI/EIII/EIEI de todos los Estados Miembros la oportunidad de compartir sus experiencias en la gestión de los aspectos relacionados con la ciberseguridad durante la pandemia de COVID-19.

- **Tres (3) seminarios web:**
  a) **Empoderamiento de la mujer en materia de ciberseguridad:** Los ponentes de este seminario web debatirán el papel de la mujer en el ámbito de la ciberseguridad en todos los sectores. Esta serie de eventos estará abierta a todos los participantes.
  b) **Gestión de cibercrisis:** Las estrategias encaminadas a la gestión de las cibercrisis constituyen la piedra angular de la ciberresiliencia nacional. En esta mesa redonda participarán expertos en el campo de la gestión de cibercrisis. Esta serie de eventos estará abierta a todos los participantes.
  c) **Medición y mejora del nivel de madurez de los EIII:** Esta mesa redonda se centrará en la medición y la mejora del nivel de madurez como aspectos esenciales para el progreso y el fortalecimiento constantes de las capacidades de los EIISI. Este seminario web contará con la participación de expertos dotados de una amplia experiencia de trabajo con EIII. Esta serie de eventos estará abierta a todos los participantes.
- **Seis (6) sesiones de formación:**
  a) Los expertos de la UIT, en colaboración con otras organizaciones asociadas, dirigirán las distintas sesiones de formación, que tendrán lugar en días diferentes a una hora preestablecida. Las sesiones de formación comprenderán debates sobre creación de capacidades eficaces en materia de inteligencia de ciberamenazas (CTI*, cyber threat intelligence*), respuesta a incidentes, comunicación en el marco de la gestión de crisis, ciberseguridad y respuesta a incidentes en el ámbito industrial, detección de noticias falsas e inteligencia práctica de ciberamenazas. Estas sesiones de capacitación estarán abiertas a todos los participantes.
- **Seis (6) ejercicios basados en casos hipotéticos:**
  a) La realización de ejercicios basados en casos hipotéticos es uno de los puntos más destacados de los cibersimulacros de la UIT. Este año, la UIT ha previsto realizar seis ejercicios basados en casos hipotéticos en días diferentes a una hora determinada. Estos ejercicios solo estarán abiertos a los EIII/EIISI nacionales/gubernamentales, y cada país participante estará representado por un equipo compuesto de un mínimo de dos (2) y un máximo de cuatro (4) participantes.

Los seminarios web regionales sobre "EIII y enseñanzas extraídas del COVID-19" solo estarán abiertos a los Estados Miembros de la región en cuestión. Los demás seminarios virtuales, sesiones de formación y ejercicios basados en casos hipotéticos estarán abiertos a todos los participantes, con independencia de la región.

## 4 DESTINATARIOS

En los diálogos regionales, los seminarios web y las actividades de formación pueden participar EIII/EIISI nacionales, ministerios, organismos reguladores, operadores de telecomunicaciones, instituciones académicas y educativas, fabricantes de equipo de telecomunicaciones, institutos de investigación y diseño, desarrolladores de software y otros interesados de los Estados Miembros y los Miembros de Sector de la UIT.

En los ejercicios solo podrán participar EIII/EIISI nacionales/gubernamentales y cada país inscrito estará representado por un equipo de dos (2) participantes.

## 5 LOGÍSTICA

Recomendamos que todos los participantes dispongan de una computadora o un ordenador portátil con una conexión estable y adecuada a Internet cuando participen en eventos del cibersimulacro.

## 6 INSCRIPCIÓN

Para obtener más información e inscribirse en los eventos, le rogamos visite el sitio web del cibersimulacro: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx.

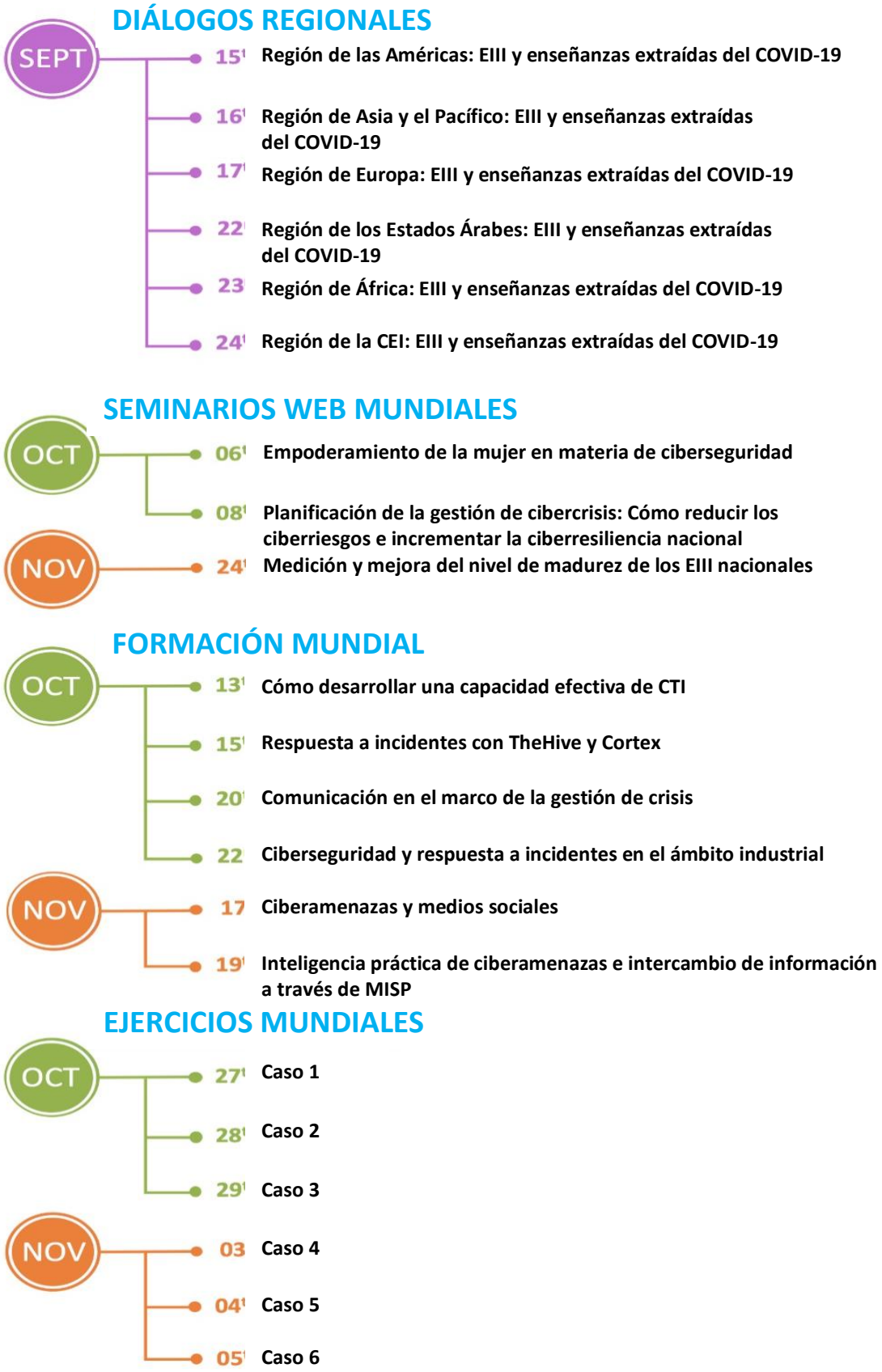
Los participantes recibirán la información relativa a la inscripción, incluidos los enlaces a las reuniones y otros datos al respecto, en la dirección de correo electrónico registrada. El plazo de inscripción en las sesiones de formación y los ejercicios se cerrará el miércoles 30 de septiembre de 2020, o en el momento en que se cubran todas las plazas.

## 7 DATOS DE CONTACTO

Si tiene alguna pregunta, no dude en ponerse en contacto con el coordinador regional de ciberseguridad de la UIT que le corresponda:

- Oficina Regional para África, Sr. Serge Valery Zongo (serge.zongo@itu.int)
- Oficina Regional para las Américas, Sr. Pablo Palacios (Pablo.Palacios@itu.int)
- Oficina Regional para los Estados Árabes, Sra. Rouda Al Amir Ali (Rouda.AlamirAli@itu.int)
- Oficina Regional para Asia y el Pacífico, Sr. Sameer Sharma, (sameer.sharma@itu.int)
- Oficina Regional para la CEI, Sr. Farid Nakhli (farid.nakhli@itu.int)
- Oficina Regional para Europa, Sr. Jaroslaw Ponder (jaroslaw.ponder@itu.int)

## 8 CALENDARIO DE EVENTOS




El orden del día se actualizará periódicamente en la página web del cibersimulacro; le rogamos consulte el calendario en línea para obtener información detallada y actualizada: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx.